

PROFESJONALNE TESTY PENETRACYJNE

Zbuduj własne środowisko do testów | Wydanie II



Thomas Wilhelm

 **Helion**

Tytuł oryginału: Professional Penetration Testing, Second Edition: Creating and Learning in a Hacking Lab

Tłumaczenie: Robert Górczyński

ISBN: 978-83-246-9033-6

Copyright © 2013 Elsevier, Inc.
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

This edition of Professional Penetration Testing: Creating and Learning in a Hacking Lab by Thomas Wilhelm is published by arrangement with ELSEVIER INC., a Delaware corporation having its principal place of business at 360 Park Avenue South, New York, NY 10010, USA.

Translation copyright © 2014 Helion SA

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie bierze jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Wydawnictwo HELION nie ponosi również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: <http://helion.pl> (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/protes>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Podziękowania	9
O autorze	11
O recenzencie technicznym	13
Przedmowa	15
Rozdział 1. Wprowadzenie	17
Wprowadzenie	17
Informacje o tym wydaniu książki	18
Przygotowanie do założenia laboratorium	19
Przeprowadzanie testów penetracyjnych	20
Wewnętrzne testy penetracyjne	21
Wymagane umiejętności	22
Łącza i pliki pomocnicze	22
Witryna HackingDojo.com	22
Maszyny wirtualne	23
Pliki konfiguracyjne urządzeń	25
Podsumowanie	26
Rozdział 2. Etyka i hacking	27
Uzyskanie pozwolenia na hacking	27
Kanon kodeksu etycznego (ISC) ²	28
Dlaczego warto zachować postawę etyczną?	29
Negatywni hakerzy	29
Pozytywni hakerzy	32
Neutralni hakerzy	33
Standardy etyczne	34
Certyfikaty	34
Przestępczość komputerowa	39
Rodzaje przestępstw komputerowych i ataków	40
Uzyskiwanie zgody na przeprowadzenie ataku	49
Umowa poufności	49
Zobowiązania firmy	50
Zobowiązania wykonawcy	51
Podsumowanie	54
Odwołania	54

4 Spis treści

Rozdział 3. Przygotowanie laboratorium	57
Wprowadzenie	57
Cele ataku w laboratorium przeznaczonym do testów penetracyjnych	58
Problemy związane z nauką hackingu	58
Rzeczywiste scenariusze	59
Gotowe scenariusze	61
Czym jest LiveCD?	62
Sieci wirtualne w laboratorium przeznaczonym do testów penetracyjnych	65
Zachowaj prostotę	65
Oprogramowanie służące do wirtualizacji	66
Ochrona danych testu penetracyjnego	74
Rodzaje szyfrowania	74
Zabezpieczenie systemu używanego do przeprowadzania testu penetracyjnego	76
Kwestie dotyczące bezpieczeństwa mobilnego	78
Dane laboratorium bezprzewodowego	78
Zaawansowane laboratoria przeznaczone do przeprowadzania testów penetracyjnych	79
Rozważania dotyczące sprzętu	80
Konfiguracja sprzętowa	81
Systemy operacyjne i aplikacje	83
Analiza złośliwego oprogramowania — wirusy i robaki	85
Inne cele ataków	92
Podsumowanie	95
Odwołania	95
Rozdział 4. Metodologia i frameworki	97
Wprowadzenie	97
Dokument ISSAF	97
Planowanie i przygotowania — faza 1.	98
Rekonesans — faza 2.	99
Zgłaszanie, sprzątanie i usuwanie zbędnych artefaktów — faza 3.	103
Podręcznik Open Source Security Testing Methodology Manual	104
Reguły postępowania	105
Kanały	106
Moduły	107
Podsumowanie	109
Odwołania	110
Rozdział 5. Zarządzanie projektem testu penetracyjnego	111
Wprowadzenie	111
Metryki testu penetracyjnego	112
Metody ilościowe, jakościowe i mieszane	112
Kierowanie testem penetracyjnym	117
Standard PMBOK	117
Członkowie zespołu projektu	129
Zarządzanie projektem	138

Przeprowadzanie testów penetracyjnych w pojedynkę	146
Etap rozpoczęcia	147
Etap planowania	147
Etap realizacji	148
Etap zakończenia	148
Monitorowanie i kontrola	148
Archiwizacja danych	149
Czy należy zachować dane?	149
Ochrona dokumentacji	152
Czyszczenie laboratorium	156
Archiwizacja danych laboratorium	157
Tworzenie i używanie obrazów systemów	158
Utworzenie „czystego systemu”	161
Planowanie następnego testu penetracyjnego	166
Rejestr zarządzania ryzykiem	166
Baza danych wiedzy	168
Wywiad po zakończeniu działania	171
Podsumowanie	174
Odwołania	174
Rozdział 6. Zbieranie informacji	175
Wprowadzenie	175
Pasywne zbieranie informacji	176
Obecność w sieci	177
Dane korporacyjne	187
Informacje uzyskane na podstawie whois i DNS	190
Dodatkowe zasoby internetowe	193
Aktywne zbieranie informacji	195
Zapytania DNS	195
Konta poczty elektronicznej	197
Identyfikacja granic sieci	199
Sprawdzanie sieci	203
Podsumowanie	205
Odwołania	205
Rozdział 7. Wykrywanie luk w zabezpieczeniach	207
Wprowadzenie	207
Skanowanie portów	208
Sprawdzenie istnienia celu ataku	209
Skanowanie UDP	213
Skanowanie TCP	213
Skanowanie unikające granic sieci	216
Identyfikacja systemów	220
Aktywne ustalanie systemu operacyjnego	221
Pasywne ustalanie systemu operacyjnego	221

6 Spis treści

Identyfikacja usług	224
Pozyskiwanie banerów	224
Wymienianie nieznanych usług	225
Identyfikacja luk w zabezpieczeniach	227
Podsumowanie	229
Rozdział 8. Wykorzystanie luk w zabezpieczeniach	231
Wprowadzenie	231
Narzędzia zautomatyzowane	233
Skrypty narzędzia nmap	235
Skanowanie loginu domyślnego	237
OpenVAS	239
JBroFuzz	240
Metasploit	242
Kod pozwalający na wykorzystanie luki w zabezpieczeniach	253
Witryny internetowe	253
Podsumowanie	256
Rozdział 9. Ataki w systemie lokalnym	259
Wprowadzenie	259
Wykorzystanie luk w zabezpieczeniach systemu	260
Wewnętrzne luki w zabezpieczeniach	260
Dane wrażliwe	265
Meterpreter	266
Powłoki i powłoki odwrotne	269
Powłoka netcat	270
Powłoka odwrotna netcat	273
Szyfrowane tunele	277
Dodanie zapory sieciowej (opcjonalne)	278
Konfiguracja powłoki odwrotnej SSH	279
Konfiguracja kluczy publicznych i prywatnych	279
Uruchomienie szyfrowanej powłoki odwrotnej	282
Inne metody szyfrowania i tunelowania	284
Podsumowanie	285
Rozdział 10. Eskalacja uprawnień	287
Wprowadzenie	287
Ataki na hasła	287
Zdalne ataki na hasła	288
Lokalne ataki na hasła	292
Ataki z użyciem słowników	294
Podsluchiwanie pakietów sieciowych	298
Socjotechnika	304
Wabienie	305
Phishing	305
Pretexting	306

Manipulacje danymi dzienników zdarzeń	306
Logowanie użytkownika	308
Dzienniki zdarzeń aplikacji	311
Ukrywanie plików	312
Ukrycie plików w zasięgu wzroku	313
Ukrycie plików za pomocą systemu plików	314
Ukrycie plików w systemie Windows	317
Podsumowanie	319
Odwołania	319
Rozdział 11. Ataki na systemy pomocnicze	321
Wprowadzenie	321
Ataki na bazy danych	321
Udziały sieciowe	329
Podsumowanie	332
Rozdział 12. Ataki na sieci	335
Wprowadzenie	335
Protokoły sieci bezprzewodowych	336
Atak na standard WPA	337
Ataki na WEP	342
Protokół SNMP	344
Podsumowanie	349
Rozdział 13. Ataki na aplikacje sieciowe	351
Wprowadzenie	351
SQL Injection	352
Cross-site scripting	354
Luki w zabezpieczeniach aplikacji sieciowych	356
Narzędzia zautomatyzowane	357
Podsumowanie	363
Rozdział 14. Prezentacja wyników testu	365
Wprowadzenie	365
Co powinno się znaleźć w raporcie?	366
Kwestie spoza zakresu	366
Odkrycia	367
Rozwiązania	368
Przygotowanie raportu	369
Raport wstępny	370
Recenzja merytoryczna	371
Sprawdzanie faktów	372
Metryki	373
Raport końcowy	380
Dodatkowa recenzja merytoryczna	380
Dokumentacja	381
Podsumowanie	390
Odwołania	391

8 Spis treści

Rozdział 15. Kariera w świecie hackingu	393
Wprowadzenie	393
Ścieżki kariery	396
Architektura sieci	396
Administracja systemem	398
Aplikacje i bazy danych	399
Certyfikaty	400
Certyfikaty na wysokim poziomie	403
Umiejętności i certyfikaty charakterystyczne dla producenta	415
Stowarzyszenia i organizacje	420
Organizacje zrzeszające profesjonalistów	421
Konferencje	422
Społeczności lokalne	427
Listy dyskusyjne	428
Zebranie wszystkiego w całość	429
Życiorys	430
Oferty pracy	432
Informacje dotyczące wynagrodzenia	433
Dokumenty osobiste	436
Podsumowanie	436
Odwołania	438
 Skorowidz	 441

ROZDZIAŁ 6.

Zbieranie informacji

W tym rozdziale omawiam:

- pasywne zbieranie informacji;
- aktywne zbieranie informacji.

WPROWADZENIE

Zbieranie informacji to pierwszy i bez wątpienia najważniejszy krok podczas przeprowadzania testu penetracyjnego. Po zakończeniu tej fazy powinniśmy dysponować dokładną mapą sieci celu ataku, a także znać ilość wysiłku, jaki trzeba będzie włożyć w pełne wykonanie zadania. Ponadto w trakcie tej fazy należy zidentyfikować rodzaje systemów w sieci (między innymi używane systemy operacyjne), co pozwoli na wybór odpowiedniego personelu oraz narzędzi używanych w pozostałej części projektu testu penetracyjnego. Klienci zwykle dostarczają sporo informacji dotyczących ich sieci, aby w ten sposób nieco Ci pomóc w wykonaniu zadania. Nie powinieneś się jednak zdziwić, gdy otrzymane informacje okażą się błędne. Dlatego też konieczne jest przeprowadzenie omawianej tutaj fazy niezależnie od ilości informacji otrzymanych od klienta.

Są dwa rodzaje zbierania informacji: zbieranie pasywne i zbieranie aktywne. W przypadku pasywnego zbierania informacji naszym celem jest zebranie maksymalnej ilości danych o systemach i sieci będących celem ataku, ale bez bezpośredniego łączenia się z nimi. Oznacza to również próbę zebrania wiadomości o korporacji, między innymi: kto jest jej właścicielem, gdzie mieści się siedziba, gdzie znajdują się komputery i sieć, jak jest zaprojektowana siedziba firmy (w przypadku, gdy trzeba przeprowadzić fizyczny test penetracyjny), i innych informacji, w zależności od celów projektu testu penetracyjnego.

Drugi rodzaj zbierania informacji to zbieranie aktywne. W tym przypadku następuje bezpośrednie połączenie z celem ataku. Ten rodzaj zbierania informacji ma za zadanie jedynie zapewnić lepsze rozeznanie w kwestii wysiłku koniecznego do włożenia, a także w kwestii ustalenia typu i liczby systemów, które ma objąć projekt. W dalszej części rozdziału dokładnie zostaną wymienione rodzaje gromadzonych informacji. W tym momencie najważniejsze jest, aby lepiej zrozumieć podejmowane przez nas działania.

Istnieje przekonanie, że aktywne zbieranie informacji jest bardziej użyteczne od technik pasywnych. Jednak bardzo często wymienione przekonanie jest fałszywe. Nierzadko zdarzało się, że dane wrażliwe lub o znaczeniu krytycznym wyciekły, a następnie zostały zarchiwizowane, nawet po usunięciu problemu. Podczas przeprowadzania testu penetracyjnego ten rodzaj błędów jest bardzo przydatny, zwłaszcza jeśli ujawnione informacje dotyczą atakowanej sieci. Wcale nie tak trudno znaleźć zarchiwizowane informacje o plikach konfiguracyjnych i instalacyjnych wraz z danymi poufnymi obejmującymi na przykład sekrety firmy.

W tym rozdziale skupimy się przede wszystkim na metodologii przedstawionej w dokumencie ISSAF (ang. *Information Systems Security Assessment Framework*). W wymienionej metodologii faza zbierania informacji została podzielona na kilka znacznie dokładniejszych kroków. Jednak zrealizujemy również cele przedstawione w podręczniku OSSTMM (ang. *Open Source Security Testing Methodology Manual*), w którym większość danych dotyczących zbierania informacji zawarto w module zatytułowanym *Logistics* i skoncentrowano się na wymienionych poniżej obszarach:

- framework,
- jakość sieci,
- czas.

Według podręcznika OSSTMM framework wiąże się ze wszystkim, co zostanie omówione w tym rozdziale, czyli z pasywnym i aktywnym zbieraniem informacji. Dodatkowe testy powiązane z jakością sieci i z czasem nie będą tutaj omówione, ponieważ są trudne do replikacji w laboratorium, jeśli nie zostanie wykorzystany dodatkowy sprzęt sieciowy. Test jakości sieci dotyczy utraty pakietów i współczynnika szybkości mierzonego w wielu sieciach, ale to naprawdę nie jest czynnik znaczący w małych i wielkich laboratoriach. Z kolei analiza czasu ma na celu synchronizację zegarów systemowych oraz harmonogramy pracy systemów i uczestników.

W tej fazie testu penetracyjnego będziemy zbierali wymienione informacje (a także wiele innych), ale całą operację podzielimy na dwie odmienne czynności: pasywne i aktywne zbieranie informacji, jak to zostało zasugerowane przez ISSAF. Mimo że dokument ten ma pewne istotne wady, tak naprawdę sprawdza się doskonale, dostarczając krok po kroku poleceń, jak zebrać niezbędne informacje. W tym rozdziale przeanalizujemy pewne wady nieodłącznie towarzyszące metodologii ISSAF. Jednak przedstawione tutaj sugestie mają za zadanie pomóc zrozumieć cele w wykonywanych krokach oraz wzbogacić wiedzę, aby w ten sposób zwiększyć Twoje umiejętności i efektywność podczas przeprowadzania testu penetracyjnego.

PASYWNE ZBIERANIE INFORMACJI

Jak wcześniej wspomniano, pasywne zbieranie informacji dotyczy gromadzenia danych przechowywanych w systemach, które nie znajdują się w sieci klienta. Podczas fazy zbierania informacji przeprowadzanych jest wiele rodzajów operacji wyszukiwania,

obejmujących dane niekoniecznie związane z siecią będącą celem ataku, na przykład informacje o pracownikach, o fizycznym położeniu i o działalności biznesowej. Poniżej wymieniono różne rodzaje danych, które mogą być zbierane na tym etapie.

- Ustalenie obecności celu ataku w sieci (uwaga: nie dotyczy to jedynie stron internetowych).
- Zgromadzenie zwracanych przez wyszukiwarki internetowe wyników dotyczących celu ataku.
- Wyszukanie grup internetowych zawierających komentarze pracowników firmy.
- Przeanalizowanie witryn domowych pracowników firmy.
- Zebranie informacji dotyczących zabezpieczeń oraz wszelkich danych finansowych o firmie będącej celem ataku.
- Sprawdzenie wszelkich witryn podających dane statystyczne o długości nieprzerwanego działania.
- Przejrzenie archiwalnych witryn internetowych w celu znalezienia dodatkowych informacji.
- Przeanalizowanie ofert pracy publikowanych przez cel ataku.
- Przejrzenie grup dyskusyjnych.
- Przeszukanie portali społecznościowych w celu zebrania informacji udostępnianych przez pracowników firmy.
- Sprawdzenie informacji podawanych firmie zajmującej się rejestracją i obsługą domen.
- Sprawdzenie, czy cel ataku udostępnia informacje DNS za pomocą usługi oferowanej przez firmę trzecią.

Po zakończeniu tej fazy osoba przeprowadzająca test penetracyjny będzie miała sporo informacji dotyczących celu ataku, nawet pomimo faktu, że jeszcze nie odwiedziła sieci będącej celem ataku. Wszystkie informacje zgromadzone w trakcie fazy pasywnego zbierania informacji pochodzą z zasobów firm trzecich, które zebrały dane o naszym celu ataku lub mają prawo tego rodzaju dane przechowywać.

Na końcu omawianej fazy osoba przeprowadzająca test penetracyjny może być zaskoczona ilością dostępnych w internecie informacji, nawet tych, które nie powinny być ujawniane. Po wykonaniu przedstawionych w rozdziale przykładów dotyczących gromadzenia informacji przekonasz się, jak trudno zachować prywatność i jak wiele zmieniło się w ostatnich dekadach na skutek gwałtownego rozwoju internetu.

Obecność w sieci

Ta faza bardzo często pozwala na zdobycie cennych danych dotyczących firmy klienta, na przykład informacji o pracownikach, lokalizacji fizycznej i logicznej, typów używanych systemów (między innymi marek i systemów operacyjnych), a także informacji o architekturze sieci. Na szczęście ta faza testu penetracyjnego opiera się na bardzo prostych narzędziach wymienionych w metodologii ISSAF. Są to:

- przeglądarka internetowa,
- Dogpile.com,
- Alexa.org,
- Archive.org,
- Shodanhq.com,
- dig,
- nslookup.

Do zdobycia informacji o celu wykorzystamy przede wszystkim witryny internetowe wymienione na powyższej liście, choć skorzystamy także z kilku innych witryn. Jak zwykle podręcznik OSSTMM nie zawiera żadnych zalecanych narzędzi i sugeruje oprzeć się na doświadczeniu osoby przeprowadzającej test penetracyjny i jej umiejętności wyboru najodpowiedniejszych i najbardziej użytecznych narzędzi. Witryny internetowe wymienione w dokumencie ISSAF, jak również użycie przeglądarki internetowej nie wymagają dalszych objaśnień. Prawdziwa trudność polega na zrozumieniu, jakich informacji szukamy. Odpowiedź brzmi: wszystkiego, co można znaleźć.

Poniżej przedstawiono listę sugerowanych informacji, których warto poszukać. Oczywiście lista ta na pewno nie jest kompletna. Elementy listy można dodawać (lub usuwać) w zależności od rodzaju podpisanej umowy i systemów będących celem ataku. Jednak poniższa lista stanowi dobry punkt wyjścia i powinna pomóc w określeniu innych rodzajów informacji, które mogą być dostępne w zależności od celu ataku. Im więcej informacji uda się zebrać w tej fazie, tym łatwiej będzie można wykonywać kolejne zadania.

- Adres (lub adresy) witryn internetowych.
- Typ serwera WWW.
- Położenie serwera.
- Daty, łącznie z datami ostatniej modyfikacji.
- Łącza internetowe — zarówno wewnętrzne, jak i zewnętrzne.
- Drzewo katalogów serwera WWW.
- Używane technologie (sprzęt i oprogramowanie).
- Standardy szyfrowania.
- Użyte sieciowe języki programowania.
- Pola (w tym również ukryte) formularzy sieciowych.
- Zmienne formularzy.
- Metoda przekazywania formularzy do serwera WWW.
- Informacje kontaktowe firmy.
- Znaczniki meta.
- Wszelkie komentarze na stronach internetowych.
- Możliwości w zakresie e-commerce'u.
- Oferowane usługi i produkty.

Ostrzeżenie

Informacje zebrane w tej fazie mogą nie być upublicznione. Bardzo ważne jest, aby osoba przeprowadzająca test penetracyjny traktowała te wszystkie informacje jako „zastrzeżone”, nawet jeśli zostały znalezione w publicznie dostępnych witrynach internetowych.

Ze względu na to, że koncepcje znacznie łatwiej zrozumieć przez *działanie*, a nie tylko czytanie o nich, przejdziemy teraz do przykładu praktycznego. Kiedy będziesz wykonywać kroki przedstawione w książce, pamiętaj, że informacje mogły ulec zmianie od chwili jej pisania. Jednak celem ćwiczenia jest przekonanie się, dlaczego zbieramy niezbędne informacje, a nie przedstawienie kolejnych kroków do wykonania, ponieważ takie rozwiązanie okazuje się po prostu nieelastyczne i prowadzi do powstania luk w wiedzy. Dzięki zrozumieniu, *dlaczego* wykonujemy działania przedstawione w tej fazie, zyskasz większe umiejętności w zakresie przeprowadzania profesjonalnego testu penetracyjnego niż w przypadku ich wykonywania zawsze w ten sam sposób, przez powtarzanie tych samych kroków wyuczonych na pamięć.

Przyjmujemy założenie, że nigdy nie słyszeliśmy o narzędziu nmap. Jeżeli użyjemy wyszukiwarki internetowej w celu zdobycia bogatszych informacji na temat wymienionego narzędzia i jego twórcy, wtedy prawdopodobnie trafimy na trzy różne witryny internetowe powiązane z narzędziem nmap, jak pokazano na rysunku 6.1. Witryna <http://nmap.org/> wydaje się naturalnym wyborem, ale <http://insecure.org/> i <http://sectools.org/> zdają się być pośrednio powiązane ze skanerem nmap.

Insecure.Org - Nmap Free Security Scanner, Tools & Hacking resources
 Network Security Tools/Software (Free Download) including Nmap Open Source Network Security Scanner; Redhat Linux, Microsoft Windows, FreeBSD, UNIX Hacking.
insecure.org/ - [Similar pages](#)

Download the Free Nmap Security Scanner for Linux/MAC/UNIX or Windows
 Official Download site for the Free Nmap Security Scanner. Helps with network security, administration, and general hacking.
nmap.org/download.html - 2 hours ago - [Similar pages](#)

Chapter 8. Remote OS Detection
 Chapter 8. Remote OS Detection. Table of Contents. Introduction · Reasons for OS Detection · Determining vulnerability of target hosts · Tailoring exploits ...
nmap.org/book/osdetect.html - [Similar pages](#)

Nmap: The Art of Port Scanning
 The Art of Port Scanning - by Fyodor. WARNING: this page was last updated in 1997 and is completely out of date. If you aren't here for historical purposes, ...
nmap.org/nmap_doc.html - [Similar pages](#)

Top 100 Network Security Tools
 Review of the top 100 network security tools (free or commercial), as voted on by 3200 Nmap Security Scanner users.
sectools.org/ - [Similar pages](#)

RYSUNEK 6.1.

Witryny internetowe zawierające informacje o narzędziu nmap

Zanim przejdziemy do kolejnego kroku, warto przypomnieć, że to dopiero połowa fazy zbierania informacji. Jak dotąd gromadzimy dane, nawet nie dotykając systemu lub sieci będącej celem ataku — oznacza to, że nie klikamy łączy wyświetlonych w wynikach wyszukiwania. Bez wątpienia pojedyncze kliknięcie i przejście na stronę internetową celu nie spowoduje wywołania alarmu — w końcu firma będąca naszym celem chce, aby jej witryna internetowa była odwiedzana i dlatego wspomniana witryna jest dostępna w internecie. Jednak bardzo ważne jest zrozumienie, jak wiele informacji można po prostu znaleźć w innych zasobach internetu. Ponadto duża ilość interesujących nas danych nie znajduje się już w witrynie internetowej celu, ale została zachowana w archiwach internetu. Inną zaletą pasywnego zbierania informacji jest to, że im później pojawisz się na radarze celu ataku, tym lepiej, zwłaszcza gdy inżynierowie odpowiedzialni za sieć klienta wiedzą o zleceniu na przeprowadzenie testu penetracyjnego. Im mniej *szumu*, tym mniejsze prawdopodobieństwo, że administratorzy systemu spróbują zabezpieczyć go przed penetracją.

W dalszej części testu penetracyjnego sprawdzimy, jak administratorzy reagują na próbę włamania. Teraz z pewnością nie chcemy, aby zaczęli dokładniej analizować dzienniki zdarzeń i blokować nasze działania już na wczesnym etapie testu penetracyjnego.

Warto pamiętać, że w trakcie omawianej fazy wreszcie dotrzemy do usług innych niż WWW, co niewątpliwie zwiększy niebezpieczeństwo wykrycia naszej działalności. Im dłużej pozostajemy niewykryci i unikamy kontaktu z siecią będącą celem ataku, tym lepiej dla nas.

Mamy więc trzy witryny internetowe związane z celem. Przystępujemy do zdobycia nieco większej ilości informacji. Z przedstawionej wcześniej listy narzędzi wybieramy teraz witrynę <http://www.alex.com/>. Na rysunku 6.2 pokazano wyraźnie, że według Alexa.org witryny <http://nmap.org/> i <http://insecure.org/> są powiązane, ponieważ łącznie Site info witryny <http://nmap.org/> wskazuje witrynę <http://insecure.org/>. Jeżeli wykonasz to samo zapytanie, dokonasz kolejnego interesującego odkrycia, pokazanego na rysunku 6.3. Wydaje się, że witryna <http://nmap.org/> obsługuje subdomeny, na co wskazuje istnienie jednej z nich — scanme.nmap.org. Ponadto nazwa sugeruje możliwość przeprowadzenia skanowania odkrytej subdomeny. Skoro jesteśmy na etapie pasywnego zbierania informacji i nie chcemy połączyć się z siecią będącą celem ataku, wstrzymamy się teraz z przeprowadzeniem operacji skanowania.



Nmap - Free Security Scanner For Network Exploration & Security...
Nmap Free Security Scanner For Network Exploration & Hacking. Download open source software for Redhat Linux,Microsoft Windows,UNIX,FreeBSD,etc.
nmap.org
Site info for insecure.org



Insecure.Org - Nmap Free Security Scanner, Tools & Hacking resources
Network Security Tools/Software (Free Download) including Nmap Open Source Network Security Scanner; Redhat Linux,Microsoft Windows,FreeBSD,UNIX Hacking.
insecure.org
Site info for insecure.org

RYSUNEK 6.2.

Wyświetlone przez Alexa.org wyniki dla zapytania nmap



Go ahead and ScanMe!

Hello, and welcome to Scanme.Nmap.Org, a service provided by the Nmap Security Scanner Project and Insecure.Org. We set up this machine to help folks learn about Nmap and also to ...
 scanme.nmap.org
 Site info for insecure.org

RYSUNEK 6.3.

Informacje dodatkowe dotyczące witryny nmap.org

Jeżeli w witrynie Alexa.org te same zapytania wykonamy dla domen insecure.org i sectools.org, uzyskamy informacje podobne jak w przypadku witryny nmap.org, łącznie z istnieniem subdomeny scanme.insecure.org. Na tym etapie po dodaniu nowego celu do listy możemy powrócić na początek fazy zbierania informacji i dołączyć nowe adresy URL do listy witryn przeznaczonych do sprawdzenia. Gromadzenie danych to najczęściej odpowiedni krok. Jednak ostateczną decyzję pozostawiam Tobie — powtórzenie tutaj tych samych działań nie przyczyni się do lepszego zrozumienia zaprezentowanych wcześniej kroków.

Zdobyliśmy pewną ilość informacji dotyczących witryny nmap.org, a więc możemy już przystąpić do odwiedzenia samej witryny internetowej — na tym etapie także nie dotykamy bezpośrednio systemu będącego celem ataku. Istnieje kilka witryn internetowych archiwizujących bieżące i dawne strony znajdujące się w serwerze WWW naszego celu. Do wspomnianych witryn zalicza się między innymi google.com, ale rozpoczniemy od archive.org, czyli witryny pozwalającej na obserwację zmiany danej witryny internetowej w ciągu lat. Zaletą archive.org jest przechowywanie informacji, które nie są dłużej dostępne za pomocą Google'a ani obecne w bieżącej wersji docelowej witryny internetowej.

Wskazówka

Witryna archive.org nie oferuje archiwum z ostatnich sześciu miesięcy. Jeżeli potrzebujesz jednej z najnowszych migawek strony internetowej, powinieneś skorzystać z oferowanej przez Google'a funkcji buforowania strony.

Na rysunku 6.4 pokazano wyniki zapytania w witrynie archive.org. Jak możesz się przekonać, witryna nmap.org była archiwizowana przez wiele lat, począwszy od 2000 roku. Teraz zapoznamy się z jedną z ostatnich wersji witryny, wprowadzoną 24 września 2006 roku. Istnieje jeszcze nowsza wersja, ale według archive.org nie różni się zbyt wiele od wersji z 24 września 2006 roku. Jeżeli przeprowadzasz prawdziwy test penetracyjny, wówczas prawdopodobnie przejrzysz wszystkie dostępne łącza, aby przekonać się, jakie informacje zostały dodane lub usunięte w trakcie kolejnych uaktualnień. Witryny internetowe zmieniają się z różnych powodów. Nas najbardziej interesuje jeden z nich, czyli naprawa pomyłek związanych z ujawnieniem informacji wrażliwych o sieci, serwerze lub personelu.

INTERNET ARCHIVE
WaybackMachine

Enter Web Address: All

Searched for <http://nmap.org> 107 Results

Note some duplicates are not shown. [See all](#).
 * Denotes when site was updated.
 Material typically becomes available here 6 months after collection. [See FAQ](#).

Search Results for Jan 01, 1996 - Jul 08, 2008

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
0 pages	0 pages	0 pages	0 pages	4 pages	15 pages	11 pages	25 pages	15 pages	9 pages	11 pages	1 pages	0 pages
				Aug 16, 2000 *	Jan 19, 2001 *	Jan 19, 2002	Feb 07, 2003	Apr 06, 2004	Feb 11, 2005	Jan 01, 2006	Jul 03, 2007	
				Sep 30, 2000 *	Feb 01, 2001 *	Mar 25, 2002	Feb 08, 2003	Apr 12, 2004	Feb 13, 2005	Jan 02, 2006		
				Oct 17, 2000	Feb 02, 2001 *	Mar 28, 2002	Feb 14, 2003	May 18, 2004	Mar 24, 2005	Jan 03, 2006		
				Oct 19, 2000	Feb 02, 2001 *	May 25, 2002	Feb 17, 2003	May 20, 2004	Nov 08, 2005 *	Jan 04, 2006		
					Feb 26, 2001 *	Jun 02, 2002	Mar 29, 2003 *	Jun 05, 2004	Nov 24, 2005	Feb 02, 2006 *		
					Mar 01, 2001 *	Jun 06, 2002 *	Apr 19, 2003	Jun 12, 2004	Dec 14, 2005	Mar 15, 2006 *		
					Mar 02, 2001 *	Sep 23, 2002 *	Apr 22, 2003	Jun 14, 2004	Dec 24, 2005	Apr 24, 2006 *		
					May 04, 2001 *	Sep 28, 2002	Apr 23, 2003	Jul 27, 2004	Dec 25, 2005	Jul 02, 2006 *		
					Jun 21, 2001 *	Nov 25, 2002 *	May 25, 2003 *	Aug 31, 2004	Dec 31, 2005	Aug 24, 2006 *		
					Jun 28, 2001	Nov 27, 2002	Jun 04, 2003	Sep 01, 2004		Sep 17, 2006		
					Jul 20, 2001 *	Nov 29, 2002	Jun 05, 2003	Sep 06, 2004		Sep 24, 2006 *		
					Sep 24, 2001 *		Jun 10, 2003	Sep 19, 2004				
					Nov 08, 2001 *		Jul 22, 2003 *	Sep 26, 2004				
					Nov 30, 2001 *		Aug 08, 2003	Nov 27, 2004				
					Dec 05, 2001		Sep 23, 2003 *	Nov 30, 2004				
							Sep 30, 2003					
							Oct 16, 2003 *					
							Oct 29, 2003 *					
							Nov 10, 2003					
							Nov 26, 2003 *					
							Nov 28, 2003					
							Dec 15, 2003					
							Dec 19, 2003					
							Dec 23, 2003					
							Dec 28, 2003					

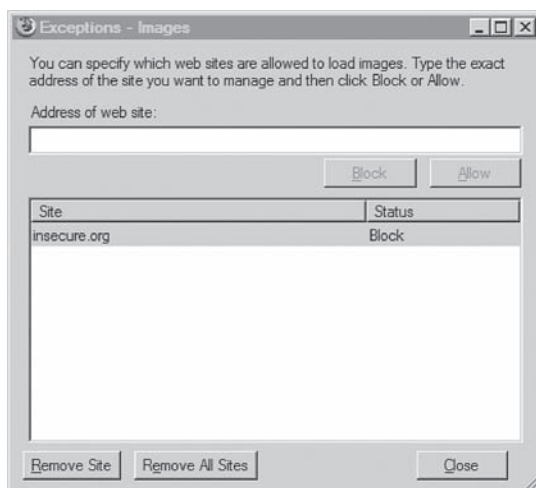
RYSunek 6.4.

Wyniki zapytania wykonanego w witrynie archive.org

Zanim przejdiesz dalej, powinienes wiedziec, ze pewne zarchiwizowane strony moga nawiazywac polaczenie z serwerem WWW bacydym celem ataku. Tego rodzaju polaczenie jest bardzo czysto wykonywane w celu pobrania obrazow. Skoro jesteemy na etapie pasywnego zbierania informacji, chcemy jak najdluzej pozostac niewykryci i dlatego powinniemy zabronic przegladarce internetowej pobierania obrazow z witryny insecure.org. Wprawdzie tego rodzaju rozwiyzanie jest ekstremalne nawet w trakcie rzeczywistego testu penetracyjnego, ale w ten sposob zmniejszamy ryzyko chocby przypadkowego nawiyzania polaczenia z celem ataku. Wspomniane ograniczenie mozna nalozyc przez zdefiniowanie wyjatku w przegladarce internetowej. Na przyklad w przegladarce Firefox przejdz do *Narzedzia/Opcje/Treść* i kliknij przycisk *Wyjatki...* umieszczony obok *Pobieraj obrazki automatycznie*¹. Na rysunku 6.5 pokazano okno dialogowe, w ktorym wida wyjatki zdefiniowane dla witryny insecure.org. Wprawdzie nie uniemozliwi to wszelkich kontaktow z systemem bacydym celem ataku, ale stanowi dodatkowy poziom kontroli. Takie rozwiyzanie jest rowniez wystarczajace na potrzeby pokazania, jak zbierac informacje bez przeprowadzania bezposredniej komunikacji z celem.

Po wybraniu wyniku z 24 wrzesnia 2006 roku na ekranie zostanie wyswietlona witryna z podanego dnia (zob. rysunek 6.6). Od razu mozna dostrzec, ze witryny insecure.org i sectools.org sa ze soba powiazane za pomoca obrazow uzywanych w obu tych portalach.

¹ W nowszych wersjach przegladarki Firefox wymieniona opcja w ustawieniach zostala usunieta — *przyp. tłum.*



RYSUNEK 6.5.

Wyłączenie automatycznego pobierania obrazów z witryny insecure.org

Narzędzia i pułapki

Całkowite wyłączenie dostępu do systemu będącego celem ataku

Jeżeli chcesz w maksymalnym stopniu zapewnić sobie niewykrywalność, wtedy na etapie zbierania informacji możesz zablokować wszystkie połączenia z witryną internetową celu. Pewne witryny internetowe, na przykład google.com i archive.org, będą nawiązywały połączenia z serwerem WWW celu, jeśli nie zostaną podjęte dodatkowe środki bezpieczeństwa. Oczywiście możliwość dostępu do wspomnianej witryny internetowej celu można włączyć z powrotem na dalszym etapie testu penetracyjnego. W systemie Microsoft Windows ograniczenie dostępu do systemu docelowego można przeprowadzić za pomocą przycisku *Opcje internetowe*, a dokładnie przez dodanie witryny do strefy *Witryny z ograniczeniami*.



RYSUNEK 6.6.

Buforowana przez archive.org witryna internetowa nmap.org

Aby zebrać maksymalną ilość informacji o witrynie będącej celem ataku, należy kliknąć wszystkie łącza wyświetlone na stronie, w szczególności te, które znajdują się w lewej kolumnie. Po kliknięciu łącza *Intro* (przenoszącego nas na stronę: <http://web.archive.org/web/20060303150420/www.insecure.org/nmap/> nadal dostępną w archiwum archive.org) odkrywamy wiele różnych informacji, w tym łącza do wiadomości o licencji, opis narzędzia nmap, łącza do dokumentacji i tak dalej.

Przewijając stronę do dołu, docieramy do list dyskusyjnych, jak pokazano na rysunku 6.7. Jeżeli analizujemy łącze seclists.org (wymienioną nazwę domeny należy dodać do listy witryn powiązanych z narzędziem nmap), odkrywamy łącza prowadzące do archiwalnych postów w różnych listach dyskusyjnych, w tym także dotyczących narzędzia nmap. Archiwum dostępne w witrynie archive.org obejmuje wiadomości z lat 2000 – 2004 i zawiera użyteczne informacje o narzędziu nmap, nawet pomimo braku wzmianki o dostępności danych sprzed roku 2004.



RYSUNEK 6.7.

Informacje dotyczące list dyskusyjnych w witrynie insecure.org

Po przeczytaniu wybranych postów odkryjemy adres e-mail autora narzędzia (Fyodora, jak się wkrótce okaże; jego prawdziwe imię i nazwisko to Gordon Lyon), co pokazano na przykładowym fragmencie na rysunku 6.8. Odkrywamy także nowe adresy e-mail, które zaczynamy dodawać do innych zebranych podczas analizy archiwum listy dyskusyjnej.



RYSUNEK 6.8.

Fragment pobrany z listy dyskusyjnej poświęconej narzędziu nmap

Zanim opuścimy kilka ostatnich rysunków, warto spojrzeć na formularz subskrypcji listy dyskusyjnej, który pokazano wcześniej na rysunku 6.7. Dzięki analizie kodu źródłowego (w witrynie archive.org) wspomnianego formularza zyskujemy wiedzę na temat sieci i systemów celu ataku. Kod źródłowy formularza przedstawia się następująco:

```
<FORM ACTION="/cgi-bin/subscribe-nmap-hackers.cgi" METHOD="GET">
<INPUT TYPE="text" NAME="emailaddy" SIZE=20>
<font color="#000000"><INPUT TYPE="submit" VALUE="Subscribe to Nmap-hackers"></font>
</FORM>
```

Nie jest to zbyt ekscytujący kod (brak ukrytych pól formularza sieciowego), ale dostarcza pewnych informacji, takich jak fakt istnienia katalogu `/cgi-bin` oraz używania metody GET protokołu HTTP. W systemie docelowym znajduje się jeszcze jeden formularz sieciowy, używany do przeprowadzenia operacji wyszukiwania i łączący się z Google'em. Na tym etapie testu penetracyjnego nie jest to dla nas szczególnie interesujące. Jednak dzięki zebraniu tego rodzaju informacji można się dowiedzieć o użyciu w systemie docelowym aplikacji, która ma znane luki w zabezpieczeniach. Wykorzystywanie wspomnianych aplikacji można bardzo często odkryć tylko przez analizę kodu źródłowego stron internetowych.

Czego jeszcze możemy się dowiedzieć o naszym celu ataku? Przeanalizujmy kwestię subdomen. Dokument ISSAF sugeruje użycie witryny internetowej netcraft.com do wyszukania listy wszystkich subdomen powiązanych z daną witryną internetową. Na rysunkach od 6.9 do 6.11 pokazano subdomeny, które według netcraft.com istnieją dla naszego celu ataku.

Results for .insecure.org				
Found 4 sites				
Site	Site Report	First seen	Netblock	OS
1. cgi.insecure.org		november 2003	titan networks	linux - fedora
2. download.insecure.org		february 2002	new dream network, llc	linux
3. www.insecure.org		march 1998	titan networks	linux - fedora
4. images.insecure.org		november 2002	titan networks	linux - fedora

RYSUNEK 6.9.

Wynik zapytania insecure.org w witrynie netcraft.com

Results for .sectools.org				
Found 1 site				
Site	Site Report	First seen	Netblock	OS
1. mirror.sectools.org		may 2007	titan networks	linux - fedora

RYSUNEK 6.10.

Wynik zapytania sectools.org w witrynie netcraft.com

Results for .nmap.org				
Found 2 sites				
Site	Site Report	First seen	Netblock	OS
1. scanme.nmap.org		october 2005	titan networks	linux - fedora
2. www.nmap.org		may 2000	titan networks	linux - fedora

RYSUNEK 6.11.

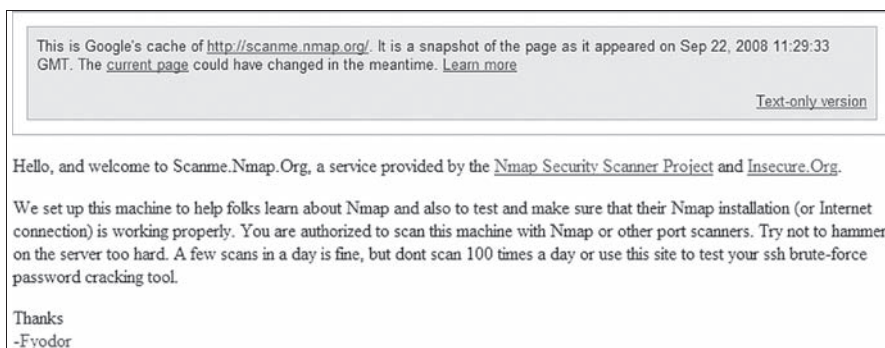
Wynik zapytania nmap.org w witrynie netcraft.com

Podstawową witryną dla Fyodora wydaje się insecure.org — zawiera trzy subdomeny. Wracając z powrotem do archive.org, subdomena download.insecure.org wygląda na stronę z nowościami wyświetlaną na stronie głównej witryny. Niczego nowego tutaj nie znajdziemy. A co z subdomeną images.insecure.org? Jeżeli przeanalizujesz łącze, znajdziesz tekst odwołujący się do firmy VA Linux Systems, Inc, która później stała się VA Software Corporation, a następnie SourceForge, Inc. Wydaje się, że subdomena jest nadal używana, ale strona początkowa nie została zmodyfikowana od dość długiego czasu. Taka informacja może być użyteczna w przyszłości, ale teraz jest tylko interesującym drobiazgiem. Użyteczne informacje to również te dotyczące systemu operacyjnego. Wykorzystamy je na dalszym etapie testu penetracyjnego.

Wprawdzie wspomniane subdomeny mogą zawierać dodatkowe katalogi z użytecznymi dla nas informacjami, ale pobieżne przejrzanie Google'a i witryny archive.org nie wskazuje na istnienie czegokolwiek w odkrytych subdomenach. Prowadząc dalszą analizę, możemy powrócić do Google'a i wykonać zapytanie `site:cgi.insecure.org`, którego wykonanie daje 46 różnych stron, łącznie z prezentacjami przedstawianymi na konferencjach dotyczących bezpieczeństwa. (Może to być niezwykle pomocne w lepszym zapoznaniu się z działaniem narzędzia, ale niekoniecznie ma związek z przeprowadzanym przez nas testem penetracyjnym, jeśli rzeczywiście chcemy taki wykonać). W przypadku subdomen nadzieje na zdobycie większej ilości informacji dotyczących witryny i narzędzia nmap wiążemy z `cgi.insecure.org`, ponieważ odkryty wcześniej katalog `/cgi-bin` zawiera skrypty, które ewentualnie mogą zawierać możliwe do wykorzystania luki w zabezpieczeniach.

Wyszukanie `mirror.sectools.org` za pomocą Google'a i witryny archive.org nie przynosi wyników. Chociaż domena może zawierać przydatne dla nas informacje, na tym etapie nie zgromadzimy większej ilości danych, dopóki nie nawiążemy połączenia z celem ataku. W przeciwnym razie niczego więcej nie znajdziemy już w archiwalnych rekordach. Warto wrócić do wspomnianej subdomeny później, gdy cel będziemy dokładnie analizować podczas testu penetracyjnego.

Wykonanie zapytania `scanme.nmap.org` w witrynie archive.org nie przynosi wyników. Z kolei po przejściu do Google'a możemy zobaczyć buforowaną wersję witryny. Na rysunku 6.12 pokazano, co się znajduje (a raczej *znajdowało się*) na stronie. Okazuje się, że dzięki Fyodorowi dysponujemy w internecie celem, względem którego można przeprowadzić skanowanie. Możliwość tę wykorzystamy później, w trakcie doskonalenia technik skanowania w internecie.



RYСУNEK 6.12.

Buforowana wersja strony scanme.nmap.org

Według Google'a z analizowaną subdomeną nie są powiązane żadne inne strony. Ponownie istnieje możliwość, że dowiemy się więcej po faktycznym nawiązaniu połączenia z atakowanym celem. Jednak teraz jesteśmy zadowoleni z poczynionych odkryć.

Dane korporacyjne

Ten krok pozwoli nam lepiej zrozumieć, kto stoi za narzędziem nmap, gdzie się znajduje, czy i jakich zatrudnia pracowników, a być może odkryjemy także jakieś informacje dotyczące sieci. W tym miejscu trzeba koniecznie zwrócić uwagę na to, jak głęboko zejdziemy na tym etapie testu penetracyjnego. Jeśli poświęcimy odpowiednią ilość czasu, istnieje duże prawdopodobieństwo odkrycia informacji osobistych, takich jak miejsca zamieszkania pracowników korporacji lub ich prywatne numery telefonów. Jeżeli nie jest wymagane przeprowadzenie działań z zakresu socjotechniki, to zbierając tego rodzaju informacje, możesz przekroczyć granice etyczne. Nawet jeśli wspomniane informacje są dostępne, nie oznacza to, że musisz je zgromadzić.

To samo dotyczy prywatnych stron internetowych pracowników korporacji, na przykład ich blogów lub witryn związanych z rodziną. Być może uda się tam znaleźć pewne użyteczne informacje, takie jak uzyskane przez inżynierów certyfikaty z zakresu systemów operacyjnych lub aplikacji. Jednak nie oznacza to, że o pracownikach korporacji powinieneś gromadzić informacje takie, jak ich znaki zodiaku lub zdjęcia bliskich (to będzie wyjątkowo podłe). Pamiętaj o zachowaniu równowagi między informacjami faktycznie użytecznymi a po prostu dostępnymi.

Spójrzmy na strony informacyjne witryn insecure.org i sectools.org (w tym przypadku mamy tylko dwie wymienione opcje, ponieważ łącznie z witryny nmap.org prowadzi do witryny insecure.org). Na rysunku 6.13 pokazano informacje kontaktowe obejmujące adres siedziby, numer telefonu i adres e-mail. W przypadku witryny sectools.org informacje pozostają takie same, poza adresem e-mail. Zwróć uwagę na nazwę firmy — Insecure.com — która w ten sposób dostarcza nam jeszcze jedną nazwę domeny do sprawdzenia.

Company Info for insecure.org:

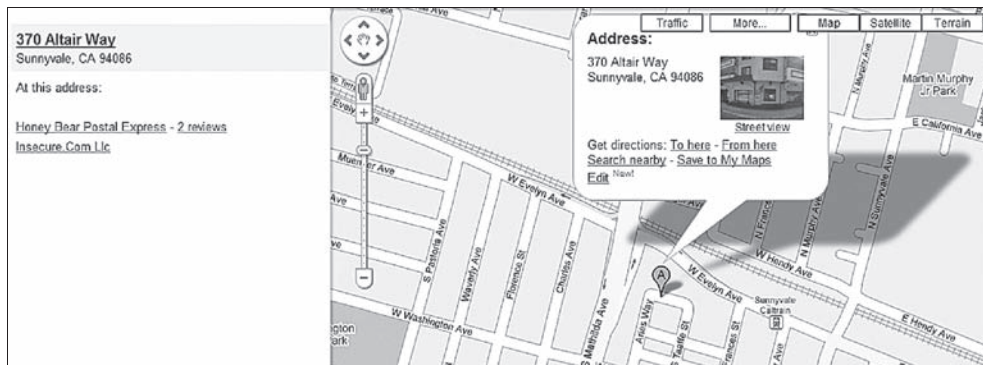
Insecure.Com Lic
 370 Altair Way #113
 Sunnyvale, CA
 94086
 US

Phone: +1 530 323 8588
 hostmaster[at]insecure.org

RYSUNEK 6.13.

Informacje o firmie, które znajdziemy w witrynie insecure.org

W jaki sposób możemy wykorzystać zebrane informacje? Jeżeli mamy fizycznie sprawdzić bezpieczeństwo siedziby, więcej informacji można zdobyć za pomocą map Google'a. Na rysunku 6.14 pokazano położenie na mapie Google'a adresu widocznego na rysunku 6.13, a także informacje dotyczące budynku. Na podstawie znalezionych tutaj informacji dowiadujemy się, że firma Insecure.com do prowadzenia biznesu korzysta ze skrzynki pocztowej.

**RYSUNEK 6.14.**

Wynik w mapach Google'a otrzymany po podaniu adresu firmy Insecure.com

Jeżeli adres wskazywałby budynek dużej korporacji, opcja *Street View* dostarczyłaby wielu użytecznych szczegółów, takich jak budynki przyległe lub znajdujące się po drugiej stronie ulicy, położenie drzwi, okien, drogi wejścia/wyjścia, a także być może pewnych informacji dotyczących zabezpieczeń, na przykład oświetlenia, monitoringu, kontroli dostępu. Jeżeli te informacje nie są wystarczające, wtedy można wykorzystać Google Earth (<http://www.google.com/earth/>) w celu przejrzenia widoku satelitarnego okolicy, co może dostarczyć wielu informacji dodatkowych, takich jak parkingi, inne drogi i tak dalej. Użycie map Bing (<http://www.bing.com/maps/>) również może dać inny punkt widzenia, pozwalając nam na użycie wielu narzędzi do tego samego celu, a tym samym zwiększając możliwość zidentyfikowania unikalnych danych.

Analizę archiwum możemy prowadzić dalej, aby się przekonać, czy uda się zebrać jeszcze inne informacje dotyczące narzędzia nmap lub Fyodora. Jednak po przejściu do Google'a i wykonaniu zapytania „nmap fyodor palo alto” odkryjemy następujące łącze do Wikipedii: http://en.wikipedia.org/wiki/Gordon_Lyon. Na tym etapie już wiemy, kim jest

autor narzędzia nmap. W chwili pisania tej książki w wymienionym artykule Wikipedii znajdowało się również zdjęcie Gordona. Teraz oprócz nazwiska znamy też twarz Gordona, choć nie przekłada się to na żaden praktyczny sposób użycia. Jednak zdjęcia pracowników korporacji będącej celem ataku mogą być niezwykle użyteczne w innych projektach testów penetracyjnych, zwłaszcza w tych, które wymagają zastosowania socjotechniki.

Skoro doskonale wiemy, że informacje opublikowane w Wikipedii mogą być nieprawdziwe, warto poszukać innych źródeł informacji o właścicielu interesujących nas witryn internetowych. Powracając do rysunku 6.13, przypominamy sobie, że nazwa firmy to Insecure.com. Zaletą szukania informacji o firmie jest fakt, że firmy są rejestrowane przez organy administracji państwowej. W przypadku Insecure.com odkrywamy, że firma znajduje się w stanie Kalifornia, którego władze przygotowały portal zawierający informacje związane z firmami zarejestrowanymi w tym stanie.

Na rysunku 6.15 możesz zobaczyć wynik wykonania zapytania dotyczącego firmy Insecure.com. Według informacji dostępnych na stronie <http://www.sos.ca.gov/business/> właścicielem firmy jest Gordon Lyon, co potwierdza dane zamieszczone w Wikipedii.

The screenshot shows the California Business Portal interface. At the top, there's a header with the state seal and the name 'Secretary of State DEBRA BOWEN'. Below this are navigation tabs: SECRETARY OF STATE, ELECTIONS & VOTER INFO, POLITICAL REFORM, CA BUSINESS PORTAL (selected), ARCHIVES & MUSEUM, and OTHER SERVICES. The main content area is titled 'LP/LLC' and 'Limited Partnerships/Limited Liability Companies'. It includes a search bar with the text 'INSECURE.COM LLC' and a 'New Search' button. To the left is a sidebar with various links like 'Business Search LP/LLC', 'Printer Friendly Page', 'New Search', 'Search Tips', 'Field Definitions', 'Status Definitions', 'LLC Name Availability', 'LP Name Availability', 'Business Entities', 'Records Order Form', 'Certificates', 'Copies', 'Status Reports', 'LLC FAQs', 'LP FAQs', 'LLC Main Page', 'LP Main Page', and 'Site Search'. The main results area shows details for 'INSECURE.COM LLC' with fields for Number (200010310013), Date Filed (4/6/2000), Status (active), Jurisdiction (CALIFORNIA), Address (370 ALTAIR WAY #113, SUNNYVALE, CA 94086), and Agent for Service of Process (GORDON LYON, 370 ALTAIR WAY #113, SUNNYVALE, CA 94086). There are 'Printer Friendly' and 'New Search' buttons at the bottom. A disclaimer at the bottom states that fees and instructions for requesting certification of limited partnership and/or limited liability company records are included on the Business Entities Records Order Form, and that blank fields indicate information not contained in the computer file.

RYСУNEK 6.15.

Informacje o firmie Insecure.com znajdujące się w portalu prowadzonym przez władze Kalifornii

Informacje z portalu stanowego potwierdzają także adres (Sunnyvale w Kalifornii) jako siedzibę firmy, co wcześniej zostało przez nas ustalone — tam mieści się firmowa skrzynka pocztowa. Wiemy także, kiedy został złożony wniosek o rejestrację firmy jako spółki o ograniczonej odpowiedzialności. Z powodu kosztów oraz faktu, że informacje o firmach

mają być publicznie dostępne, większość stanów prowadzi portale zawierające dane o firmach, ich właścicielach i siedzibach². Dzięki temu zdobycie wiadomości dotyczących firmy stało się znacznie łatwiejsze i nie wymaga nawet połączenia z siecią sprawdzanej korporacji.

Informacje uzyskane na podstawie whois i DNS

Spójrzmy na informacje DNS dotyczące witryny internetowej nmap.org. Na rysunku 6.16 pokazano wiele informacji, przede wszystkim adres IP witryny (64.13.134.48), łącznie z dodatkowymi subdomenami (<http://mail.nmap.org/>).

NAME SERVERS				SOA RECORD	
Name Server	IP	Location		Name Server	ns1.titan.net
ns1.titan.net	64.13.134.58	Palo Alto, CA, US		Email	hostmaster@insecure.org
ns2.titan.net	64.13.134.59	Palo Alto, CA, US		Serial Number	2008091400
ping.nmap.org				Refresh	8 hours
				Retry	1 hour
				Expiry	7 days
				Minimum	1 day

DNS RECORDS				
Record	Type	TTL	Priority	Content
*.nmap.org	A	1 day		64.13.134.48 (Palo Alto, CA, US)
mail.nmap.org	MX	1 day	0	mail.titan.net
nmap.org	A	1 day		64.13.134.48 (Palo Alto, CA, US)
nmap.org	MX	1 day	0	mail.titan.net
nmap.org	NS	1 day		ns1.titan.net
nmap.org	NS	1 day		ns2.titan.net
nmap.org	SOA	1 day		ns1.titan.net. hostmaster.insecure.org. 2008091400 28800 3600 604800 86400
nmap.org	TXT	1 day		v=spf1 a mx ptr ip4:64.13.134.0/26 -all

RELATED DOMAINS	
titan.net	insecure.org
- Whois - Information - DNS Records	- Whois - Information - DNS Records

RYСУNEK 6.16.

Informacje whois dotyczące witryny internetowej nmap.org

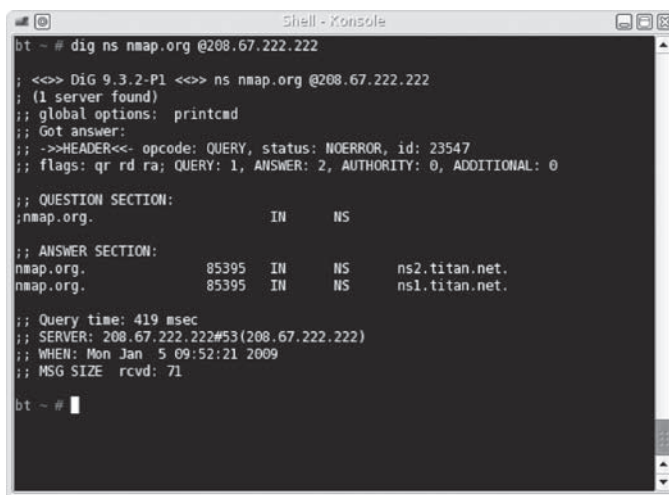
Wydaje się, że witryna nmap.org znajduje się w sieci o nazwie titan.net. Jeżeli pójdiesz za tą informacją, to odkryjesz, że titan.net jest powiązana z firmą DreamHost Web Hosting, co niewątpliwie wykracza poza nasz obszar zainteresowania, ponieważ próbujemy dowiedzieć się czegoś na temat narzędzia nmap i jego twórcy (bądź twórców). Jednak jeśli dalej będziemy prowadzić analizę, to dowiemy się nieco więcej na temat serwerów obsługujących witrynę (AMD Dual Core Opteron lub Intel Dual Processor Xeon), używanych systemów operacyjnych (Linux-VServer lub Debian Linux) oraz potencjalnych usług dostępnych dla użytkowników hostingu (między innymi MySQL,

² W Polsce informacje o firmie można sprawdzić w portalu Centralnej Ewidencji i Informacji o Działalności Gospodarczej (<https://prod.ceidg.gov.pl/ceidg.cms.engine/>) — przyp. tłum.

POP/IMAP, FTP). W ten sposób zdobędziemy większą wiedzę na temat serwerów, które mają być celem ataku. Kiedy przystąpimy do wykorzystywania luk w zabezpieczeniach systemów będących celem ataku, zdobyte teraz informacje pomogą w zawężeniu liczby potencjalnych luk w zabezpieczeniach, które mogą nas interesować.

Niektóre ze zdobytych teraz informacji będziemy wykorzystywać później, po przejściu do fazy aktywnego zbierania informacji. W ten sposób nie tylko dowiesz się, jak zbierać informacje z poziomu wiersza poleceń, ale również jak zweryfikować te, które zostały zgromadzone w fazie pasywnego zbierania informacji. Zawsze istnieje prawdopodobieństwo, że rekordy pokazane na rysunku 6.16 są nieaktualne (to kolejny powód, dla którego zawsze warto korzystać z dwóch różnych narzędzi do zbierania informacji).

Inny zestaw narzędzi zalecany przez dokument ISSAF do użycia na etapie zbierania informacji to dig i nslookup. Spójrzmy na te narzędzia i przekonajmy się, jak możemy je wykorzystać do naszych celów. Narzędzie dig pozwala na wykonywanie zapytań do serwera nazw w celu pobrania informacji o interesującym nas systemie. Wspomniane informacje mogą być pobierane z dowolnego dostępnego serwera DNS, a nie tylko z obsługującego sprawdzaną domenę. Na rysunku 6.17 pokazano wykonanie zapytania dla witryny nmap.org w celu pobrania informacji od obsługującego ją serwera. Użyty serwer nazw to 208.67.222.222 (resolver1.opendns.com), który jest serwerem dla OpenDNS, czyli firmy oferującej bezpłatną usługę DNS. Będzie to użyteczne, gdy nie jesteś pewien niezawodności działania Twojego dostawcy DNS lub jeśli chcesz po prostu mieć alternatywę.



```

bt ~ # dig ns nmap.org @208.67.222.222

; <<>> DiG 9.3.2-P1 <<>> ns nmap.org @208.67.222.222
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 23547
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;nmap.org.                IN      NS

;; ANSWER SECTION:
nmap.org.                 85395   IN      NS      ns2.titan.net.
nmap.org.                 85395   IN      NS      ns1.titan.net.

;; Query time: 419 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Mon Jan 5 09:52:21 2009
;; MSG SIZE rcvd: 71

bt ~ #

```

RYСУNEK 6.17.

Wynik wykonania zapytania za pomocą narzędzia dig

Zapiski z podziemia

OpenDNS.com

Nazwa może być nieco myląca — OpenDNS nie jest oprogramowaniem typu open source, lecz komercyjnym. Dostępne są usługi dodatkowe, o których powinieneś wiedzieć, zanim zaczniesz korzystać z bezpłatnej usługi oferowanej przez OpenDNS. Do wspomnianych usług dodatkowych należą filtry antyphishingowe, blokowanie domen i wyświetlanie odpowiedniego komunikatu podczas próby nawiązania połączenia za pomocą przeglądarki internetowej z nazwą nieistniejącej domeny. W zależności od wymagań OpenDNS może być cennym zasobem lub czymś, czego lepiej unikać.

Uzyskane przez nas informacje pokazują, że titan.net to faktycznie serwer nazw dla nmap.org. Skoro znamy serwer, możemy spróbować dowiedzieć się o nim czegoś więcej.

Kolejne narzędzie, którego użycie jest zalecane w dokumencie ISSAF, to nslookup. Użycie wymienionego narzędzia na obecnym etapie testu penetracyjnego jest bardzo uproszczone. Na rysunku 6.18 pokazano kilka poleceń wykorzystujących narzędzie nslookup zgodnie z sugestiami zamieszczonymi w dokumencie ISSAF. Jednak w wymienionym dokumencie nie ma zbyt wielu informacji dotyczących elastyczności narzędzia nslookup, a także pominięto informacje opcjonalne, które mogą być użyteczne podczas gromadzenia większej ilości danych z celu ataku. Jak wspomniano wcześniej, jest to ogólny problem związany z metodologią ISSAF — w dokumencie przedstawiono opcje narzędzi używanych w przykładach, ale nie omówiono innych możliwych scenariuszy. Niektóre inne opcje narzędzia nslookup zostaną przedstawione w dalszej części rozdziału, w fazie aktywnego zbierania informacji.

```

bt ~ # nslookup nmap.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
Name:   nmap.org
Address: 64.13.134.48

bt ~ # nslookup
> set q=ns
> nmap.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
nmap.org     nameserver = ns1.titan.net.
nmap.org     nameserver = ns2.titan.net.

Authoritative answers can be found from:
ns1.titan.net internet address = 64.13.134.58
ns2.titan.net internet address = 64.13.134.59
>

```

RYСУNEK 6.18.

Użycie narzędzia nslookup do zebrania informacji DNS zgodnie z sugestiami zawartymi w dokumencie ISSAF

W późniejszych przykładach wskażemy serwer DNS, z którym narzędzie nslookup ma się połączyć w celu zebrania informacji dodatkowych. Teraz po prostu skorzystamy z domyślnego serwera nazw zdefiniowanego dla analizowanej sieci. Czasami możliwość

wskazania serwera DNS jest bardzo ważna, ponieważ występuje pewne opóźnienie podczas wprowadzania zmian DNS. Bieżąca faza polega na pasywnym zbieraniu informacji, więc dane nieautorytatywne są wystarczające.

Ostrzeżenie

W pewnych przypadkach bezpośrednie wykonanie zapytania do serwera nazw spowoduje złamanie założonej pasywności. Jeżeli informacje mają być naprawdę zbierane w sposób pasywny, nawiązanie połączenia z nieautorytatywnymi serwerami nazw może być kiepskim pomysłem ze względu na to, kto jest właścicielem serwera.

Dodatkowe zasoby internetowe

Dodatkowy obszar warty sprawdzenia to aktywność w grupach dyskusyjnych. Na rysunku 6.19 można zobaczyć jeden z nowszych postów zamieszczonych na grupie dyskusyjnej poświęconej narzędziu nmap. Grupę dyskusyjną można przeszukać pod kątem nazwy nmap lub adresu URL <http://insecure.org/>, aby przekonać się, co inni mają do powiedzenia na temat narzędzia nmap lub poświęconej mu witryny. Jeżeli przejrysz grupy dyskusyjne, z reguły znajdziesz użytkowników z całego świata zamieszczających posty dotyczące narzędzia nmap. Istnieje więc realna możliwość zebrania pewnych informacji zarówno o samym narzędziu, jak i o jego witrynie domowej. Pamiętaj, że konieczne jest zebranie wielu informacji, a prawdziwe perełki można czasem znaleźć nawet w obskurnych miejskach.

Search results for nmap

match

sort by in order

show ☒ posting ☒ total ☐ new ☐ speed ☐ retention

for ☐ inactive ☒ normal ☐ commercial ☐ posting servers

Displaying matches: 1-4

SERVER	POSTING	LAST CHECKED	GROUP	ARTICLES
textnews.news.cambrium.nl	No	2009-01-07	alt.fr.outil.nmap	22
			gmane.comp.security.nmap.devel	3
ger.gmane.org	Yes	2009-01-07	gmane.comp.security.nmap.devel	9103
			gmane.comp.security.nmap.general	157

RYСУNEK 6.19.

Grupa dyskusyjna przeszukana pod kątem nazwy narzędzia nmap — przykład pochodzi z witryny <http://freenews.maxbaud.net/>

Dokument ISSAF sugeruje także przeanalizowanie celu, aby ustalić, czy znajduje się na liście wymieniającej spam. Jeżeli cel ataku został wymieniony w bazie danych spamu, a nie powinien się w niej znajdować, może to wskazywać na włamanie do serwera poczty w przeszłości. Zgodnie z wynikami pokazanymi na rysunku 6.20 witryna insecure.org nie została dodana do bazy danych spamu, którą można przeglądać pod adresem: <http://www.dnsbl.info/>.

Spam Database Lookup Results for 64.13.134.2

The following are blacklist test results. Being listed with a DNSBL does not always indicate the IP address is a source of spam. Some DNSBL's criteria are based of the IP address' country or connection type. If you are listed with a DNSBL click on the link for removal criteria.

If you are listed with a DNSBL we cannot remove you. We can only try to help diagnose the problem and direct you to where you may be able to be delisted (by visiting the DNSBL's website directly.)

 asiaspam.spamblocked.com	 b.barracudacentral.org	 bl.deadbeef.com
 bl.emailbasura.org	 bl.spamcannibal.org	 bl.spamcop.net
 blackholes.five-ten-sg.com	 blacklist.woody.ch	 bogons.cymru.com
 cbl.abuseat.org	 cdl.anti-spam.org.cn	 combined.abuse.ch
 combined.rbl.msrbl.net	 db.wpbl.info	 dnsbl-1.uceprotect.net
 dnsbl-2.uceprotect.net	 dnsbl-3.uceprotect.net	 dnsbl.ahbl.org
 dnsbl.cyberlogic.net	 dnsbl.inps.de	 dnsbl.njabl.org
 dnsbl.sorbs.net	 drone.abuse.ch	 drone.abuse.ch
 dulinv.aupads.org	 dul.dnsbl.sorbs.net	 dul.ru

RYSUNEK 6.20.

Sprawdzenie, czy dana witryna została umieszczona w bazie danych spamu

Warto również przejrzeć informacje o poszukiwanych pracownikach, co często dostarcza wiadomości dotyczących sprzętu i oprogramowania używanego przez daną firmę. Poniżej przedstawiono fragment ogłoszenia, w którym firma Google szuka inżyniera (zob. odwołanie na końcu rozdziału).

Wymagania:

- licencjat z informatyki lub podobne doświadczenie;
- doświadczenie w pracy z MySQL (mile widziane doświadczenie w administracji i/lub w dostosowywaniu wydajności MySQL), a także znajomość przynajmniej dwóch z wymienionych języków: Python, Perl, SQL, powłoka;
- podstawowe umiejętności w zakresie rozwiązywania problemów w systemach operacyjnych Linux oraz związanych z siecią;
- doświadczenie w opracowywaniu i/lub obsłudze systemu ETL;
- dodatkowym atutem będzie doświadczenie w zarządzaniu ogromnym systemem z wieloma komponentami;
- kolejnym atutem będzie doświadczenie w zakresie analizy dzienników zdarzeń oraz danych.

Na podstawie powyższych wymagań dowiedzieliśmy się, że firma Google używa gdzieś systemu Linux, bazy danych MySQL oraz programów utworzonych w językach Python i Perl. Ponadto w Google'u istnieje przynajmniej jedna baza danych używająca architektury ETL. Tego rodzaju informacje będą niewątpliwie użyteczne, ponieważ pozwalają na zmniejszenie wysiłku ponoszonego w trakcie projektu, a także na dokładniejsze zdefiniowanie wymagań względem członków zespołu realizującego dany projekt.

AKTYWNE ZBIERANIE INFORMACJI

Na tym etapie testu penetracyjnego można się już mniej przejmować interakcją z siecią będącą celem ataku. Powód jest prosty: zdołaliśmy zebrać sporą ilość informacji dotyczących celu ataku, a tym samym nie ma konieczności dalszego zbierania informacji na dużą skalę. Aktywne zbieranie informacji skutkuje wynikami podobnymi do uzyskanych za pomocą technik zbierania pasywnego. Zalety zastosowania pasywnego zbierania informacji podczas testu penetracyjnego są dwie: identyfikacja informacji historycznych oraz potwierdzenie odkryć w wyniku użycia metod aktywnych.

Dodatkowa umiejętność pozwalająca na zdobycie jeszcze innych informacji to socjotechnika, ale ten temat nie zostanie omówiony w książce. Ujmując rzecz najprościej: socjotechnika oznacza uzyskanie użytecznych (i często nieautoryzowanych) informacji od pojedynczych osób związanych z celem ataku. Socjotechnika to niezwykle efektywna metoda zbierania informacji dotyczących celu — najczęściej znacznie efektywniejsza niż przeprowadzenie skanowania lub podjęcie próby wykorzystania luk w zabezpieczeniach. W tej książce nie będziemy się zajmować użyciem socjotechniki, ponieważ temu tematowi zostało poświęconych wiele innych pozycji wydanych przez Syngress. We wspomnianych pozycjach socjotechnikę omówiono znacznie lepiej, niż mógłbym to zrobić tutaj (ze względu na brak wystarczającej ilości miejsca). Ogólnie rzecz biorąc: korzystaj z dostępnych narzędzi i technik pozwalających na zebranie informacji wymaganych do przeprowadzenia testu penetracyjnego w uzgodnionym zakresie.

Zapytania DNS

Jednym z rodzajów użytecznych informacji jest poznanie wersji serwera BIND (ang. *Berkeley Internet Name Domain*) działającego w naszym celu ataku. Kierując się poleceniami sugerowanymi w dokumencie ISSAF i pokazanymi na rysunku 6.21, odkrywamy, że wersja serwera to 9.3.4. Po przeszukaniu zasobów internetu dowiadujemy się, że wymieniona wersja została wydana w styczniu 2007 roku i nie jest najnowszą wersją serwera. Tych informacji możemy użyć na dalszym etapie testu penetracyjnego w celu sprawdzenia istnienia znanych luk w zabezpieczeniach, które można by wykorzystać. Teraz jedynie zapisujemy odkryte informacje i przechodzimy dalej.

Dokument ISSAF proponuje wydanie jeszcze kilku innych poleceń dig pozwalających na zebranie informacji o serwerach poczty. Jednak tego rodzaju informacje zebraliśmy już wcześniej, o czym możesz się przekonać, ponownie spoglądając na rysunek 6.16. Bardzo ważne jest używanie dwóch różnych narzędzi do tego samego celu i tym samym weryfikacja zbieranych informacji. Zawsze istnieje ryzyko, że witryny informacyjne, takie jak na przykład pokazana wcześniej na rysunku 6.16, zawierają nieaktualne wiadomości. Użycie wiersza poleceń zdecydowanie poprawia dokładność informacji — po prostu zachowaj ostrożność i dokładnie wybieraj systemy, z którymi się łączysz, zwłaszcza jeśli chcesz pozostać niewykryty.

```

bt ~ # dig @ns1.titan.net version.bind chaos txt

; <<>> DiG 9.3.2-P1 <<>> @ns1.titan.net version.bind chaos txt
; (1 server found)
; global options: printcmd
; Got answer:
; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 61387
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

; QUESTION SECTION:
;version.bind.                CH      TXT

; ANSWER SECTION:
version.bind.                0      CH      TXT      "9.3.4"

; AUTHORITY SECTION:
version.bind.                0      CH      NS       version.bind.

; Query time: 374 msec
; SERVER: 64.13.134.58#53(64.13.134.58)
; WHEN: Mon Jan 5 10:48:43 2009
; MSG SIZE rcvd: 62

bt ~ #

```

RYSUNEK 6.21.

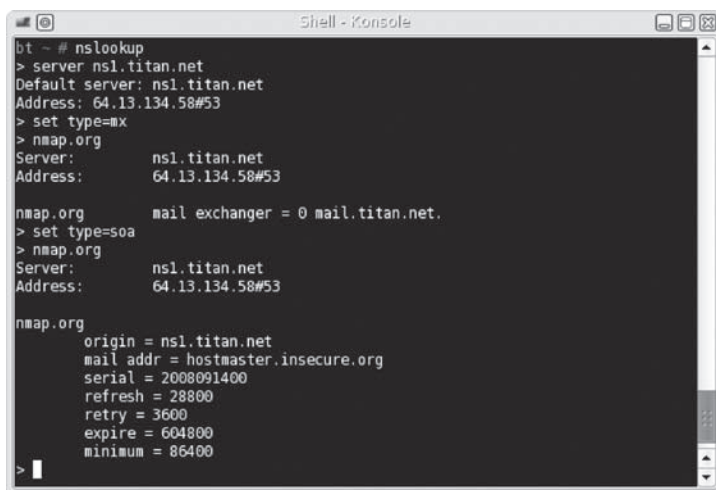
Wykonanie zapytania w celu ustalenia wersji serwera BIND

Wskazówka

Być może będziesz musiał zapytać klienta, czy koncepcja opóźnień w uaktualnieniach DNS jest problemem, zwłaszcza gdy podstawowym zmartwieniem pozostaje dostępność serwera. Jeżeli serwer nazw zostanie zaatakowany lub przejęty, wtedy propagacja DNS powinna nastąpić jak najszybciej. Niektóre firmy oferujące usługi hostingowe bardzo wolno uaktualniają rekordy DNS.

Zawsze istnieje ryzyko, że domyślny serwer DNS (lub jakikolwiek serwer DNS niepołączony bezpośrednio z serwerem docelowym) będzie miał nieaktualne dane. Dzięki bezpośredniej komunikacji z ns1.titan.net możemy zdobyć aktualne informacje. Ponadto wspomniana komunikacja dostarczy dodatkowych informacji o serwerze poczty, jak również o witrynie nmap.org. Na rysunku 6.22 pokazano dodatkowe polecenia nslookup pozwalające na rozszerzenie naszych poszukiwań. Jak widzisz, za pomocą narzędzia nslookup można zgromadzić znacznie więcej informacji, niż zasugerowano w dokumencie ISSAF.

Narzędzia wiersza poleceń i wykorzystujące je przykłady przedstawione w dokumencie ISSAF są niezwykle użyteczne, ale nie obejmują wszystkich możliwych zapytań. Moim kursantom zalecam nie tylko wykorzystanie narzędzi i wykonanie poleceń przedstawionych w dokumencie ISSAF, ale również poznanie funkcji oferowanych przez poszczególne aplikacje, co pozwoli im w przyszłości na jeszcze lepsze przeprowadzanie testów penetracyjnych.



```

bt ~ # nslookup
> server ns1.titan.net
Default server: ns1.titan.net
Address: 64.13.134.58#53
> set type=mx
> nmap.org
Server:      ns1.titan.net
Address:     64.13.134.58#53

nmap.org      mail exchanger = 0 mail.titan.net.
> set type=soa
> nmap.org
Server:      ns1.titan.net
Address:     64.13.134.58#53

nmap.org
origin = ns1.titan.net
mail addr = hostmaster.insecure.org
serial = 2008091400
refresh = 28800
retry = 3600
expire = 604800
minimum = 86400
>

```

RYСУNEK 6.22.

Wykonanie dodatkowych poleceń nslookup w celu zebrania informacji dotyczących DNS

Konta poczty elektronicznej

Jeżeli cel ataku ma serwer poczty (jak w omawianym przykładzie), wówczas można spróbować utworzyć listę użytkowników systemu. Wspomniana lista okaże się przydatna nie tylko podczas ataku typu brute force lub podczas logowania, ale również do celów powiązanych z socjotechniką. Według dokumentu ISSAF należy nawiązać bezpośrednie połączenie z serwerem poczty i wykonać zapytania, za każdym razem podając tę samą nazwę użytkownika. Takiej operacji nie możemy przeprowadzić względem serwera poczty nmap.org, ponieważ nie mamy zezwolenia na tego rodzaju działania. Wykorzystamy więc cel ataku umieszczony na stronie internetowej poświęconej książce. Naszym celem stanie się Hackerdemia LiveCD — ta dystrybucja została na to przygotowana, celowo zawiera włączone usługi, na które można przeprowadzać ataki. Jedną z usług jest serwer sendmail. Obraz dysku z dystrybucją Hackerdemia można pobrać ze strony: <http://hackingdojo.com/pentest-media/> (odpowiedniego łącza szukaj w sekcji *Virtual Images*). W rozdziale 3. znajdziesz informacje dotyczące konfiguracji laboratorium do użycia obrazu Hackerdemia lub innej dowolnej dystrybucji LiveCD z wymienionej strony.

Na rysunku 6.23 możesz zobaczyć atak na dystrybucję Hackerdemia LiveCD przeprowadzony za pomocą poleceń zaproponowanych w dokumencie ISSAF. Udało nam się zidentyfikować niektórych użytkowników serwera (root i david) oraz wykluczyć innych (anyone i michelle).

Tego rodzaju metoda wymaga wypróbowania różnych nazw użytkowników, po jednej w każdym zapytaniu, jeśli włączone są odpowiednie opcje zachowania prywatności, na przykład pokazane na rysunku 6.23 novrfy i noexpn. Sam proces może zająć dużo czasu, w zależności od liczby użytkowników serwera oraz stanu naszej wiedzy z zakresu konwencji nazw e-mail.


```

bt ~ # nc -vv 192.168.1.123 25
192.168.1.123: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [192.168.1.123] 25 (smtp) open
220 slax.example.net ESMTP Sendmail 8.13.7/8.13.7; Sun, 11 Jan 2009 13:45:27 GMT
EHLO heorot.net
250-slax.example.net Hello [192.168.1.10], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-AUTH DIGEST-MD5 CRAM-MD5
250-DELIVERBY
250 HELP
VRFY root
252 2.5.2 Cannot VRFY user; try RCPT to attempt delivery (or try finger)
EXPN root
502 5.7.0 Sorry, we do not allow this operation
MAIL FROM: twilhelm@slax.example.net
250 2.1.0 twilhelm@slax.example.net... Sender ok
RCPT TO: anyone@slax.example.net
550 5.1.1 anyone@slax.example.net... User unknown
RCPT TO: root@slax.example.net
250 2.1.5 root@slax.example.net... Recipient ok
RCPT TO: david@slax.example.net
250 2.1.5 david@slax.example.net... Recipient ok
RCPT TO: michelle@slax.example.net
550 5.1.1 michelle@slax.example.net... User unknown
sent 204, rcvd 661
bt ~ #

```

RYСУNEK 6.23.

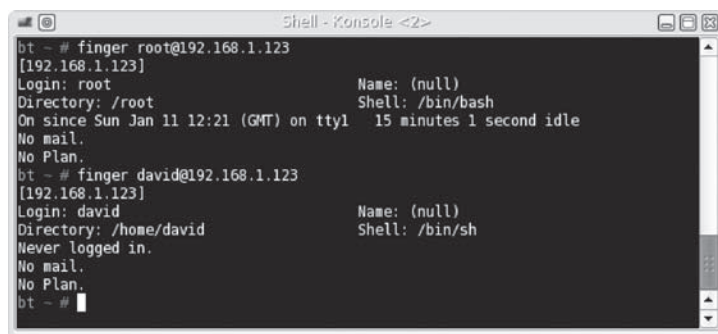
Wykonywanie zapytań do serwera poczty dystrybucji Hackerdemia LiveCD

Uwaga

Jeżeli chcesz wyłączyć pewne zabezpieczenia dotyczące prywatności i przekonać się, jaka będzie odpowiedź po nawiązaniu połączenia z serwerem sendmail dystrybucji Hackerdemia, wtedy po prostu przeprowadź edycję pliku `/etc/mail/sendmail.cf`. Modyfikacja powinna polegać na umieszczeniu komentarza na początku wiersza rozpoczynającego się od `PrivacyOptions`. Konieczne będzie również ponowne uruchomienie serwera sendmail przez wykonanie jako użytkownik root polecenia `/etc/rc.d/rc.sendmail restart`.

Na rysunku 6.23 widać sugestię użycia narzędzia finger względem naszego celu ataku. Zwykle trudno jest znaleźć w sieci komputer, w którym włączono możliwość użycia finger. Jednak ponieważ dystrybucja Hackerdemia została opracowana jako narzędzie szkoleniowe, włączono w niej możliwość użycia narzędzia finger. Na rysunku 6.24 pokazano, czego można się spodziewać po nawiązaniu połączenia z narzędziem finger w systemie.

Jak widzisz, narzędzie finger dostarcza znacznie więcej informacji, niż uzyskałbyś po nawiązaniu połączenia z klientem poczty. Warto w tym miejscu przypomnieć, że użycie finger rzadko będzie możliwe. Uważaj się za szczęśliwego, jeśli znajdziesz w internecie system udostępniający narzędzie finger. Upewnij się również o dezaktywacji tego narzędzia w używanym przez siebie systemie, jeśli nie masz naprawdę ważnego powodu, aby pozostawić je dostępne.



```

bt ~ # finger root@192.168.1.123
[192.168.1.123]
Login: root                                Name: (null)
Directory: /root                          Shell: /bin/bash
On since Sun Jan 11 12:21 (GMT) on tty1    15 minutes 1 second idle
No mail.
No Plan.

bt ~ # finger david@192.168.1.123
[192.168.1.123]
Login: david                                Name: (null)
Directory: /home/david                    Shell: /bin/sh
Never logged in.
No mail.
No Plan.

bt ~ #

```

RYСУNEK 6.24.

Użycie narzędzia finger względem dystrybucji Hackerdemia LiveCD

Identyfikacja granic sieci

W ogromnych organizacjach bardzo często można się natknąć na strefy zdemilitaryzowane (ang. *Demilitarized Zones* — DMZ) znajdujące się w zakresie będącym przedmiotem testu penetracyjnego. Ujmując rzecz najprościej: strefa zdemilitaryzowana to najczęściej sieci mające bezpośrednie połączenie z internetem i stanowiące bufor między internetem i wewnętrzną siecią korporacji. Powinieneś się dowiedzieć, czy możesz penetrować strefę zdemilitaryzowaną i włamać się do sieci korporacyjnej. Dla osoby przeprowadzającej test penetracyjny problemem jest ustalenie, gdzie rozpoczyna się sieć celu ataku, oraz określenie infrastruktury łączącej cel ataku z internetem.

Wprawdzie brzmi to sensownie, ale implementacja rozwiązania jest już znacznie trudniejsza. Trzeba zachować ostrożność podczas wybierania celu, aby nie zaatakować systemu, który nie należy do klienta. Przyjmuje się założenie, że klient dostarcza listę adresów IP wszystkich systemów pozostających pod jego kontrolą. Warto pamiętać, że zdarzają się pewne przeoczenia, na przykład do sieci dodano nowe komputery, ale zapomniano uaktualnić rekordy. Jeżeli znajdziesz tego rodzaju „przeoczone” systemy, istnieje możliwość, że przeoczono je również podczas uaktualnień oprogramowania, co może ułatwić wykorzystanie luk w zabezpieczeniach sieci.

Na rysunku 6.25 pokazano wynik użycia narzędzia traceroute w sieci docelowej, czyli należącej do firmy Insecure.com. Zwróć uwagę na kilka różnych nazw domen, które warto sprawdzić: us.above.net i sv.svcolo.com. Z kolei na rysunkach 6.26 i 6.27 pokazano informacje whois dla domen above.net i svcolo.com. Od razu widać, że wymienione systemy należą do innych osób niż właściciel insecure.org. Jeżeli przeprowadzimy dalsze czynności sprawdzające, wtedy przekonamy się, że above.net zapewnia połączenie z internetem, natomiast svcolo.com — usługi w zakresie obsługiwanego centrum danych.

64.13.134.49 is from United States(US) in region North America

TraceRoute to 64.13.134.49 [insecure.org]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	16	28	14	72.249.0.65	-
2	7	6	6	209.249.122.73	209.249.122.73.available.above.net
3	18	11	8	64.125.26.213	ge-2-0-0.mpr2.dfw2.us.above.net
4	11	14	17	64.125.26.134	so-1-1-0.mpr4.iah1.us.above.net
5	46	50	43	64.125.25.18	so-1-1-0.mpr4.lax9.us.above.net
6	53	53	61	64.125.26.30	so-0-1-0.mpr2.sjc2.us.above.net
7	57	53	58	64.125.31.69	xe-0-1-0.mpr2.pao1.us.above.net
8	76	56	89	208.185.168.173	metro0.sv.svcolo.com
9	62	58	53	64.13.134.49	insecure.org

Trace complete

RYСУNEK 6.25.

Wynik uruchomienia narzędzia traceroute dla sieci insecure.org

```

Administrative Contact:
AboveNet Communications, Inc.                dns@ABOVE.NET
50 W SAN FERNANDO ST STE 1010
SAN JOSE, CA 95113-2414
US
408-367-6666 fax: 408-367-6688

Technical Contact:
AboveNet Communications, Inc.                dns@ABOVE.NET
AboveNet Communications, Inc.
50 W SAN FERNANDO ST STE 1010
SAN JOSE, CA 95113-2414
US
408-367-6673 fax: 408-367-6688

Record expires on 10-Jun-2014.
Record created on 09-Jun-1996.
Database last updated on 12-Jan-2009 14:59:11 EST.

Domain servers in listed order:
NS.ABOVE.NET                207.126.96.162
NS3.ABOVE.NET               207.126.105.146
  
```

RYСУNEK 6.26.

Informacje whois dla domeny above.net

Zajmijmy się teraz znacznie bardziej interesującym aspektem, dzięki któremu jeszcze lepiej zrozumiemy, na co można się natknąć podczas identyfikacji granic sieci. Na rysunku 6.28 pokazano wynik uruchomienia narzędzia traceroute dla google.com. Po przesko-
ku 6 nie widzimy żadnych informacji dotyczących właściciela serwera, co wymaga prze-
prowadzenia dalszej analizy. Jeżeli wykonamy polecenie whois dla adresu IP 66.249.94.94
(jak pokazano na rysunku 6.29), wtedy dowiemy się, że właścicielem sprawdzanego
systemu jest google.com. Na tym etapie możemy określić 66.249.94.94 jako granicę sieci
i rozpocząć atak na ten system, pod warunkiem że mamy odpowiednie uprawnienia.
(Skoro to jedynie przykład pokazujący sposób określania granic sieci, nie przeprowa-
dzamy ataku na podany system).

```

Domain name: SVCOLO.COM

Administrative Contact:
  Gianniandrea, John  hostmaster@svcolo.com
  P.O. Box 390804
  Mountain View, CA 94039
  US
  +1.4084000550
Technical Contact:
  hostmaster, meer.net  hostmaster@meer.net
  P.O. Box 390804
  Mountain View, CA 94039
  US
  +1.8888446337    Fax: +1.6506181482

Registration Service Provider:
  Meer.net LLC, support@meer.net
  888-844-6337
  650-618-1482 (fax)
  http://www.meer.net/
  P.O. Box 390804
  Mountain View, CA 94039
  USA

```

RYSUNEK 6.27.

Informacje whois dla domeny svcolo.com

74.125.45.100 is from United States(US) in region North America

TraceRoute to 74.125.45.100 [google.com]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	36	39	19	72.249.0.65	-
2	9	12	11	206.123.64.22	-
3	57	102	11	216.52.189.9	border4.te4-4.colo4dallas-4.ext1.dal.pnap.net
4	16	44	34	216.52.191.34	core3.tge5-1-bbnet1.ext1.dal.pnap.net
5	13	14	25	207.88.185.73	207.88.185.73.ptr.us.xo.net
6	43	51	57	207.88.185.130	207.88.185.130.ptr.us.xo.net
7	50	47	43	66.249.94.94	-
8	31	29	29	72.14.238.243	-
9	82	34	79	209.85.253.173	-
10	62	37	36	209.85.253.145	-
11	66	31	29	74.125.45.100	yx-in-f100.google.com

Trace complete

RYSUNEK 6.28.

Wynik uruchomienia narzędzia traceroute dla google.com

```

bt ~ # whois 66.249.94.94

OrgName:   Google Inc.
OrgID:     GOOL
Address:    1600 Amphitheatre Parkway
City:      Mountain View
StateProv:  CA
PostalCode: 94043
Country:    US

NetRange:   66.249.64.0 - 66.249.95.255
CIDR:       66.249.64.0/19
NetName:    GOOGLE
NetHandle:  NET-66-249-64-0-1
Parent:     NET-66-0-0-0-0
NetType:    Direct Allocation
NameServer: NS1.GOOGLE.COM
NameServer: NS2.GOOGLE.COM
NameServer: NS3.GOOGLE.COM

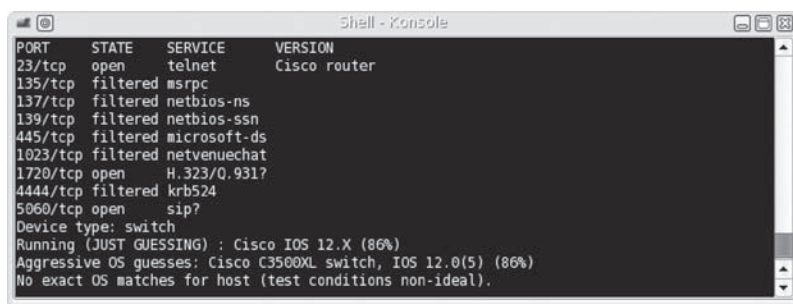
```

RYSUNEK 6.29.

Informacje whois dla adresu IP 66.249.94.94

Istnieje prawdopodobieństwo, że urządzenie podane w przeskoku 7 jest routerem. Można to sprawdzić, przeprowadzając operację skanowania portów (w omawianym przykładzie jednak tego nie zrobimy). Znacznie bardziej interesująca jest liczba różnych sieci, które przeskanujemy, zanim dotrzemy do sieci docelowej — 74.125.45.100. Jeżeli wykonamy polecenia whois dla pozostałych adresów IP, wtedy dowiemy się, że ich właścicielem również jest Google. Powstaje więc pytanie: co się dzieje między przeskokami 7 i 11, które pokazano na rysunku 6.28? Na tym etapie pozorowanego testu penetracyjnego nie musimy przeprowadzać żadnych dokładniejszych operacji sprawdzających, choć naprawdę nie zaszkodzi dowiedzieć się, co można w tej sytuacji zrobić. W tym celu przeprowadzimy kilka prostych operacji skanowania, aby dowiedzieć się nieco więcej na temat wspomnianych urządzeń.

Wprawdzie nadal nie będziemy skanować żadnych elementów sieciowych firmy Google (nie mamy zezwolenia na takie działania), ale chciałbym Ci pokazać, jak może wyglądać wynik operacji skanowania sieci. Na rysunku 6.30 pokazano wynik skanowania portów routera Cisco. Na dalszym etapie testu penetracyjnego tego rodzaju informacje będą szczególnie użyteczne do identyfikacji protokołów (i prawdopodobnie systemów operacyjnych) używanych w sieci, co z kolei pomoże w sprawdzeniu ich podatności na atak. Jednak teraz tego rodzaju informacje wykorzystamy do sprawdzenia, czy połączenie nawiązano z przełącznikiem sieciowym, routerem, równoważnikiem obciążenia, przekątnikiem, czy może zaporą sieciową. Taka wiedza pozwala czasami na lepszą identyfikację granic sieci.



```
Shell - Konsole
PORT      STATE SERVICE      VERSION
23/tcp    open  telnet       Cisco router
135/tcp   filtered msrpc
137/tcp   filtered netbios-ns
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1023/tcp  filtered netvenuechat
1720/tcp  open  H.323/0.931?
4444/tcp  filtered krb524
5060/tcp  open  sip?
Device type: switch
Running (JUST GUESSING) : Cisco IOS 12.X (86%)
Aggressive OS guesses: Cisco C3500XL switch, IOS 12.0(5) (86%)
No exact OS matches for host (test conditions non-ideal).
```

RYСУNEK 6.30.

Przeprowadzone w laboratorium skanowanie sieci za pomocą narzędzia nmap

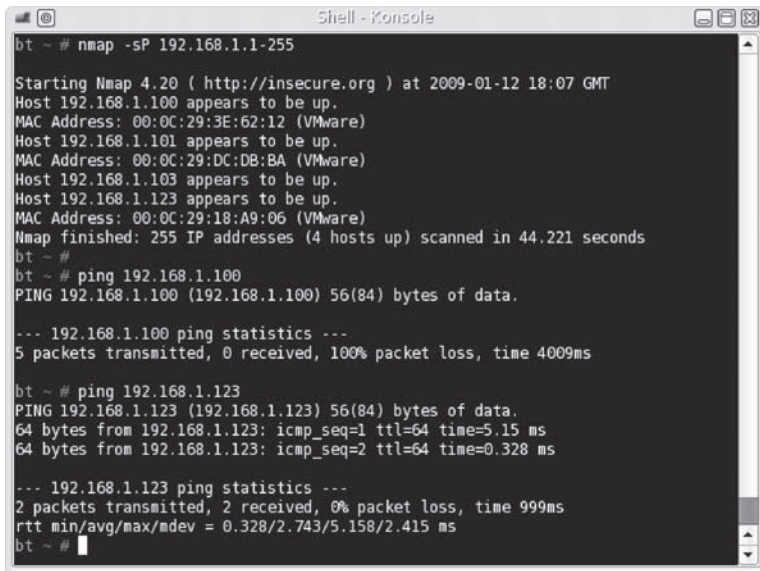
W celu identyfikacji granic sieci nie trzeba zbyt wiele robić, ale jest to krok o znaczeniu krytycznym w każdym teście penetracyjnym. Podstawowym celem tego kroku jest upewnienie się, że nie będą atakowane żadne urządzenia lub systemy, na atakowanie których nie mamy zezwolenia. Jeżeli umowa z klientem zawiera wymienione konkretne adresy IP, wówczas zadanie jest łatwiejsze, ponieważ działania można prowadzić tylko względem wymienionych adresów. Jednak jeśli zadanie polega na przeprowadzeniu testu penetracyjnego sieci, wtedy trzeba w pełni zdawać sobie sprawę, które systemy znajdują się w sieci, a które są poza zasięgiem testu penetracyjnego.

Warto również pamiętać, że systemy mogą blokować komunikaty ICMP (ang. *Internet Control Message Protocol*), aby utrudnić ich wykrycie. Inne metody wykrywania systemów zostaną omówione w rozdziale 7.

Sprawdzanie sieci

Po określeniu granic atakowanej sieci kolejnym krokiem jest identyfikacja wszystkich znajdujących się w niej urządzeń. Na tym etapie nie próbujemy ustalić rodzaju poszczególnych urządzeń (routerów, przełączników sieciowych, zapór sieciowych, serwerów i tak dalej), a jedynie określić liczbę urządzeń znajdujących się w sieci oraz powiązane z nimi adresy IP. Później przeprowadzimy skanowanie wszystkich urządzeń w celu zebrania informacji dodatkowych. Teraz wystarczy po prostu przygotować listę urządzeń sieci, aby dopracować i dostosować harmonogram działań w projekcie, jeśli zajdzie potrzeba.

Wystarczające będzie przeprowadzenie prostej operacji skanowania. Na rysunku 6.31 pokazano wynik użycia narzędzia nmap do przeskanowania jednego z laboratorium. Skaner wykrył obecność w sieci czterech komputerów, w tym także systemu przeprowadzającego skanowanie. Warto pamiętać, aby do skanowania sieci będącej celem ataku użyć co najmniej dwóch różnych narzędzi. Zdarza się, że pewne systemy nie odpowiadają na działania skanera, co jest skutkiem zastosowania mechanizmów bezpieczeństwa w takim systemie. Aby przekonać się, jak to działa, na rysunku 6.31 pokazano również wynik wydania polecenia ping względem dwóch systemów (o adresach IP 192.168.1.100 i 192.168.1.123.) zidentyfikowanych podczas skanowania za pomocą nmap.



```

bt ~ # nmap -sP 192.168.1.1-255

Starting Nmap 4.20 ( http://insecure.org ) at 2009-01-12 18:07 GMT
Host 192.168.1.100 appears to be up.
MAC Address: 00:0C:29:3E:62:12 (VMware)
Host 192.168.1.101 appears to be up.
MAC Address: 00:0C:29:DC:DB:BA (VMware)
Host 192.168.1.103 appears to be up.
Host 192.168.1.123 appears to be up.
MAC Address: 00:0C:29:18:A9:06 (VMware)
Nmap finished: 255 IP addresses (4 hosts up) scanned in 44.221 seconds
bt ~ #
bt ~ # ping 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.

--- 192.168.1.100 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4009ms

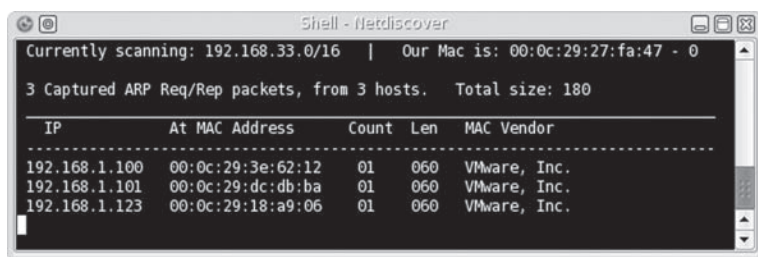
bt ~ # ping 192.168.1.123
PING 192.168.1.123 (192.168.1.123) 56(84) bytes of data.
64 bytes from 192.168.1.123: icmp_seq=1 ttl=64 time=5.15 ms
64 bytes from 192.168.1.123: icmp_seq=2 ttl=64 time=0.328 ms

--- 192.168.1.123 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.328/2.743/5.158/2.415 ms
bt ~ #
  
```

RYСУNEK 6.31.

Skanowanie sieci w laboratorium za pomocą narzędzia nmap

Jeżeli przeprowadzone zostanie jedynie sprawdzenie zakresu adresów IP za pomocą polecenia ping, pominięte będzie co najmniej jedno urządzenie w sieci. Po raz kolejny przekonujemy się, dlaczego do wykonania danego kroku lub zadania warto używać wielu różnych narzędzi. (Czytelnicy, którzy brali udział w prowadzonych przeze mnie szkoleniach, zapewne doskonale pamiętają powtarzaną mantrę: „Zawsze bądź cyniczny — zawsze używaj więcej niż tylko jednego narzędzia do wykonania danego zadania”). To naprawdę może zmienić przebieg Twojej kariery na polu przeprowadzania testów penetracyjnych). Nigdy nie możesz przewidzieć, jaka będzie reakcja systemu, gdy używasz jedynie ulubionego narzędzia. Podążając za przedstawioną powyżej radą, do sprawdzenia urządzeń w sieci wykorzystamy także narzędzie netdiscover, jak pokazano na rysunku 6.32. Wymienione narzędzie nasłuchuje ruchu ARP (ang. *Address Resolution Protocol*) w sieci i przechwytuje wszystko, co tylko może przechwycić.



IP	At MAC Address	Count	Len	MAC Vendor
192.168.1.100	00:0c:29:3e:62:12	01	060	VMware, Inc.
192.168.1.101	00:0c:29:dc:db:ba	01	060	VMware, Inc.
192.168.1.123	00:0c:29:18:a9:06	01	060	VMware, Inc.

RYСУNEK 6.32.

Wyniki skanowania za pomocą narzędzia netdiscover

Podobnie jak w przypadku większości narzędzi, także netdiscover ma pewne ograniczenia. Ze względu na to, że żądania ARP nie wychodzą poza router, narzędzie może wykryć jedynie systemy znajdujące się w tej samej podsieci, w której jest system przeprowadzający skanowanie. Ponadto wykryte mogą być tylko systemy aktywnie rozgłaszające swoją obecność lub wysyłające dane. Jednak w przypadku sieci znajdującej się w naszym laboratorium narzędzie netdiscover sprawdza się doskonale. Zidentyfikowane zostały wszystkie działające systemy, a odkrycia pokrywają się z wynikami skanowania przeprowadzonego za pomocą narzędzia nmap.

To jedynie niewielki fragment operacji, jaką jest skanowanie sieci. W dalszej części testu penetracyjnego dowiesz się znacznie więcej o systemach znajdujących się w sieci. Przedstawiony tutaj krok miał za zadanie jedynie przeprowadzenie prostej operacji wykrycia urządzeń znajdujących się w sieci jako fragmentu fazy zbierania informacji. Na tym etapie naszym celem nie jest zebranie wszelkich danych dotyczących urządzeń w sieci, aby sprawdzić, czy są podatne na ataki — tym zajmiemy się w rozdziałach 7. i 8.

PODSUMOWANIE

Ten pierwszy krok w profesjonalnym teście penetracyjnym wymaga dużego wysiłku. Niestety, często jest niedoceniany lub wykonywany bardzo pobieżnie. Po części wynika to z faktu, że kolejne kroki testu penetracyjnego (na przykład wykorzystywanie luk w zabezpieczeniach) są często uznawane za znacznie bardziej ekscytujące. Bywa więc, że faza zbierania informacji jest przeprowadzana szybko i niechlujnie, aby osoba przeprowadzająca test penetracyjny mogła jak najszybciej zająć się „ciekawszymi działaniami”. Wprawdzie omówiona w tym rozdziale faza jest prawdopodobnie znacznie nudniejsza niż kolejne kroki testu penetracyjnego, ale jednocześnie może okazać się najcenniejsza w każdym projekcie, zarówno dla inżynierów, jak i menedżerów projektu. Stwierdzam to na podstawie własnego doświadczenia, jako osoba od wielu lat zajmująca się przeprowadzaniem profesjonalnych testów penetracyjnych.

Jeżeli faza zbierania informacji zostanie przeprowadzona prawidłowo, może zaoszczędzić ogromną ilość czasu w trakcie całego cyklu życiowego projektu. Ujmując rzecz najprościej: im więcej pracy wykonasz w fazie zbierania informacji, tym efektywniej i trafniej przeprowadzisz projekt testu penetracyjnego. Dokładne omówienie systemów, z jakimi przyjdzie Ci się zmierzyć, niewątpliwie pomoże w odrzuceniu nieefektywnych rozwiązań w zakresie wykorzystania luk w zabezpieczeniach. Ponadto zmniejszy ilość dokumentacji koniecznej do przeczytania, aby lepiej poznać aplikację lub protokół atakowany na dalszym etapie testu penetracyjnego.

Przedstawiłem tutaj różne sposoby zbierania informacji o celu ataku, zarówno w sposób pasywny, jak i aktywny. W trakcie analizy wymieniałem wiele witryn internetowych. Po lekturze tego rozdziału powinieneś zapamiętać nie nazwy witryn, które musisz odwiedzić, ale rodzaje informacji, jakie można znaleźć w internecie bez nawiązywania bezpośredniego połączenia z siecią będącą celem ataku. Dzięki wykorzystaniu publicznie dostępnych zasobów można przygotować obraz celu bez wysłania choćby jednego pakietu do sieci będącej celem ataku.

Pamiętaj, że wspomniane w rozdziale rodzaje informacji można zebrać bez nawiązywania połączenia z atakowaną siecią. Najważniejsze jednak jest to, że zgromadzone informacje — nawet jeśli pochodzą z publicznie dostępnych witryn internetowych — nie są własnością publiczną. Zachowaj szczególną ostrożność podczas pracy ze wszystkimi danymi klienta, nawet informacjami znalezionymi w internecie.

ODWOŁANIA

Google Inc. 2009. Production Engineer — Mountain View.

Skorowidz

(ISC)2, 28, 403

A

administracja systemem, 398
adres
 IP, 72
 MAC, 223, 338
AES, Advanced Encryption
 Standard, 387
agent CORE Impact, 263
aktywne zbieranie informacji,
 195
algorytm AES, 387
analiza
 archiwum, 188
 danych, 91
 ilościowa, 113
 jakościowa, 114
 malware, 87, 160, 161
 mieszana, 115
 subdomen, 187
 witryn, 181, 184
 złośliwego
 oprogramowania, 85, 158
aplikacja, 84, 399
 Java Bro Fuzzer, 242
 WebGoat, 64
 Webmin, 228
aplikacje
 sieciowe, 363
 typu open source, 65
architektura sieci, 83, 396
archiwizacja danych, 149
 kontrola dostępu, 153
 kwestie prawne, 150
 metody, 153
 miejsce przechowywania, 154
niszczenie danych, 156
ochrona dokumentacji, 152
odkrycia, 152
poczta elektroniczna, 151
zgromadzonych w
 laboratorium, 157
ARP, Address Resolution
 Protocol, 204, 298
ASME, 135
atak
 brute force, 235, 238
 DoS, 40
 metodą powtórzenia, 354
 MITM, 298
 na aplikacje sieciowe, 351
 na bazę danych, 321
 na BIOS, 164
 na hasło, 287, 291, 327
 lokalny, 292
 zdalny, 288
 na protokoły sieciowe, 335
 na standard WPA, 337
 na systemy, 335
 na użytkownika, 332
 na WEP, 342
 słownikowy, 292, 294
 SQL Injection, 352, 353
 typu brute force, 65
 typu phishing, 305
 XSS, 356
 zatrucia ARP, 299, 301
 zewnętrzny, 335
ataki w systemie lokalnym, 259
audyt, 52
automatyczne pobieranie
 obrazów, 183

B

BackTrack, 25
baza danych wiedzy, 168, 170
bazy danych, 399
bezpieczeństwo
 aplikacji, 102
 baz danych, 102
 dysków, 77
 fizyczne, 106
 komputerów, 101
 mobilne, 78
 sieci, 100
bezpieczna
 koperta, 385, 389
 powłoka, 225
 przysłań, 42
BGP, Border Gateway
 Protocol, 303
blokowanie domen, 192
błąd 401, 362
BSSID, Basic Service Set
 Identifier, 338
bufor ARP, 223

C

CEH, Certified Ethical Hacker,
 34
cel ataku, 57, 60, 92, 209
certyfikat, 34, 384, 400, 402
 CAP, 405
 CCIE Security, 417
 CCNA Security, 416
 CCNP Security, 416
 CISA, 410
 CISM, 410
 CISSP, 28, 34, 406

certyfi­kat

CISSP-ISSMP, 408
CompTIA, 413
CSSLP, 406
GIAC, 411
GISF, 417, 418
GLSC, 412
GPEN, 418
GSE, 412
GSEC, 418
ISSAP, 407
ISSEP, 408
JNCIA-Junos, 420
PMP, 413
SCSECA, 420
Security+, 413
SSCP, 405

certyfikowanie dokumentu, 382
CROSS-SITE SCRIPTING, 354
CTF, Capture the Flag, 93
cyberprzestępczość, 150
cyberwojna, 41
cykl życiowy projektu, 118
członkowie zespołu projektu, 129
czysty system, 158, 161
czyszczenie laboratorium, 156

D

dane

dzienników zdarzeń, 306
klienta, 74
korporacyjne, 187
uwierzytelniające, 360
uwierzytelniające
szyfrowane, 360
wrażliwe, 265

De-ICE, 63
demon sshd, 281
DHCP, Dynamic Host
Configuration Protocol, 303
DMCA, Digital Millennium
Copyright Act, 30
DNS, 190, 195, 196
dokument ISSAF, 97, 176, 185
bezpieczeństwo aplikacji, 102

bezpieczeństwo

baz danych, 102
bezpieczeństwo
komputerów, 101
bezpieczeństwo sieci, 100
planowanie, 98
rekonesans, 99
socjotechnika, 102
tworzenie raportów, 103
usuwanie artefaktów, 104
dokumentacja, 153, 381
dokumentowanie odkryć, 368
dokumenty osobiste, 436
dokumenty RFC, 37
DoS, Denial of Service, 40, 224
dostęp
do bazy danych, 325
do danych klienta, 74
do katalogów, 315
do konta, 287
do systemu, 183
na poziomie powłoki, 330
dowiązanie do zdalnego
udziału, 247

dyrektywa

2013/40/UE, 44
95/46/EC, 42

dystrybucja

BackTrack, 69, 72
De-ICE, 63, 82
Hackerdemia, 64
LiveCD, 62

działalność charytatywna, 431
dzienniki zdarzeń aplikacji, 311

E

etap

planowania, 140, 147
realizacji, 141, 148
rozpoczęcia, 138, 147
zakończenia, 144, 148

etyka, 28

F

falszowanie

adresu IP, 42
DHCP, 303
odpowiedzi, 303

filtry antyphishingowe, 192

firma

Check Point, 419
Cisco Systems, 416
Juniper Networks, 419
Oracle, 420

formalny przegląd projektu, 144

formularz, 185

framework, 97, 176

Metasploit, 242, 256
strukturalny, 129

FTP, 243

fundacja OWASP, 64

funkcja MD5, 76

funkcje haszujące, 75

fuzzing, 240

G

generowanie raportu, 375

Google Earth, 188

gromadzenie danych, 181

grupa procesów

monitorowania i kontroli, 127
planowania, 121
realizacji, 124
rozpoczęcia, 119
zakończenia, 126

grupy dyskusyjne, 428

H

Hackerdemia, 64

hacking, 27, 57, 58

hakerzy

negatywni, Black Hackers,
27, 29
neutralni, 33
pozytywni, White Hackers,
27, 32

hash, 75, 164

I

IAB, 37
 ICMP, Internet Control Message Protocol, 208, 303
 idea dowodu koncepcji, 157
 identyfikacja
 granic sieci, 199
 luk w zabezpieczeniach, 227, 359
 priorytetu przyszłych projektów, 145
 systemu operacyjnego, 220, 225
 usług, 224
 identyfikator sesji menedżera, 355
 IDS, Intrusion Detection System, 60, 81
 IEEE, 37
 informacje
 dotyczące
 certyfikatów, 435
 stanowiska, 434
 wynagrodzenia, 433
 o certyfikatach, 401
 o firmie, 188, 189
 o systemie, 268
 o tabelach, 327
 o witrynie, 184
 whois, 190, 199–201
 instrukcje NOP, 366
 instytucje, 36
 interfejsy sieciowe, 72
 inżynieria
 mechaniczna, 135
 odwrotna, 145, 157
 inżynierowie testu
 penetracyjnego, 132, 397
 IPS, Intrusion Prevention System, 60, 81
 iptables, 278
 ISSA, 36

J

Johansen Jon, 33

K

kanal, 106
 kariera, 393
 kierowanie testem penetracyjnym, 117
 klient SSH, 282
 klucz, 279
 WEP, 344
 WPA, 342
 kod
 proof-of-concept, 94
 reguły, 297
 wykorzystujący luki, 254, 265
 kodeks etyczny, 28
 komunikacja bezprzewodowa, 107
 konferencje, 422–427
 konfiguracja
 agenta lokalnego, 262
 interfejsu sieciowego, 73
 iptables, 278
 kluczy, 279
 komputera, 68
 laboratorium wirtualnego, 68, 74
 ładunku, 361
 Metasploitable, 238
 powłoki odwrotnej SSH, 279
 routera, 67, 82
 sieciowa, 89
 sprzętowa, 81
 konkurs CTF, 93
 konsorcjum (ISC)2, 34
 konta poczty elektronicznej, 197
 kopie zapasowe, 77, 161
 kradzież haseł, 42

L

laboratoria zaawansowane, 79
 laboratorium, 19, 57, 156
 analiza malware, 158
 archiwizacja danych, 157
 bezprzewodowe, 78
 HackingDojo.com, 67
 idea dowodu koncepcji, 157
 metody sanitizacji, 161

obraz systemu, 158
 obraz typu ghost, 160
 niewirtualne, 86
 przemysłowe, 60
 weryfikacja dysków, 164
 wirtualne, 74, 86
 licencja, 159
 licencja typu shrink-wrap, 47
 lider zespołu, 131
 lista procesów netcat, 316
 listy dyskusyjne, 428
 logowanie użytkownika, 308
 luki w zabezpieczeniach, 59, 60
 aplikacji sieciowych, 356
 informacje, 94
 przeglądarek internetowych, 61
 SQL, 61
 WebGoat, 64
 luki wewnętrzne, 260

Ł

ładunek, payload, 243, 361
 łączy do maszyn wirtualnych, 24

M

MAC, Media Access Control, 223
 malware, 85–88, 92, 157–161
 maszyna wirtualna, VM, 23, 70, 159
 Matahari, 284
 menedżer projektu, 129, 132, 144
 Metasploit, 247
 Meterpreter, 266
 metodologia
 ISSAF, 177
 RAD, 414
 metody
 archiwizacji, 153
 ilościowe, 112
 jakościowe, 112
 mieszane, 112
 sanitizacji, 161
 szyfrowania, 284, 386, 388
 metryki, 373

metryki testu penetracyjnego, 112
 MIB, Management Information Base, 347
 mieszane metody analizy, 115
 MITM, man in the middle, 298, 303
 model
 kaskadowy, 118
 OSI, 209
 spiralny, 118
 TCP/IP, 209
 moduły, 107
 narzędzia medusa, 238
 systemu Nepenthes, 89
 modyfikacja
 dziennika zdarzeń, 310
 interfejsu użytkownika, 303
 tylnych drzwi, 316
 monitorowanie i kontrola, 52, 143, 148
 MySQL, 248

N

nadużycie, 41
 narzędzia
 SNMP, 349
 zautomatyzowane, 233, 357
 narzędzie
 aircrack-ng, 340–344
 airodump-ng, 339, 343
 CORE Impact, 260, 262, 374
 cryptcat, 284
 dig, 191
 ettercap, 298–303
 finger, 199
 Intruder, 361, 362
 JTR, 297
 Metasploit, 59, 90, 242, 269, 333
 Nessus, 59, 373
 netcat, 226, 273, 285
 netdiscover, 204
 nmap, 179, 184, 190, 193
 nslookup, 192
 Proxytunnel, 284
 shred, 162

smbclient, 227
 Socat, 284
 Spider, 358, 359
 Stunnel, 284
 traceroute, 199, 201
 nauka hackingu, 58
 Nepenthes, 89
 NFS, Network File Shares, 248
 nielegalne treści, 41
 niszczenie danych, 156
 NOP, No Operation Performed, 226

O

obraz
 systemu, 158
 typu ghost, 160
 ocena
 projektu, 171
 zespołu, 171
 ochrona
 danych, 86
 dokumentacji, 152
 oCTF, Open Capture the Flag, 93
 odkrycia, 145, 169, 367
 odmowa usługi, 40
 odpowiedzialność, 130
 OECD, 38
 oferty pracy, 432
 opcje
 ataku MITM, 300
 dostarczania, 386
 zabezpieczeń dokumentu, 390
 oprogramowanie
 dla sieci wirtualnej, 68
 open source, 66
 organizacja
 (ISC)2, 404
 ASIS, 421
 edukacyjna, 36
 funkcjonalna, 134
 IEEE, 421
 ISACA, 421
 ISSA, 421
 macierzowa, 135

oparta na projektach, 137
 TOOOOL, 421
 oszacowanie
 ryzyka, 112
 wysiłku, 144
 oszustwo, 41

P

pasywne zbieranie informacji, 176
 pentesterzy, 399
 pharming, 303
 phishing, 305
 ping, 210
 piractwo komputerowe, 41
 planowanie
 następnego testu, 166
 testu, 98
 plik dziennika zdarzeń, 309
 pliki
 .vmx, 72
 konfiguracyjne urządzeń, 25
 PMBOK, 117
 PMI, Project Management Institute, 118
 pobieranie
 danych, 268
 informacji, 323
 pliku konfiguracyjnego, 349
 podręcznik OSSTMM, 104, 176
 kanały, 106
 komunikacja
 bezprowadowa, 107
 moduły, 107
 reguły postępowania, 105
 podsłuchiwanie, 40
 pakietów sieciowych, 298
 podsumowanie, 375
 podszywanie się, 41
 polecenie
 attrib, 317
 date, 310
 snmpwalk, 347
 whois, 202
 PostgreSQL, 249
 powiadomienie o
 przechwyceniu danych, 340

powłoka
 Meterpreter, 267
 netcat, 270
 odwrotna, 284, 269
 odwrotna netcat, 273
 użytkownika root, 264
 poziom
 dostępu, 323
 zagrożenia, 380
 pozwolenie
 na atak, 49
 na hacking, 27
 pozyskiwanie banerów, 224
 pracodawca, 35
 prawo
 amerykańskie
 federalne, 46
 stanowe, 48
 polskie, 42
 unijne, 42
 pretexting, 306
 priorytet
 przyszłych projektów, 145
 ryzyka, 167
 procesy, 269
 monitorowania i kontroli,
 127
 planowania, 120
 realizacji, 124
 rozpoczęcia, 119
 zakończenia, 126
 program, *Patrz także* narzędzie
 Nessus, 33
 VMware Player, 67, 68
 Wireshark, 92
 projekt typu open source, 431
 protokoły sieci
 bezprzewodowych, 336
 protokół
 ARP, 204, 298
 BGP, 303
 DHCP, 303
 ICMP, 208, 303
 SMTP, 244
 SNMP, 335, 344
 TCP, 208
 UDP, 209
 VoIP, 42
 WPA, 289

przechwycony ruch sieciowy,
 302
 przechwytywanie
 komunikacji, 92
 portu, 303
 protokołu BGP, 303
 przejmowanie
 hasła, 42
 systemów, 42
 przekierowanie ICMP, 303
 przestępczość komputerowa,
 33, 39
 przeszukiwanie śmieci, 40
 przygotowanie
 laboratorium, 58
 raportu, 369

R

raport, 366, 369
 końcowy, 380
 wstępny, 370
 recenzja merytoryczna, 371, 380
 reguły, 297
 rejestr zarządzania ryzykiem,
 166
 rejestracja ataku, 91
 rekonesans, 99
 replikacja rzeczywistych
 zdarzeń, 60
 RFC, Request for Comments, 37
 robak Blaster Worm, 161
 robaki, 85
 rodzaje
 ataków, 40
 organizacji, 134
 przestępstw
 komputerowych, 40
 szyfrowania, 74
 role, 130
 rootkit, 317
 routery, 80
 rozwiązania, 368
 rozwiązywanie konfliktów, 53
 ryzyko, 166

S

sanityzacja, 77
 laboratorium, 156
 nośników cyfrowych, 163
 odkryć, 169
 systemu, 161, 165
 SCADA, 141
 scenariusze
 gotowe, 61
 rzeczywiste, 59
 serwer
 BIND, 195
 DNS, 196
 Hackerdemia, 282
 MySQL, 324
 PostgreSQL, 250
 pWnOS, 225, 302, 378
 Samba, 245
 SSH, 281
 VNC, 251
 sieci
 danych, 107
 wirtualne, 65, 78
 skaner
 JBroFuzz, 240
 medusa, 237
 OpenVAS, 239
 skanowanie, 186
 ACK, 218
 aktywne, 209
 FIN, 219
 loginu domyślnego, 237
 niewykrywalne TCP SYN,
 216
 nmap, 215
 pasywne, 212
 ping, 211
 połączenia TCP, 215
 portów, 208
 serwera Hackerdemia, 271
 sieci, 202, 203
 systemu, 90
 systemu Hackerdemia, 314
 TCP, 213
 typu Null, 217
 UDP, 213, 345
 unikające granic sieci, 216

skrypt, 42
 autopwn, 92
 NASL, 236
 tworzący powłokę
 odwrotną, 274
 skrypty
 Meterpreter, 269
 narzędzia nmap, 235
 słownik, 291, 296
 SMB, Server Message Block, 245
 SMTP, 244
 SNMP, Simple Network
 Management Protocol, 335, 344
 socjotechnika, 41, 102, 145, 304
 spadek wydajności, 275
 społeczności lokalne, 427
 sprawdzanie
 faktów, 372
 sieci, 203
 SQL Injection, 352
 SSH, Secure Shell, 225, 277
 standard PMBOK, 117, 118
 organizacja
 funkcjonalna, 134
 macierzowa, 135
 oparta na projektach, 137
 procesy
 monitorowania i kontroli, 127
 planowania, 120
 realizacji, 124
 rozpoczęcia, 119
 zakończenia, 126
 standard WPA, 337
 standardy etyczne, 34
 staż, 432
 stowarzyszenie ISACA, 409
 struktura organizacyjna, 130, 134
 subdomeny, 186
 system
 IDS, 81
 IPS, 81
 Nepenthes, 91
 SCADA, 141
 typu honeypot, 89

systemy
 operacyjne, 84
 plików, 314
 szkolenia, 172
 szpiegostwo, 41
 szyfrowane tunele, 277
 szyfrowanie, 387, 388
 danych, 75
 dysku, 76

Ś

ścieżka kariery, 396, 429

T

taylorizm, 135
 TCP, Transmission Control
 Protocol, 208
 technologia Xen, 88
 telekomunikacja, 107
 terroryzm, 42
 test penetracyjny, 57, 111
 archiwizacja danych, 149
 lista uczestników, 138
 metryki, 112
 planowanie nowego
 projektu, 166
 przeprowadzany
 samodzielnie, 146
 sanityzacja laboratorium,
 156
 wewnętrzny, 21
 zarządzanie projektem, 138
 zarządzanie zespołem, 117
 TTL, Time To Live, 221
 tunel SSH, 277
 tunelowanie, 284
 tworzenie
 bazy danych wiedzy, 168
 bezpiecznej koperty, 389
 czystego systemu, 161
 idei dowodu koncepcji, 157
 kopii, 154
 laboratorium, 61
 obrazu systemu, 158
 raportów, 103

rejestr zarządzania
 ryzykiem, 166
 wartości hash, 75
 tylne drzwi, 272, 315

U

UDP, User Datagram Protocol,
 209
 udział
 sieciowe, 329
 SMB, 331
 ukrywanie
 katalogu, 318
 narzędzi hackingu, 283
 plików, 312, 314, 317
 umowa poufności, 49
 uprawnienia administracyjne,
 345
 uprawnienie ALL
 PRIVILEGES, 326
 uruchomienie
 maszyny wirtualnej, 70
 szyfrowanej powłoki
 odwrotnej, 282
 powłoki zdalnej, 264
 urządzenia sieciowe, 79, 80
 urządzenie ath1, 338
 usługa
 DNS, 191
 TFTP, 82
 ustalanie
 hasła, 246
 systemu operacyjnego
 aktywne, 221
 pasywne, 221
 ustawa
 CAN-SPAM Act, 48
 DMCA, 30
 FISMA, 47
 PATRIOT, 46
 RICO, 46
 usuwanie
 plików, 163
 aplikacji, 164
 artefaktów, 103
 laboratorium, 163

V

VM, Virtual Machines, 61
 VNC, Virtual Network
 Computing, 251
 VoIP, Voice over Internet
 Protocol, 42
 VPN, Virtual Private Network,
 78

W

wabienie, 305
 wartość
 community string, 346
 hash, 164
 klucza, 343
 MIB, 348
 WebGoat, 64
 weryfikacja
 dysków, 164
 stanu sygnatury, 384
 wirtualizacja, 66
 wirusy, 85
 witryna HackingDojo.com, 22
 włamanie
 do sieci, 42
 do systemu, 59
 właściciel danych, 152, 155
 wolontariat, 430

WPA, Wi-Fi Protected Access,
 79, 289, 337
 współdzielone katalogi, 246
 wykorzystanie
 luk, 231, 259
 luk lokalnych, 261
 luki Debian OpenSSL, 378
 luki OpenSSL, 377, 379
 wykrywanie
 luk w zabezpieczeniach, 207
 maszyny wirtualnej, 87
 tylnych drzwi, 316
 włamań, 60
 wynagrodzenie, 433
 wyniki skanowania, 373
 wyszukiwanie użytkowników
 SMB, 245

Z

zabezpieczanie certyfikatu, 383
 systemu, 76
 zablokowanie konta, 292
 zacieranie śladów, 311, 319
 zadania inżyniera testu
 penetracyjnego, 133
 zaporą sieciową, 60, 80, 278
 zapytania DNS, 195
 zapytanie do bazy, 323, 324
 zarządzanie

projektem, 138
 etap planowania, 140
 etap realizacji, 141
 etap rozpoczęcia, 138
 etap zakończenia, 144
 model kaskadowy, 118
 model spiralny, 118
 monitorowanie i kontrola,
 143
 ryzykiem, 166
 testem penetracyjnym, 111
 zmianami, 165
 zatrucie ARP, 301
 bufora DNS, 303
 protokołu ARP, 223
 zbieranie informacji, 175, 193
 pasywne, 176
 aktywne, 195
 zgłaszanie odkryć, 367
 zleceniodawca, 35
 złośliwy kod, 41, 88, 158
 zmiana informacji, 40
 zobowiązania
 firmy, 50
 wykonawcy, 51

Ż

żądanie ping, 211
 życiorys, 430

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA



Helion SA

Twój przewodnik w testach penetracyjnych!

Trzonem każdego systemu informatycznego są dane oraz gwarancja ich bezpieczeństwa. Jest to szczególnie ważne, ponieważ codziennie w najróżniejszych systemach przetwarzane są setki informacji na temat każdego z nas. Czasami są to dane mało istotne — wpisy na portalach społecznościowych lub komentarze na popularnym portalu internetowym. Jednak obok nich przetwarzane są nasze dane medyczne, informacje o rachunkach bankowych oraz zobowiązaniach. Ich utrata lub ujawnienie to prawdziwa katastrofa! Jak zapobiegać takim sytuacjom? Jak zagwarantować klientom pełne bezpieczeństwo danych?

W celu sprawdzenia bezpieczeństwa serwisu przeprowadzane są testy penetracyjne — kontrolowane próby przełamania zabezpieczeń. Zajmują się tym najlepsi specjaliści, a pozytywny wynik testów pozwala mieć nadzieję, że włamywaczowi również nie uda się wtargnąć do serca systemu. Ta książka została w całości poświęcona takim testom. W trakcie lektury dowiesz się, jak przygotować środowisko pracy

oraz jak chronić dane testu penetracyjnego. Ponadto poznasz popularne metodologie, narzędzia oraz techniki zarządzania testami. Warto zwrócić uwagę na zagadnienia prawne i zapoznać oraz zapoznać się z możliwościami kariery w tej branży. Książka ta jest obowiązkową lekturą dla wszystkich zainteresowanych bezpieczeństwem systemów informatycznych oraz prowadzeniem testów penetracyjnych.

Dzięki tej książce:

- zaznajomisz się z aspektem prawnym testów penetracyjnych
- zbudujesz środowisko pracy
- poznasz ważne luki w codziennych usługach
- odkryjesz popularne narzędzia oraz metodologie prowadzenia testów
- poznasz ścieżki kariery w branży

helion.pl
księgarnia
internetowa

Nr katalogowy: 19974



Księgarnia internetowa
http://helion.pl



Zamówienia telefoniczne:

0 801 339900



0 601 339900



Helion

Sprawdź najnowsze promocje:

• <http://helion.pl/promocje>

Książki najchętniej czytane:

• <http://helion.pl/bestsellery>

Zamów informacje o nowościach:

• <http://helion.pl/nawosci>

Helion SA

ul. Kościuszki 1c, 44-100 Gliwice

tel.: 32 230 98 63

e-mail: helion@helion.pl

<http://helion.pl>

sięgnij po WIĘCEJ



KOD KORZYŚCI

ISBN 978-83-246-9033-6



9 788324 690336

cena: 69,00 zł

Informatyka w najlepszym wydaniu