

Kali Linux

Wydanie II

Zaawansowane testy penetracyjne za pomocą narzędzi Nmap, Metasploit, Aircrack-ng i Empire

Glen D. Singh

Helion 



Tytuł oryginału: The Ultimate Kali Linux Book: Perform advanced penetration testing using Nmap, Metasploit, Aircrack-ng, and Empire, 2nd Edition

Tłumaczenie: Joanna Zatorska

ISBN: 978-83-283-9835-1

Copyright © Packt Publishing 2022. First published in the English language under the title 'The Ultimate Kali Linux Book - Second Edition – (9781801818933)'

Polish edition copyright © 2023 by Helion S.A.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

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

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<https://helion.pl/user/opinie/kaliz2>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: <https://helion.pl> (księgarnia internetowa, katalog książek)

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści |

O autorze	15
O recenzentach	16
Wstęp	17

CZĘŚĆ 1. Wprowadzenie do testów penetracyjnych

Rozdział 1	
Wstęp do etycznego hakowania	25
Identyfikacja złośliwych aktorów i ich zamierzeń	26
Co ma znaczenie dla złośliwych aktorów	29
Czas	29
Zasoby	29
Czynniki finansowe	30
Wartość hakowania	30
Terminologia związana z cyberbezpieczeństwem	30
Dlaczego trzeba przeprowadzać testy penetracyjne i na jakie etapy można je podzielić	33
Tworzenie planu bitwy testu penetracyjnego	34
Podejścia stosowane w testach penetracyjnych	38
Rodzaje testów penetracyjnych	39
Etapy hakowania	41
Rekonesans, czyli zbieranie informacji	42
Skanowanie i enumeracja	42
Uzyskanie dostępu	43
Utrzymanie dostępu	43
Zacieranie śladów	44
Platforma Cyber Kill Chain	44
Rekonesans	45
Zbrojenia	46

Dostarczanie	46
Eksploracja	48
Instalacja	48
Połączenia Command and Control (C2)	48
Działanie	49
Podsumowanie	49
Dalsza lektura	50

Rozdział 2

Tworzenie laboratorium do testów penetracyjnych	51
Wymagania techniczne	52
Ogólny opis laboratorium i wykorzystywanych w nim technologii	52
Konfiguracja hipernadzorcy i odizolowanych sieci wirtualnych	54
Część 1. Wdrażanie hipernadzorcy	55
Część 2. Tworzenie odizolowanych sieci wirtualnych	56
Konfiguracja systemu Kali Linux i praca w nim	57
Część 1. Konfiguracja systemu Kali Linux na maszynie wirtualnej	57
Część 2. Dostosowanie maszyny wirtualnej z systemem Kali Linux oraz kart sieciowych	60
Część 3. Początki pracy w systemie Kali Linux	64
Część 4. Aktualizowanie źródeł i pakietów	66
Wdrażanie podatnego na atak systemu Metasploitable 2	68
Część 1. Wdrażanie systemu Metasploitable 2	68
Część 2. Konfigurowanie ustawień sieciowych	70
Implementacja systemu Metasploitable 3 za pomocą Vagranta	72
Część 1. Konfigurowanie wersji dla systemu Windows	72
Część 2. Konfiguracja wersji dla Linuksa	75
Konfigurowanie systemów z aplikacjami WWW podatnymi na ataki	77
Część 1. Wdrażanie projektu OWASP Juice Shop	78
Część 2. Konfigurowanie projektu OWASP Broken Web Applications	82
Podsumowanie	84
Dalsza lektura	85

Rozdział 3

Konfiguracja dla zaawansowanych technik hakerskich	86
Wymagania techniczne	86
Budowanie laboratorium AD czerwonego zespołu	87
Część 1. Instalowanie systemu Windows Server 2019	89
Część 2. Instalowanie systemu Windows 10 Enterprise	93
Część 3. Konfigurowanie usług AD	95
Część 4. Podnoszenie do poziomu kontrolera domeny	96

Część 5. Tworzenie kont użytkowników i administratora domeny	98
Część 6. Wyłączanie ochrony przed złośliwym oprogramowaniem oraz zapory sieciowej domeny	99
Część 7. Konfiguracja przygotowująca do ataków na mechanizmy udostępniania plików i uwierzytelniania	101
Część 8. Przyłączanie klientów do domeny AD	103
Część 9. Konfiguracja na potrzeby przejęcia lokalnego konta i ataków SMB	104
Konfigurowanie laboratorium do bezprzewodowych testów penetracyjnych	105
Implementowanie serwera RADIUS	107
Podsumowanie	115
Dalsza lektura	116

CZĘŚĆ 2. Rekonesans i testy penetracyjne sieci

Rozdział 4

Rekonesans i footprinting	119
Wymagania techniczne	119
Znaczenie rekonesansu	120
Footprinting	120
Pasywne zbieranie informacji	122
Oprogramowanie wywiadowcze open source	122
Strategie OSINT w zbieraniu danych wywiadowczych	123
Znaczenie pacynki	124
Anonimizacja ruchu sieciowego	125
Profilowanie infrastruktury IT docelowej organizacji	133
Pozyskiwanie danych pracowników	136
Rekonesans w mediach społecznościowych	149
Zbieranie danych o infrastrukturze organizacji	153
Podsumowanie	165
Dalsza lektura	165

Rozdział 5

Aktywne zbieranie informacji	166
Wymagania techniczne	167
Zasady aktywnego rekonesansu	167
Przegląd strategii Google hacking	168
Rekonesans DNS	174
Enumerowanie DNS	177
Sprawdzanie błędnej konfiguracji transferu stref DNS	178
Automatyzacja zbierania danych OSINT	181

Enumerowanie subdomen	186
Korzystanie z programu DNSmap	186
Używanie programu Sublist3r	187
Profilowanie witryn WWW za pomocą programu EyeWitness	189
Korzystanie z technik aktywnego skanowania	190
Spoofing adresów MAC	192
Wykrywanie systemów uruchomionych w sieci	193
Sondowanie otwartych portów usług, uruchomionych usług i systemów operacyjnych	196
Unikanie wykrycia	199
Enumerowanie popularnych usług sieciowych	203
Skanowanie za pomocą platformy Metasploit	204
Enumerowanie usługi SMB	205
Enumerowanie usługi SSH	208
Enumerowanie użytkowników poprzez hałaśliwe uwierzytelnianie	209
Znajdowanie wycieków danych w chmurze	212
Podsumowanie	216
Dalsza lektura	217

Rozdział 6

Ocena podatności	218
Wymagania techniczne	218
Nessus i jego zasady	219
Konfiguracja Nessusa	219
Skanowanie za pomocą Nessusa	223
Analiza wyników Nessusa	225
Eksportowanie wyników Nessusa	230
Wykrywanie podatności programem Nmap	232
Korzystanie z programu Greenbone Vulnerability Manager	236
Używanie skanerów aplikacji internetowych	242
WhatWeb	242
Nmap	243
Metasploit	244
Nikto	247
WPScan	248
Podsumowanie	249
Dalsza lektura	250

Rozdział 7

Testy penetracyjne sieci	251
Wymagania techniczne	251
Wprowadzenie do testów penetracyjnych sieci	252
Korzystanie z technologii bind shell i reverse shell	255
Zdalna powłoka z użyciem Netcata	257
Tworzenie powłoki bind shell	259
Konfiguracja mechanizmu reverse shell	261
Techniki omijania zabezpieczeń antywirusowych	262
Kodowanie ładunków programem MSFvenom	263
Tworzenie ładunków programem Shellter	266
Obsługa bezprzewodowych kart sieciowych	272
Łączenie bezprzewodowej karty sieciowej z systemem Kali Linux	274
Podłączanie bezprzewodowej karty sieciowej z mikroukładem RTL8812AU	277
Zarządzanie trybami bezprzewodowymi i monitorowanie ich	280
Ręczne konfigurowanie trybu monitorowania	280
Włączanie trybu monitorowania za pomocą pakietu Aircrack-ng	283
Podsumowanie	285
Dalsza lektura	286

Rozdział 8

Przeprowadzanie testów penetracyjnych sieci	287
Wymagania techniczne	288
Wykrywanie działających systemów	288
Profilowanie systemu docelowego	291
Ataki z wykorzystaniem haseł	293
Wykorzystanie protokołu Remote Desktop Protocol w systemie Windows	295
Tworzenie listy haseł na podstawie słów kluczowych	297
Tworzenie list słów z użyciem programu Crunch	299
Znajdowanie i wykorzystywanie podatnych usług	299
Wykorzystywanie podatnej usługi w systemie Linux	299
Wykorzystanie usługi SMB w systemie Microsoft Windows	303
Przekazywanie wartości skrótu	314
Uzyskiwanie dostępu za pośrednictwem usługi SSH	318
Wykorzystanie protokołu Windows Remote Management	321
Wykorzystywanie luk w usłudze Elasticsearch	325
Wykorzystywanie protokołu Simple Network Management Protocol	326
Ataki z wykorzystaniem taktyki wodopoju	328
Podsumowanie	329
Dalsza lektura	330

CZĘŚĆ 3. Techniki czerwonego zespołu

Rozdział 9

Zaawansowane testy penetracyjne sieci — posteksploatacja	333
Wymagania techniczne	334
Posteksploatacja za pomocą programu Meterpreter	334
Główne operacje	335
Operacje w interfejsie użytkownika	338
Przesyłanie plików	339
Eskalacja uprawnień	341
Kradzież tokenów i podszywanie się	342
Utrwalanie dostępu	345
Eskalacja pozioma i używanie hosta pośredniczącego	349
Zacieranie śladów	353
Kodowanie i eksfiltracja danych	354
Kodowanie plików wykonywalnych za pomocą programu exe2hex	354
Eksfiltracja danych za pomocą programu PacketWhisper	357
Ataki MITM i przechwytywanie pakietów	364
Przeprowadzanie ataków MITM za pomocą programu Ettercap	367
Podsumowanie	369
Dalsza lektura	369

Rozdział 10

Ataki na usługę Active Directory	371
Wymagania techniczne	371
Czym jest usługa Active Directory	372
Enumerowanie Active Directory	376
Korzystanie z programu PowerView	378
Korzystanie z programu Bloodhound	387
Wykorzystanie relacji zaufania w sieci	392
Wykorzystywanie protokołów LLMNR i NetBIOS-NS	393
Wykorzystywanie zaufania między protokołem SMB a NTLMv2 w usłudze Active Directory	399
Podsumowanie	406
Dalsza lektura	407

Rozdział 11

Zaawansowane ataki na Active Directory	408
Wymagania techniczne	408
Zasady działania Kerberos'a	409

Wykorzystanie zaufania w sieci IPv6 w usłudze Active Directory	411
Część 1. Konfiguracja potrzebna do ataku	412
Część 2. Uruchamianie ataku	414
Część 3. Przejmowanie kontroli nad domeną	417
Atakowanie Active Directory	418
Eskalacja pozioma za pomocą programu CrackMapExec	418
Eskalacja pionowa z wykorzystaniem Kerberos	421
Eskalacja pozioma za pomocą programu Mimikatz	423
Przejmowanie kontroli nad domeną i trwała obecność	427
Złoty bilet	428
Srebrny bilet	431
Klucz szkieletowy	433
Podsumowanie	436
Dalsza lektura	437

Rozdział 12

Taktyki Command and Control	438
Wymagania techniczne	438
Zasady operacji C2	439
Konfigurowanie operacji C2	440
Część 1. Konfiguracja serwera Empire	442
Część 2. Zarządzanie użytkownikami	445
Posteksploatacja za pomocą platformy Empire	447
Część 1. Konfigurowanie nasłuchiwanie	448
Część 2. Tworzenie stagera	449
Część 3. Korzystanie z agentów	450
Część 4. Tworzenie nowego agenta	454
Część 5. Lepsza emulacja zagrożeń	455
Część 6. Konfiguracja stałego dostępu	457
Używanie Starkillera	458
Część 1. Uruchamianie programu Starkiller	459
Część 2. Zarządzanie użytkownikami	459
Część 3. Korzystanie z modułów	462
Część 4. Tworzenie listenerów	463
Część 5. Tworzenie stagerów	464
Część 6. Korzystanie z agentów	466
Część 7. Dane dostępne i raportowanie	468
Podsumowanie	471
Dalsza lektura	471

Rozdział 13

Zaawansowane bezprzewodowe testy penetracyjne	473
Wymagania techniczne	474
Wprowadzenie do sieci bezprzewodowych	474
SISO i MIMO	476
Standardy bezpieczeństwa sieci bezprzewodowych	479
Rekonesans sieci bezprzewodowej	481
Ustalanie klientów powiązanych z określoną siecią	486
Włamywanie się do sieci WPA i WPA2	488
Przeprowadzanie ataków AP-less	492
Włamywanie się do bezprzewodowych sieci firmowych	497
Część 1. Konfiguracja przygotowująca do ataku	498
Część 2. Określanie celu	500
Część 3. Rozpoczynanie ataku	503
Część 4. Pobieranie danych dostępowych użytkownika	505
Tworzenie bezprzewodowego honeypota	508
Wykrywanie ataków na sieci WPA3	513
Przeprowadzanie ataków typu downgrade i słownikowych	514
Zabezpieczanie sieci bezprzewodowych	518
Zarządzanie identyfikatorami SSID	518
Filtrowanie adresów MAC	519
Poziomy mocy w antenach	520
Silne hasła	520
Zabezpieczanie firmowej sieci bezprzewodowej	521
Podsumowanie	522
Dalsza lektura	522

CZĘŚĆ 4. Inżynieria społeczna i ataki na aplikacje internetowe

Rozdział 14

Ataki na klienta — inżynieria społeczna	525
Wymagania techniczne	525
Podstawowe zasady inżynierii społecznej	526
Elementy inżynierii społecznej	527
Rodzaje ataków z wykorzystaniem inżynierii społecznej	529
Techniki oparte na interakcjach z ludźmi	529
Ataki z wykorzystaniem komputerów	530

Ataki z wykorzystaniem urządzeń mobilnych	531
Witryny społecznościowe	532
Obrona przed inżynierią społeczną	533
Planowanie ataków z wykorzystaniem inżynierii społecznej	534
Narzędzia i techniki wykorzystywane w inżynierii społecznej	535
Tworzenie witryny phishingowej	536
Tworzenie urządzeń infekujących	539
Podsumowanie	542
Dalsza lektura	543

Rozdział 15

Bezpieczeństwo aplikacji internetowych544

Wymagania techniczne	544
Charakterystyka aplikacji WWW	545
Podstawowe zasady protokołu HTTP	546
Lista OWASP Top 10: 2021	549
Zapoznanie z programami FoxyProxy i Burp Suite	551
Część 1. Konfigurowanie programu FoxyProxy	552
Część 2. Konfiguracja pakietu Burp Suite	554
Część 3. Zapoznanie z możliwościami programu Burp Suite	556
Ataki przez wstrzykiwanie	561
Przeprowadzanie ataku przez wstrzykiwanie SQL	562
Ataki wykorzystujące błędy w mechanizmach kontroli dostępu	569
Wykorzystanie błędów w mechanizmach kontroli dostępu	569
Wykrywanie usterek kryptograficznych	572
Wykorzystywanie usterek kryptograficznych	573
Zagrożenia związane z projektowaniem z pominięciem zasad bezpieczeństwa	578
Błędna konfiguracja zabezpieczeń	578
Wykorzystywanie błędnej konfiguracji	579
Podsumowanie	582
Dalsza lektura	583

Rozdział 16

Zaawansowane testy penetracyjne witryn internetowych584

Wymagania techniczne	585
Wykrywanie podatnych i przestarzałych komponentów	585
Wykrywanie podatnych komponentów	585
Wykorzystywanie usterek w identyfikacji i uwierzytelnianiu	588
Wykrywanie usterek uwierzytelniania	589

Usterki w integralności oprogramowania i danych	594
Usterki w monitorowaniu i rejestracji zdarzeń związanych z bezpieczeństwem	594
Przeprowadzanie ataków typu server-side request forgery	595
Automatyzacja ataków przez wstrzykiwanie SQL	599
Część 1. Wykrywanie baz danych	599
Część 2. Pobieranie poufnych informacji	603
Ataki cross-site scripting	606
Część 1. Wykrywanie ataków typu reflected XSS	608
Część 2. Wykrywanie ataków stored XSS	611
Przeprowadzanie ataków po stronie klienta	613
Podsumowanie	619
Dalsza lektura	619

Rozdział 17

Najlepsze praktyki dla rzeczywistych testów	620
Wymagania techniczne	620
Wskazówki dla pentesterów	621
Uzyskiwanie pisemnej zgody	621
Postępowanie etyczne	621
Kontrakt dotyczący testów penetracyjnych	621
Zasady zaangażowania	622
Lista kontrolna dla testów penetracyjnych	622
Zbieranie informacji	623
Skanowanie sieci	623
Enumeracja	624
Uzyskiwanie dostępu	624
Zacieranie śladów	625
Pisanie raportów	625
Tworzenie przybornika hakera	626
Konfigurowanie zdalnego dostępu	631
Następne kroki	635
Podsumowanie	636
Dalsza lektura	636

Skorowidz	638
------------------------	------------

Tworzenie laboratorium do testów penetracyjnych

Rozdział

2

Będąc kandydatem na etycznego hakera lub pentestera, należy pamiętać, że podczas testowania exploitów, ładunków lub ćwiczenia umiejętności hakerskich nie można zakłócać pracy ani powodować żadnych szkód w systemach i infrastrukturze sieciowej innych osób i organizacji. Choć możesz czerpać wiedzę z wielu materiałów, filmów i programów szkoleniowych, to jednak praca pentestera wymaga stałego doskonalenia umiejętności. Wiele osób z łatwością objaśnia metody działania hakerów, ale nie umie przeprowadzić ataku. Podczas nauki wykonywania testów penetracyjnych trzeba koniecznie zrozumieć teorię oraz nauczyć się wykorzystywać ją w praktyce, podczas rzeczywistego cyberataku.

W tym rozdziale dowiesz się, jak zaprojektować i zbudować na swoim komputerze środowisko laboratoryjne do testów penetracyjnych z wykorzystaniem technologii wirtualizacji. Nauczysz się tworzyć wirtualne odizolowane sieci, dzięki czemu unikniesz przypadkowego ataku na nienależące do Ciebie systemy. Następnie nauczysz się konfigurować system Kali Linux, służący do przeprowadzania ataków, a także podatne klienty i serwery, które będą celem ataków. Ćwiczenie umiejętności hakerskich na systemach i sieciach, które do Ciebie nie należą, jest niepożądane i nielegalne, ponieważ może doprowadzić do ich uszkodzenia.

W tym rozdziale zostaną omówione następujące zagadnienia:

- Ogólny opis laboratorium i wykorzystywanych w nim technologii.
- Konfiguracja hipernadzorcy i odizolowanych sieci wirtualnych.
- Konfiguracja systemu Kali Linux i praca w nim.
- Wdrażanie systemu Metasploitable 2, który będzie celem ataków.
- Implementacja systemu Metasploitable 3 za pomocą Vagranta.
- Konfiguracja systemów z aplikacjami WWW podatnymi na atak.

Zaczynamy!

Wymagania techniczne

Wykonanie ćwiczeń opisanych w tym rozdziale wymaga użycia następujących urządzeń i programów:

- Oracle VM VirtualBox: <https://www.virtualbox.org/wiki/Downloads>,
- Oracle VM VirtualBox Extension Pack:
<https://www.virtualbox.org/wiki/Downloads>,
- Vagrant: <https://www.vagrantup.com/downloads>,
- Kali Linux 2021.2: <http://old.kali.org/kali-images/kali-2021.2/>¹,
- OWASP Juice Shop: <https://owasp.org/www-project-juice-shop/>,
- Metasploitable 2:
<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>,
- Metasploitable 3:
<https://app.vagrantup.com/rapid7/boxes/metasploitable3-win2k8>,
- OWASP Broken Web Applications:
<https://sourceforge.net/projects/owaspbwa/files/>.

Ogólny opis laboratorium i wykorzystywanych w nim technologii

Dzięki własnemu laboratorium do testów penetracyjnych będziesz dysponować środowiskiem, w którym będziesz w stanie bezpiecznie rozwijać swoje umiejętności, skalować je, dodając nowe, podatne na ataki systemy, a nawet usuwać przestarzałe, niepotrzebne już systemy. Będziesz też tworzyć sieci wirtualne, aby przekierowywać swoje ataki z jednej sieci na inną. Po utworzeniu własnego wirtualnego laboratorium do testów penetracyjnych będziesz wykorzystywać wszystkie zasoby swojego komputera i unikniesz konieczności kupowania czasu laboratoriów online od różnych dostawców. Nie będziesz też musiał(a) kupować dodatkowych komputerów i usług. Dzięki temu zaoszczędzisz mnóstwo pieniędzy, ponieważ w przeciwnym razie musiał(a)byś kupić nowe komputery i urządzenia sieciowe, np. switchy i routery.

Jako szkoleniowiec i ekspert z branży cyberbezpieczeństwa zauważyłem, że wiele osób, które zaczynają swoją działalność w branży informatycznej, zwykle przecenia konieczność posiadania fizycznej infrastruktury. Rzeczywiście jest ona potrzebna, ale dzięki postępom technologicznym budowanie laboratorium fizycznego w celu doskonalenia swoich umiejętności ma wiele wad.

¹ Najnowsza wersja systemu Kali Linux jest dostępna pod adresem <https://www.kali.org/get-kali/> — przyp. tłum.

Oto kilka wad fizycznego laboratorium:

- Niezbędne jest miejsce na przechowywanie wielu potrzebnych serwerów i urządzeń sieciowych.
- Wykorzystanie energii przez urządzenia wymaga wysokich nakładów finansowych.
- Koszt zbudowania lub kupna każdego urządzenia fizycznego jest wysoki. Dotyczy to zarówno urządzeń sieciowych, jak i serwerów.

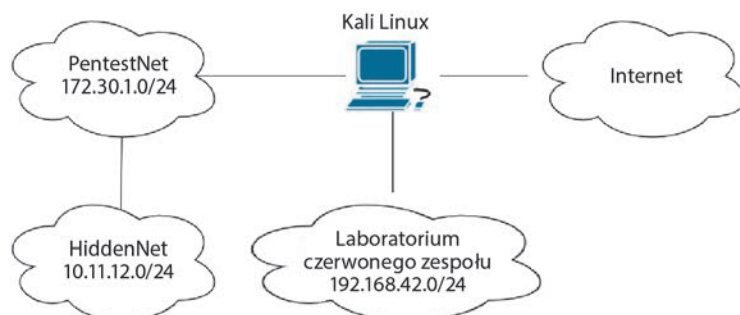
To tylko kilka problemów, z którymi styka się wielu studentów i początkujących informatyków. W licznych przypadkach początkujący ma tylko jeden komputer stacjonarny lub laptop. Technologie wirtualizacji, które rozwinęły się w reakcji na wspomniane problemy, otworzyły nowe możliwości w branży IT. Dzięki temu wiele osób i organizacji może skuteczniej zarządzać swoimi zasobami sprzętowymi.

W świecie wirtualizacji hipernadzorca jest specjalną aplikacją, za pomocą której można zwirtualizować zasoby sprzętowe na swoim systemie, a następnie udostępnić je innym systemom operacyjnym lub aplikacjom. Dzięki temu w systemie operacyjnym komputera można zainstalować wiele innych systemów operacyjnych. Wyobraź sobie, że Twój komputer działa pod kontrolą systemu operacyjnego Microsoft Windows 10, ale chcesz na tym samym komputerze korzystać również z Linuksa. Dzięki hipernadzorcy jest to możliwe. Skorzystamy zatem z wirtualizacji, aby zbudować tanie laboratorium do testów penetracyjnych.

Do zbudowania laboratorium potrzebne są następujące komponenty:

- **Hipernadzorca.** Potrzebny do utworzenia maszyn wirtualnych. Skorzystamy w tym celu z aplikacji **Oracle VM VirtualBox**.
- **Dostęp do internetu.** Niezbędny do pobrania dodatkowych aplikacji. Internet będzie też dostępny w systemie agresora, przy czym wszystkie systemy będą od siebie odizolowane w środowiskach wirtualnych.
- **Maszyna wirtualna do testów penetracyjnych.** Będzie to system agresora. Skorzystamy w tym celu z systemu Kali Linux.
- **Systemy klienckie podatne na atak.** Podczas testów zabezpieczeń będą to systemy ofiary. Użyjemy w tym celu systemów Metasploitable 2 i Metasploitable 3 (zarówno w wersji dla systemów Windows, jak i Linux), chociaż w dalszych częściach książki będziemy dodawać również inne systemy.
- **Aplikacje internetowe podatne na atak.** Są to systemy z zainstalowanymi aplikacjami WWW podatnymi na ataki, dzięki czemu można lepiej zrozumieć luki w zabezpieczeniach aplikacji WWW. Użyjemy w tym celu systemów **Open Web Application Security Project (OWASP) Juice Shop** i **OWASP Broken Web Applications (BWA)**.

Rysunek 2.1 pokazuje topologię naszego laboratorium do testów penetracyjnych.



Rysunek 2.1. Topologia laboratorium

Na diagramie przedstawione są trzy sieci prywatne. *PentestNet* to sieć 172.30.1.0/24, w której dostępne będą systemy podatne na atak, czyli Metasploitable 2 i 3, oraz maszyny wirtualne OWASP BWA. *HiddenNet* to sieć 10.11.12.0/24, dostępna tylko za pośrednictwem sieci 172.30.1.0/24. Jest to doskonały układ do nauki eskalacji poziomej i wykorzystywania hostów pośredniczących w dalszej części książki. Ponadto Kali Linux jest bezpośrednio połączony z laboratorium Red Team z siecią **Active Directory (AD)**. Jego tworzenie jest omówione w rozdziale 3., „Konfiguracja dla zaawansowanych technik hakerskich”.

Znasz już topologię laboratorium oraz systemy i technologie, z których będziemy korzystać w tej książce. Możesz zatem przystąpić do konfiguracji hipernadzorcy i sieci wirtualnych.

Konfiguracja hipernadzorcy i odizolowanych sieci wirtualnych

Na rynku dostępnych jest wiele innych hipernadzorców, ale program Oracle VM VirtualBox jest darmowy i łatwy w użyciu. Zawiera prawie wszystkie funkcje dostępne w produktach komercyjnych. W tym podrozdziale dowiesz się, jak skonfigurować hipernadzorcę VirtualBox oraz jak utworzyć sieci wirtualne.

Zanim zaczniesz, upewnij się, że spełniasz następujące wymagania:

- Procesor powinien obsługiwać funkcje wirtualizacji **VT-x/AMD-V**.
- Funkcje wirtualizacji powinny być włączone w interfejsie BIOS/UEFI.

Zaczynamy!

Część 1. Wdrażanie hipernadzorcy

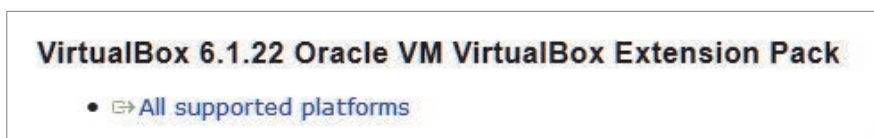
Chociaż wielu dostawców oferuje różne aplikacje hipernadzorców, w tej książce będziemy używać programu Oracle VirtualBox. Jeśli wolisz korzystać z innego hipernadzorcy, skonfiguruj go w taki sposób, aby używać tych samych systemów i konfiguracji sieci. Oto kroki potrzebne do wdrożenia programu Oracle VirtualBox:

1. Pobierz program VirtualBox (patrz rysunek 2.2) ze strony <https://www.virtualbox.org/wiki/Downloads>. Wybierz pakiet dla swojego systemu operacyjnego.



Rysunek 2.2. Strona pobierania programu VirtualBox

2. Potrzebny jest także pakiet **Oracle VM VirtualBox Extension Pack**, który rozszerza VirtualBox o dodatkowe funkcje, np. tworzenie odizolowanych od siebie sieci wirtualnych (patrz rysunek 2.3). Przewiń nieco w dół stronę *Download* i znajdź łącze pobierania.



Rysunek 2.3. Pakiet rozszerzeń dla programu VirtualBox

3. Zainstaluj pakiet programu VirtualBox pobrany w pierwszym kroku. Użyj domyślnych ustawień. Po zainstalowaniu aplikacji pojawi się na ekranie okno *Oracle VM VirtualBox Manager* (*Oracle VM VirtualBox Menedżer*).

4. Aby zainstalować pakiet **VirtualBox Extension Pack**, kliknij pobrany plik prawym przyciskiem myszy i wybierz polecenie *Open With (Otwórz za pomocą)/VirtualBox Manager*. Zaakceptuj umowę użytkownika i uruchom instalację.

Część 2. Tworzenie odizolowanych sieci wirtualnych

Podczas testów penetracyjnych w środowisku laboratoryjnym musisz mieć pewność, że nie przeskanujesz przypadkowych sieci ani systemów, np. dostępnych w internecie, ani nie uruchomisz na nich szkodliwego ładunku. Opisane dalej kroki pokazują, jak utworzyć odizolowane sieci wirtualne w programie Oracle VirtualBox, aby skonfigurować topologię sieci w laboratorium do testów penetracyjnych:

1. Aby utworzyć sieci wirtualną z serwerem DHCP i adresem 172.30.1.0/24, otwórz program *Windows Command Prompt (Wiersz polecenia systemu Windows)* i wykonaj następujące polecenia:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=PentestNet --server-ip=172.30.1.1 --lower-ip=172.30.1.20 --
upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable
```

Program VirtualBox utworzy serwer DHCP z adresem IP 172.30.1.1, umożliwiając przydzielenie adresów IP z zakresu 172.30.1.20 – 172.30.1.50 do maszyn wirtualnych połączonych z siecią PentestNet.

2. W programie Windows Command Prompt wykonaj następujące polecenia, aby utworzyć wirtualną sieć z serwerem DHCP dla ukrytej sieci. Nazwij ją HiddenNet:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=HiddenNet --server-ip=10.11.12.1 --lower-ip=10.11.12.20 --
upper-ip=10.11.12.50 --netmask=255.255.255.0 --enable
```

3. Utwórz odizolowaną sieć wirtualną dla czerwonego zespołu:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=RedTeamLab --server-ip=192.168.42.1 --lower-ip=192.168.42.20 --
upper-ip=192.168.42.50 --netmask=255.255.255.0 --enable
```

Pamiętaj, aby zachować konwencję nazewnictwa dla każdego laboratorium tworzonego w tej książce (PentestNet, HiddenNet i RedTeamLab), gwarantując prawidłowe działanie sieci wirtualnych.

W tym podrozdziale dowiedziałeś(-łaś) się, jak zainstalować hipernadzorcę i utworzyć odizolowane sieci wirtualne. Skorzystasz z nich w następnym podrozdziale podczas konfiguracji systemu agresora, czyli Kali Linux.

Konfiguracja systemu Kali Linux i praca w nim

System Kali Linux jest zbudowany na bazie dystrybucji Linuksa Debian i zawiera ponad 300 wstępnie zainstalowanych narzędzi, za pomocą których można przeprowadzać rekonesans, uruchamiać eksploity, a nawet prowadzić działania śledcze. System operacyjny Kali Linux jest przeznaczony nie tylko dla specjalistów ds. bezpieczeństwa, ale również dla administratorów IT, a nawet specjalistów ds. bezpieczeństwa sieci. Jest to darmowy system operacyjny, który zawiera narzędzia potrzebne do przeprowadzania testów bezpieczeństwa.

Kali Linux oferuje wiele funkcji i narzędzi, które nieco ułatwiają pracę pentesterom i inżynierom ds. bezpieczeństwa. Do dyspozycji są liczne narzędzia, skrypty i platformy służące do wykonania różnych zadań, takich jak zbieranie informacji o celu ataku, skanowanie sieci, wykrywanie podatności, a nawet uruchamianie exploitów.

W tym podrozdziale skonfigurujesz system Kali Linux na maszynie wirtualnej, nawiążesz połączenie z internetem i z odizolowanymi sieciami wirtualnymi oraz poznasz podstawowe zasady pracy z tym systemem.

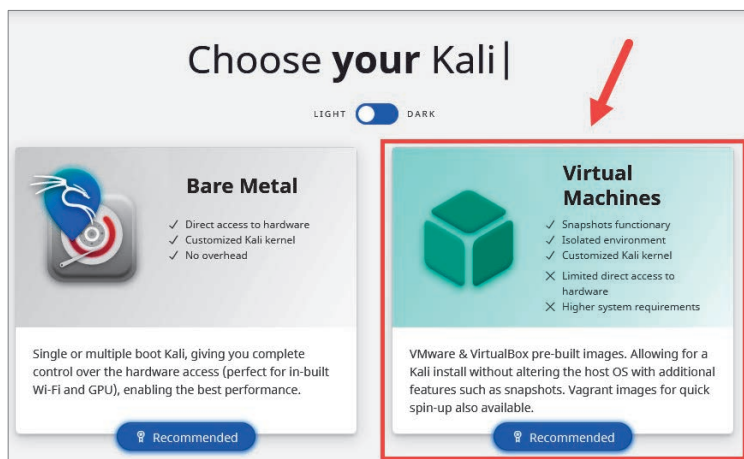
Zaczynamy!

Część 1. Konfiguracja systemu Kali Linux na maszynie wirtualnej

Kali Linux można wdrażać na różne sposoby. Można np. zainstalować podstawową wersję bezpośrednio na urządzeniu lub na urządzeniach z systemem Android. Aby uprościć ten proces, skonfigurujesz obraz maszyny wirtualnej z systemem Kali Linux w programie Oracle VirtualBox. Dzięki temu będzie można szybko rozpocząć pracę. Wykonaj następujące kroki:

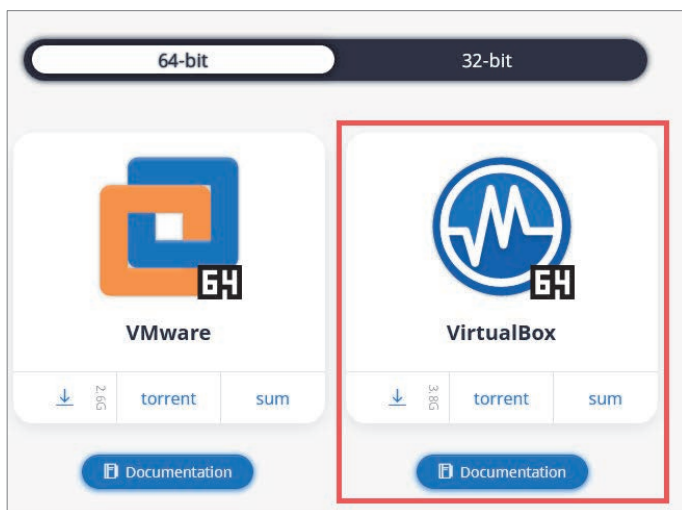
1. Aby pobrać oficjalny obraz wirtualny najnowszej wersji systemu Kali Linux, przejdź na stronę <https://www.kali.org/get-kali/>² i kliknij kartę *Virtual Machines*, widoczną na rzucie ekranu przedstawionym na rysunku 2.4.

² W książce używana jest wersja systemu 2021.1, którą można pobrać pod adresem <http://old.kali.org/kali-images/kali-2021.2/> — przyp. tłum.



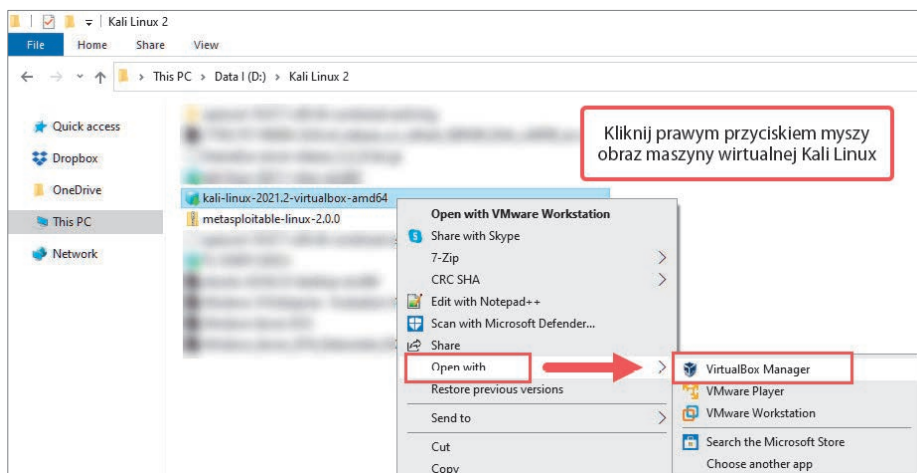
Rysunek 2.4. Obraz wirtualny systemu Kali Linux

2. Kliknij obraz *VirtualBox 64*, aby pobrać plik *Kali Linux OVA*. Możesz też użyć oficjalnego łącza systemu **torrent**, pokazanego na rysunku 2.5.



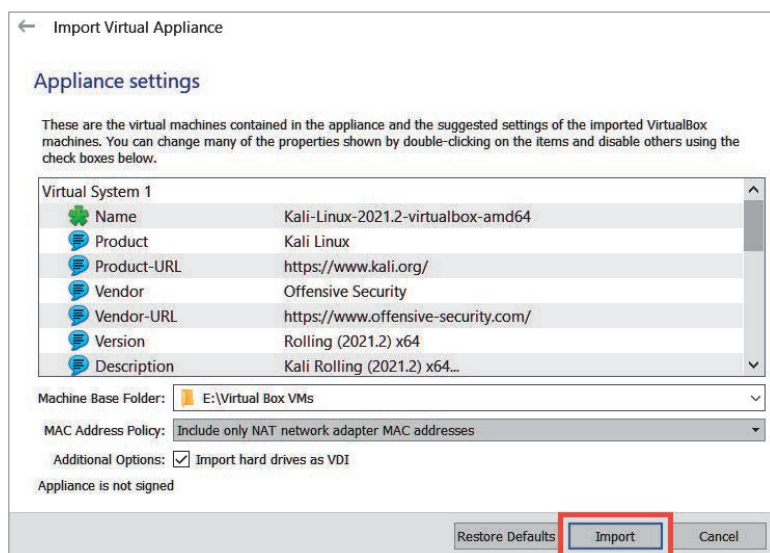
Rysunek 2.5. Pobieranie systemu Kali Linux

3. Po pobraniu pliku do systemu kliknij prawym przyciskiem myszy obraz wirtualny systemu Kali Linux, a następnie wybierz polecenie *Open with/VirtualBox Manager*, aby go zaimportować do programu VirtualBox (patrz rysunek 2.6).



Rysunek 2.6. Importowanie obrazu systemu Kali Linux

4. Na ekranie zostanie wyświetlone okno *Import Virtual Appliance* (Importuj wirtualne urządzenie), zawierające wszystkie opcje dostosowania. Kliknij przycisk *Import* (Importuj), aby rozpocząć instalację (patrz rysunek 2.7).



Rysunek 2.7. Uruchomienie instalacji

5. Kliknij przycisk *Agree* (Zaakceptuj), aby zaakceptować zasady licencji. Import potrwa kilka minut.

Po zakończeniu importu maszyna wirtualna z systemem Kali Linux będzie dostępna w programie Oracle VirtualBox Manager.

Część 2. Dostosowanie maszyny wirtualnej z systemem Kali Linux oraz kart sieciowych

Nauczysz się teraz dostosowywać środowisko wirtualne systemu Kali Linux do topologii swojego laboratorium do testów penetracyjnych. Aby poprawnie skonfigurować maszyny wirtualne z systemem Kali Linux do pracy z siecią laboratorium, wykonaj następujące kroki:

1. Wykonaj następujące polecenia w programie Windows Command Prompt, aby udostępnić maszynie wirtualnej funkcję procesora **Nested VT-x/AMD-V**:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
```

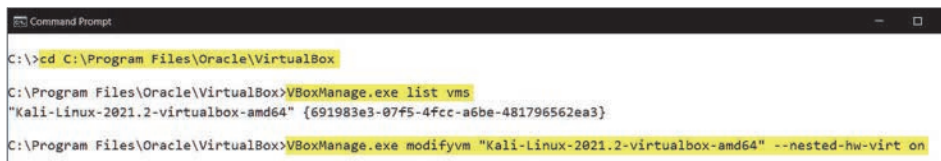
```
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
```

Polecenie to wyświetli listę nazw wszystkich maszyn wirtualnych w programie VirtualBox.

2. Użyj teraz nazwy maszyny wirtualnej z systemem Kali Linux i wykonaj następujące polecenie, aby włączyć funkcję **Nested VT-x/AMD-V** na maszynie wirtualnej:

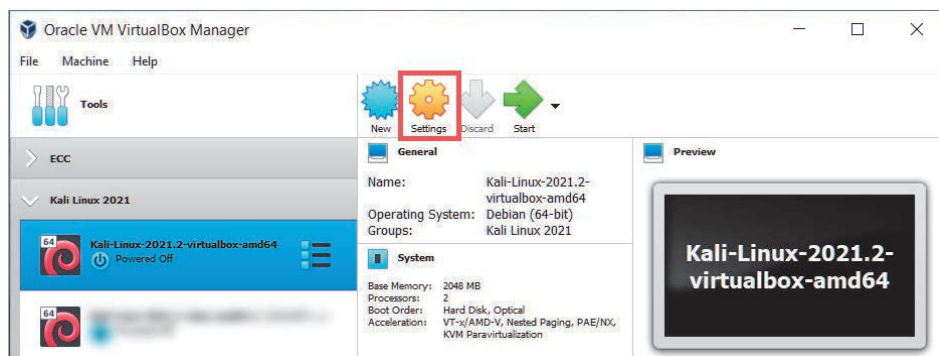
```
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "Nazwa maszyny wirtualnej" --nested-hw-virt on
```

Zastąp nazwę maszyny wirtualnej z systemem Kali Linux nazwą ujętą w cudzysłowy, jak na rysunku 2.8.

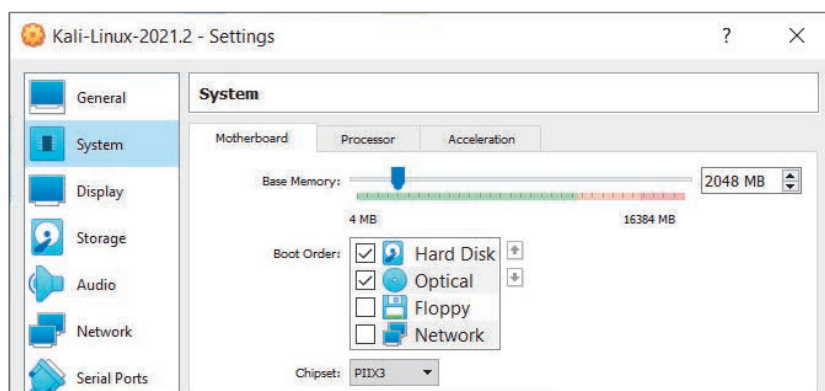


Rysunek 2.8. Włączanie zagnieżdżonej wirtualizacji na maszynie wirtualnej

3. Aby przypisać Kali Linux do każdej sieci wirtualnej, zaznacz maszynę wirtualną z systemem Kali Linux i kliknij przycisk *Settings (Ustawienia)*, jak pokazano na rysunku 2.9.
4. Wybierz *System/Motherboard/Base Memory (System/Płyta główna/RAM)*, aby dostosować ilość pamięci RAM przydzielonej do maszyny wirtualnej (patrz rysunek 2.10).



Rysunek 2.9. Wyświetlanie ustawień



Rysunek 2.10. Dostosowywanie opcji Base Memory

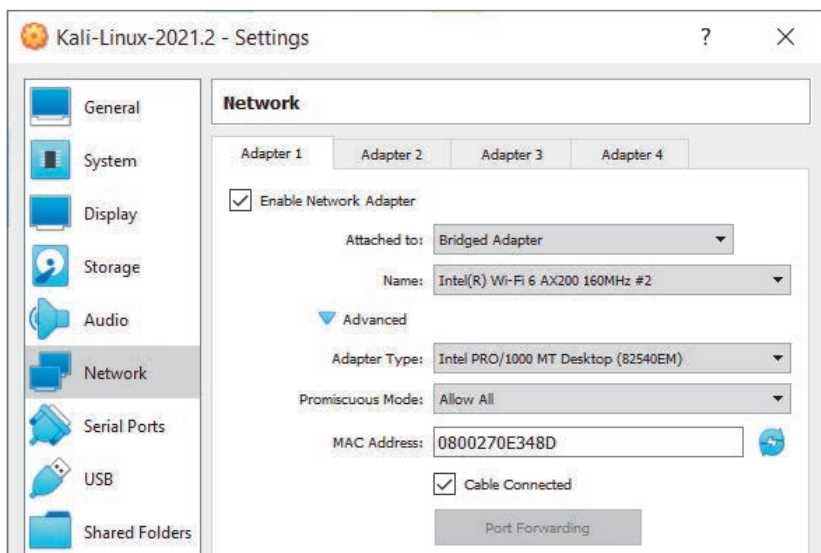
Nie zaleca się przydzielania ilości pamięci z pomarańczowego i czerwonego zakresu. Kali Linux może skutecznie działać, korzystając z 2 GB pamięci RAM; jeśli jednak w systemie masz do dyspozycji ponad 8 GB pamięci, możesz przydzielić 4 GB pamięci RAM.

W zakładce *System/Processor* (*System/Procesor*) można też dostosować liczbę rdzeni CPU, które zostaną przydzielone do maszyny wirtualnej. Wystarczy jeden lub dwa rdzenie; możesz jednak przydzielić ich więcej, jeśli pozwalają na to zasoby dostępne na komputerze.

5. Skonfiguruj bezpośredni dostęp do internetu w systemie Kali Linux. W sekcji *Settings* (*Ustawienia*) tego systemu wybierz kategorię *Network* (*Sieć*) i zakładkę *Adapter 1* (*Karta 1*). Następnie wprowadź następujące ustawienia:
 - Zaznacz opcję *Enable Network Adapter* (*Włącz kartę sieciową*).
 - *Attached to* (*Podłączona do*): *Bridged Adapter* (*Mostkowana karta sieciowa*).

- *Name (Nazwa)*: podaj nazwę karty interfejsu sieciowego swojego urządzenia, przez którą łączysz się z internetem.
- *Promiscuous Mode (Tryb nasłuchiwania)*: *Allow All (Pozwalaj wszystkim)*.

Rysunek 2.11 pokazuje konfigurację karty sieciowej.

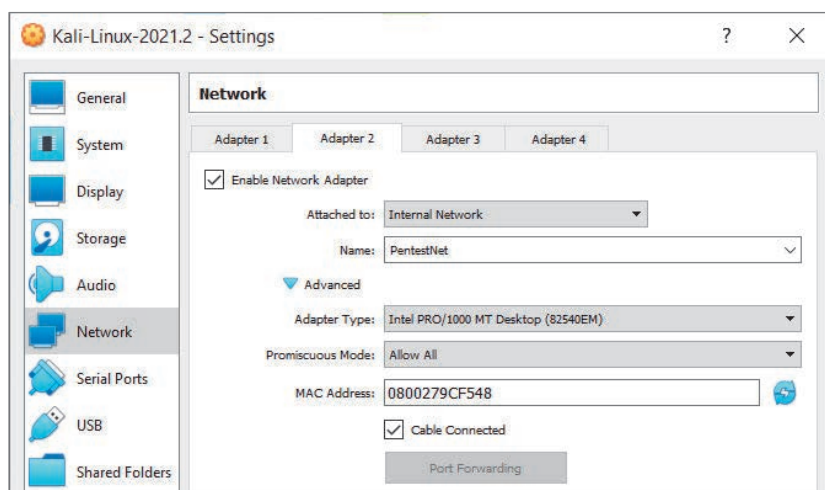


Rysunek 2.11. Karta sieciowa służąca do łączenia się z internetem

6. Przypisz sieć PentestNet do systemu Kali Linux. Wybierz zakładkę *Adapter 2* i wprowadź następujące ustawienia:
 - Zaznacz opcję *Enable Network Adapter*.
 - *Attached to*: *Internal Network (Sieć wewnętrzna)*.
 - *Name*: PentestNet.
 - *Promiscuous Mode*: *Allow All*.

Rysunek 2.12 pokazuje konfigurację karty sieciowej.

Po skonfigurowaniu zakładki *Adapter 2* usuń zaznaczenie opcji *Enable Network Adapter*, aby wyłączyć kartę. Ponieważ w programie VirtualBox będziemy korzystać z wirtualnego serwera DHCP, czasem mogą się pojawiać konflikty podczas próby połączenia jednej maszyny wirtualnej z kilkoma sieciami wirtualnymi korzystającymi z różnych wirtualnych serwerów DHCP.

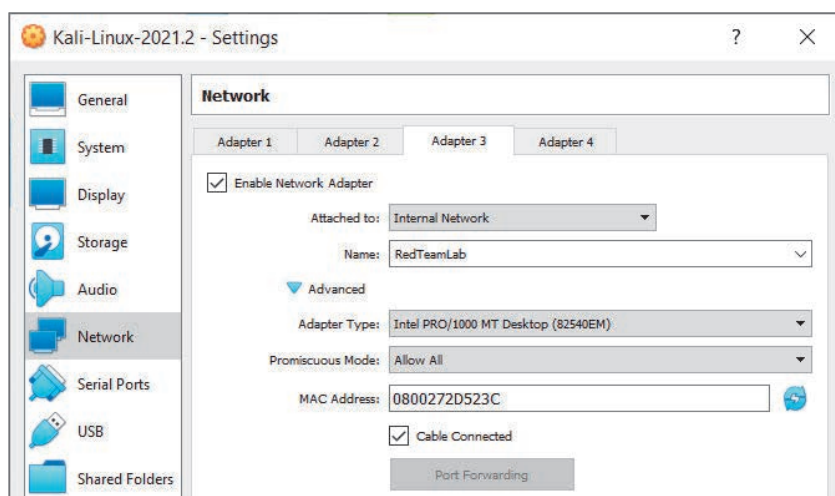


Rysunek 2.12. Przydzielanie sieci PentestNet

7. Na koniec przydziel sieć RedTeamLab do systemu Kali Linux. Wybierz zakładkę *Adapter 3* i wprowadź następujące ustawienia:

- Zaznacz opcję *Enable Network Adapter*.
- *Attached to: Internal Network*.
- *Name: RedTeamLab*.
- *Promiscuous Mode: Allow All*.

Rysunek 2.13 pokazuje konfigurację karty sieciowej.



Rysunek 2.13. Przydzielanie sieci Red Team

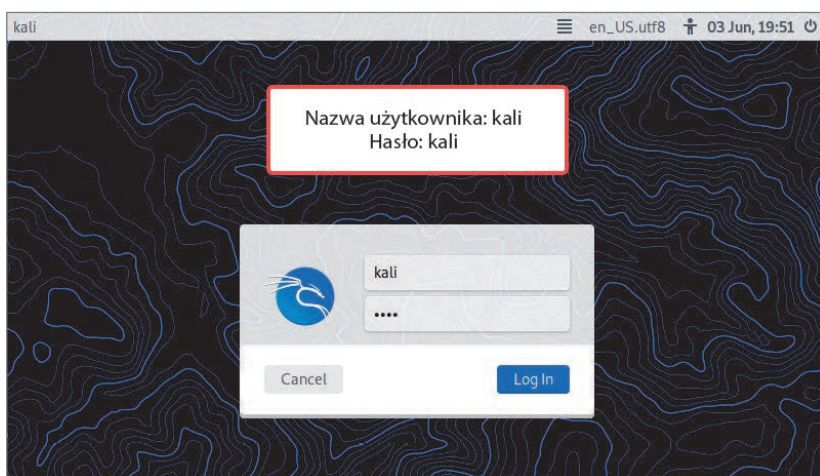
Po skonfigurowaniu zakładki *Adapter 3* usuń zaznaczenie opcji *Enable Network Adapter*, aby wyłączyć kartę sieciową. Kliknij *OK*, aby zapisać ustawienia maszyny wirtualnej.

Na tym etapie skonfigurowałeś(-łaś) wszystkie trzy karty sieciowe. Włączona pozostała tylko karta zapewniająca dostęp do internetu w maszynie wirtualnej Kali Linux; pozostałe dwie są wyłączone, aby zapobiec konfliktom.

Część 3. Początki pracy w systemie Kali Linux

Jeśli pierwszy raz korzystasz z systemu linuxowego, zalogowanie się do systemu Kali Linux może być ekscytujące. Podobnie możesz się poczuć, jeśli wiesz, że jest to jedna z najpopularniejszych dystrybucji do testów penetracyjnych w branży. Wykonaj następujące kroki, aby zacząć pracę w systemie Kali Linux:

1. W oknie *Virtual Box Manager* wybierz maszynę wirtualną z systemem Kali Linux i kliknij *Start (Uruchom)*, aby uruchomić system.
2. Na ekranie pojawi się okno logowania. Użyj domyślnej nazwy użytkownika *kali* i domyślnego hasła *kali*, jak na rysunku 2.14.

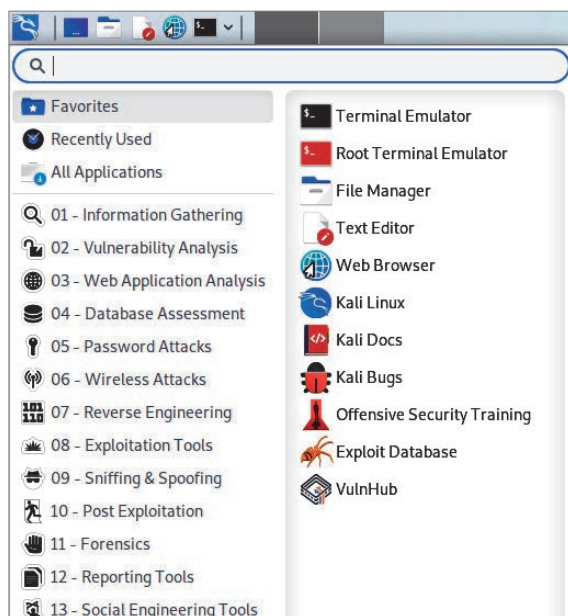


Rysunek 2.14. Okno logowania w systemie Kali Linux

Wskazówka

Jeśli ekran systemu Kali Linux nie pasuje do rozdzielczości monitora, przełącz opcję widoku w górnej części okna VirtualBox za pomocą polecenia *View/Auto-resize Guest Display* (*Widok/Automatyczne skalowanie ekranu gościa*).

3. Po zalogowaniu się kliknij ikonę Kali Linux w prawym górnym rogu okna, aby wyświetlić listę dostępnych narzędzi, taką jak na rysunku 2.15.



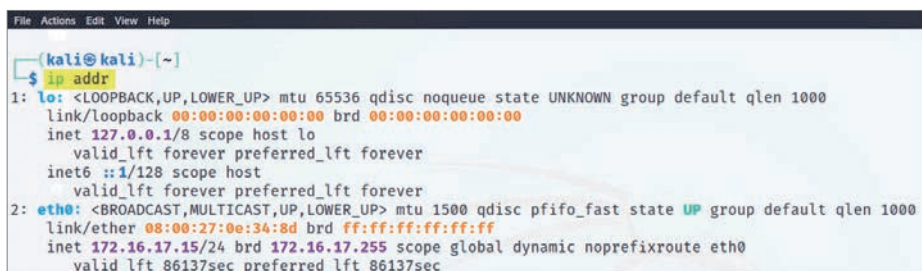
Rysunek 2.15. Lista narzędzi w systemie Kali Linux

Jak widać na zrzucie ekranu, wszystkie narzędzia są uporządkowane w kategorie odpowiadające etapom testów penetracyjnych. Na przykład wszystkie narzędzia do rekonesansu znajdują się w kategorii *01 – Information Gathering*, a narzędzia do łamania haseł — w kategorii *05 – Password Attacks*.

W tej książce zwykle korzystamy z Terminala systemu Linux. Nie przejmuj się, jeśli jeszcze tego nie robiłeś(-łaś) — nauczysz się czegoś nowego i zobaczysz, jak łatwo można używać różnych narzędzi do symulacji rzeczywistych cyberataków.

4. Sprawdź teraz, czy do maszyny wirtualnej systemu Kali Linux zostanie automatycznie przydzielony adres IP z naszej sieci za pośrednictwem karty sieciowej *Adapter 1 (Bridge)*. Otwórz Terminal i wykonaj polecenie `ip addr`, jak na rysunku 2.16.

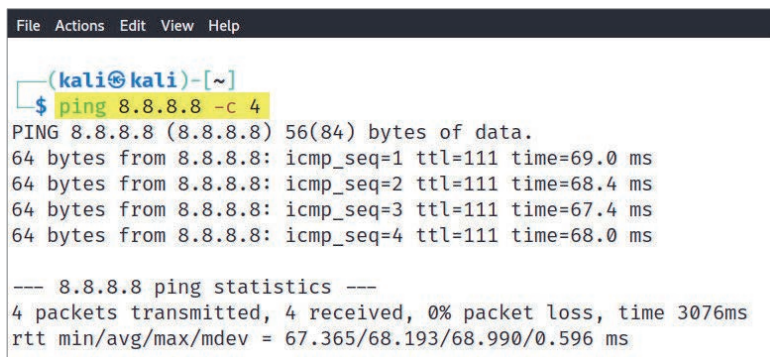
Jak widać na zrzucie ekranu, została zidentyfikowana karta sieciowa `eth0`, która ma adres IP `172.16.17.15`. Pamiętaj, że jest to adres IP z mojej sieci, a zatem Twój adres IP będzie inny. Zapamiętaj na przyszłość adresy IP swoich maszyn wirtualnych.



```
File Actions Edit View Help
(kali@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0e:34:8d brd ff:ff:ff:ff:ff:ff
    inet 172.16.17.15/24 brd 172.16.17.255 scope global dynamic noprefixroute eth0
        valid_lft 86137sec preferred_lft 86137sec
```

Rysunek 2.16. Sprawdzanie adresu IP karty sieciowej

5. Przetestuj połączenie z internetem za pomocą polecenia `ping 8.8.8.8 -c 4` (patrz rysunek 2.17). Wyśle ono cztery komunikaty ping (ICMP Echo Request) do publicznego serwera DNS witryny Google.



```
File Actions Edit View Help
(kali@kali)-[~]
$ ping 8.8.8.8 -c 4
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=69.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=68.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=67.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=68.0 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 67.365/68.193/68.990/0.596 ms
```

Rysunek 2.17. Testowanie połączenia z internetem

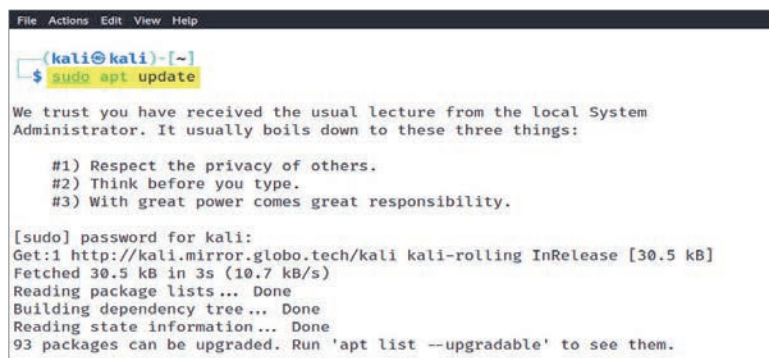
Jak widać na rysunku 2.17, Kali Linux otrzymał odpowiedzi z adresu 8.8.8.8. Oznacza to, że system agresora ma dostęp do internetu.

6. Ponieważ Kali Linux używa domyślnej nazwy użytkownika `kali` i hasła `kali`, możesz zmienić domyślne hasło na bezpieczniejsze. W tym celu użyj polecenia `passwd kali`. Podczas wpisywania hasła w systemie Linux będzie ono ukryte ze względów bezpieczeństwa.

Część 4. Aktualizowanie źródeł i pakietów

Czasem niektóre narzędzia działają niezgodnie z oczekiwaniami, a nawet ulegają zaskakującej awarii podczas testów penetracyjnych lub inspekcji zabezpieczeń. Programiści zwykle udostępniają aktualizacje swoich aplikacji. Aktualizacje obejmują poprawki błędów i nowe funkcje. Dowiesz się teraz, jak aktualizować źródła i pakiety. Wykonaj następujące kroki:

1. Aby uaktualnić pakiety oprogramowania w systemie Kali Linux, trzeba ponownie zsynchronizować indeksy pakietów. Służy do tego polecenie `sudo apt-get update`, pokazane na rysunku 2.18.



```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt update

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

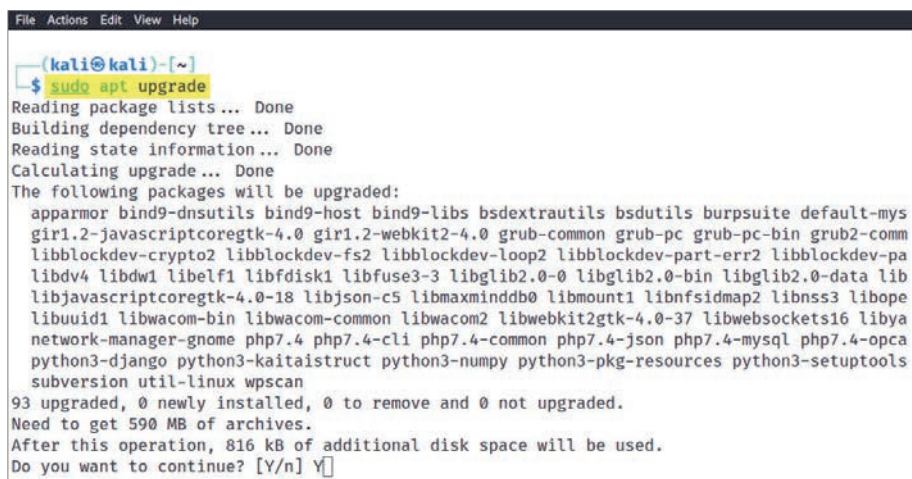
[sudo] password for kali:
Get:1 http://kali.mirror.globo.tech/kali kali-rolling InRelease [30.5 kB]
Fetched 30.5 kB in 3s (10.7 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
93 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Rysunek 2.18. Aktualizacja źródeł

Ważna uwaga

Plik `source.list` nie zawsze się poprawnie aktualizuje. Aby się upewnić, że w systemie Kali Linux skonfigurowane są właściwe ustawienia, sprawdź oficjalną dokumentację, dostępną pod adresem <https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/>.

2. Aby uaktualnić istniejące pakiety (aplikacje) w systemie Kali Linux do najnowszych wersji, wykonaj polecenie `sudo apt-get upgrade` lub `sudo apt upgrade`, jak na rysunku 2.19.



```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt upgrade

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  apparmor bind9-dnswtills bind9-host bind9-libs bsdxtrautils bsduutils burpsuite default-mys
  gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 grub-common grub-pc grub-pc-bin grub2-comm
  libblockdev-crypto2 libblockdev-fs2 libblockdev-loop2 libblockdev-part-err2 libblockdev-pa
  libdv4 libdw1 libelf1 libfdisk1 libfuse3-3 libglb2.0-0 libglb2.0-bin libglb2.0-data lib
  libjavascriptcoregtk-4.0-18 libjson-c5 libmaxminddb0 libmount1 libnfsidmap2 libnss3 libope
  libuid1 libwacom-bin libwacom-common libwacom2 libwebkit2gtk-4.0-37 libwebsockets16 libya
  network-manager-gnome php7.4 php7.4-cli php7.4-common php7.4-json php7.4-mysql php7.4-opca
  python3-django python3-kaitaistruct python3-numpy python3-pkg-resources python3-setuptools
  subversion util-linux wpscan
93 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 590 MB of archives.
After this operation, 816 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

Rysunek 2.19. Aktualizacja pakietów w systemie Kali Linux

Jeśli podczas aktualizacji zobaczysz błąd informujący, że Kali Linux nie może wykonać aktualizacji, wykonaj polecenie `sudo apt-get update --fix-missing`, a następnie — ponownie polecenie `sudo apt upgrade`.

Po przeczytaniu tego podrozdziału wiesz, jak skonfigurować maszynę wirtualną z systemem Kali Linux, skonfigurować połączenie maszyny wirtualnej z internetem i z innymi sieciami, a także uaktualnić listę źródeł repozytorium pakietów. Następnie dowiesz się, jak dodać podatnych klientów do laboratorium do testów penetracyjnych.

Wdrażanie podatnego na atak systemu Metasploitable 2

Podczas tworzenia laboratorium do testów penetracyjnych trzeba uwzględnić podatne systemy, które posłużą jako cele ataku. Te systemy zawierają specjalnie skonfigurowane usługi i aplikacje z lukami w zabezpieczeniach. Dzięki temu można ćwiczyć swoje umiejętności wykrywania i wykorzystywania podatności. Bardzo popularnym systemem z podatnościami jest Metasploitable 2. Zawiera on wiele podatności, które można wykorzystać, i świetnie nadaje się do nauki testów penetracyjnych.

Zaczynamy!

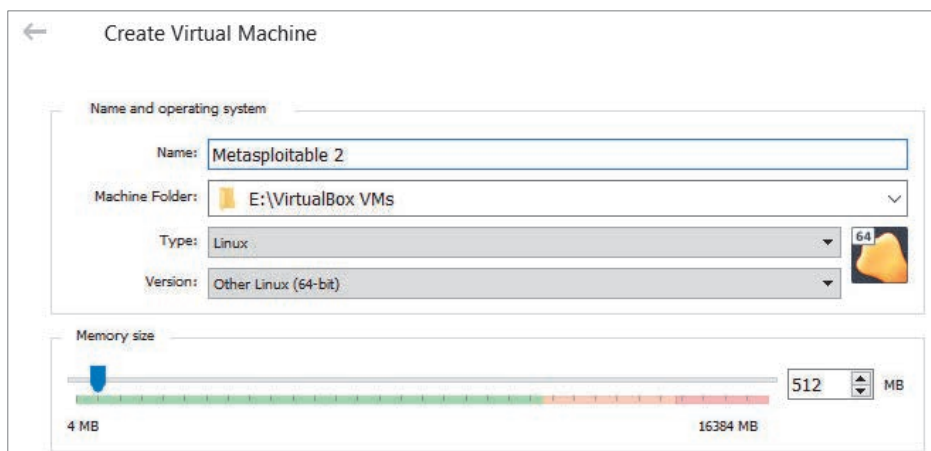
Część 1. Wdrażanie systemu Metasploitable 2

Wykonaj następujące kroki, aby pobrać maszynę wirtualną systemu Metasploitable 2 i wdrożyć w hipernadzorcy:

1. Otwórz stronę
<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
i pobierz plik *metasploitable-linux- 2.0.0.zip* do systemu hosta.
2. Po pobraniu pliku ZIP rozpakuj jego zawartość do folderu, w którym znajdują się pozostałe maszyny wirtualne. Wyodrębnione pliki są plikami wirtualnego dysku twardego systemu Metasploitable 2.
3. Utwórz środowisko wirtualne, aby wdrożyć maszynę wirtualną z systemem Metasploitable 2. W tym celu otwórz program VirtualBox Manager i kliknij *New (Nowa)*.
4. Na ekranie pojawi się okno *Create Virtual Machine (Utwórz wirtualną maszynę)*. Kliknij *Expert Mode (Tryb eksperta)*, aby zmienić okno konfiguracji.
5. Użyj następujących wartości, aby utworzyć środowisko wirtualne:
 - *Name*: Metasploitable 2,
 - *Type (Typ)*: Linux,

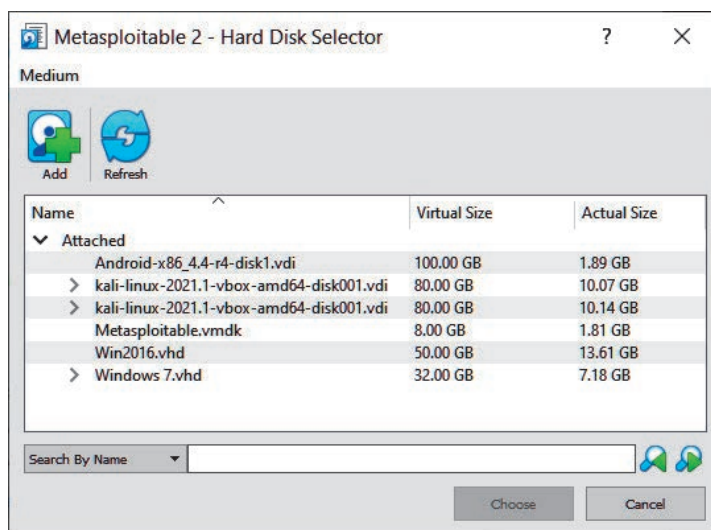
- *Version (Wersja): Other Linux (64-bit),*
- *Memory size (Rozmiar pamięci): 512 MB.*

Szczegóły te są widoczne na rysunku 2.20.



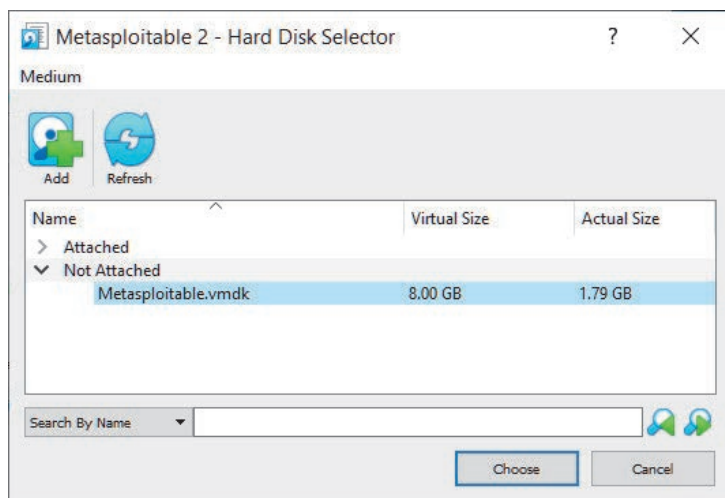
Rysunek 2.20. Tworzenie maszyny wirtualnej

6. W tym samym oknie *Create Virtual Machine* przełącz opcję *Hard disk (Dysk twardy)* na *Use an existing virtual hard disk file (Użyj istniejącego pliku wirtualnego dysku twardego)* i kliknij ikonę folderu z prawej strony, aby otworzyć okno *Hard Disk Selector* widoczne na rysunku 2.21.



Rysunek 2.21. Hard Disk Selector

7. Kliknij *Add (Dodaj)* i odszukaj folder, w którym umieściłeś(-łaś) pliki wydodrężnione w kroku 2. Wybierz plik wirtualnego dysku twardego o nazwie *Metasploitable* i kliknij *Open (Otwórz)*.
8. Następnie zaznacz plik *Metasploitable.vmdk* i kliknij *Choose*, jak na rysunku 2.22.



Rysunek 2.22. Dodawanie wirtualnego dysku twardego

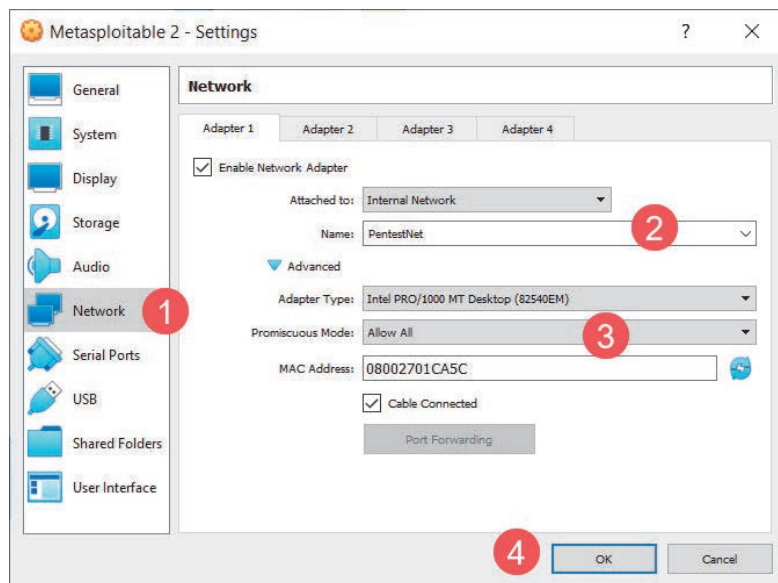
9. Powróć do okna *Create Virtual Machine* z dołączonym wirtualnym dyskiem twardym. Kliknij *Create (Utwórz)*.

Część 2. Konfigurowanie ustawień sieciowych

Ponieważ laboratorium do testów penetracyjnych zawiera kilka sieci wirtualnych, trzeba odpowiednio skonfigurować połączenie między maszyną wirtualną z systemem Kali Linux a maszyną Metasploitable 2:

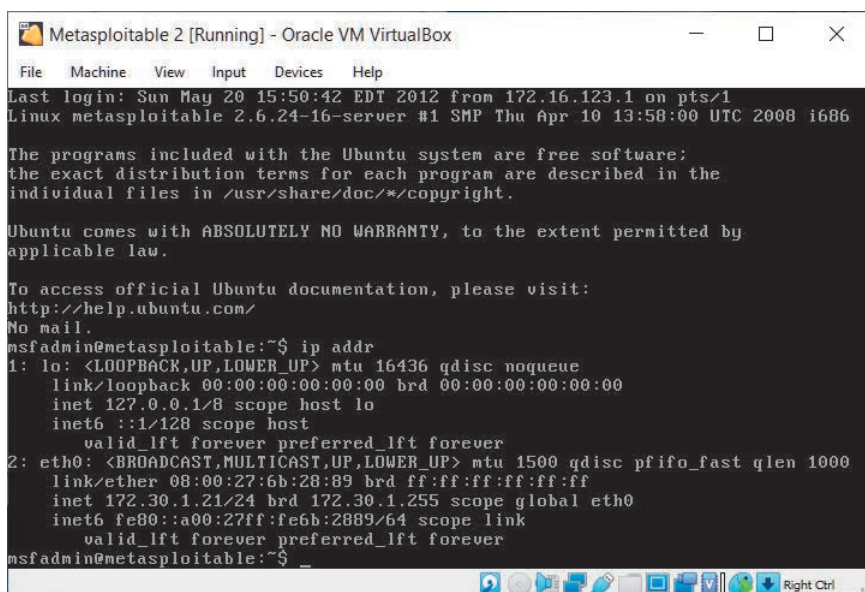
1. Aby skonfigurować ustawienia sieciowe, zaznacz maszynę wirtualną Metasploitable2 w programie VirtualBox Manager i kliknij *Settings*.
2. Przejdź do sekcji *Network* i zakładki *Adapter 1*, włącz kartę sieciową i wprowadź następujące ustawienia, aby dodać ją do sieci PentestNet należącej do laboratorium:
 - *Attached to: Internal Network*,
 - *Name: PentestNet*,
 - *Promiscuous Mode: Allow All*.

Rysunek 2.23 pokazuje ustawienia sieciowej karty wirtualnej.



Rysunek 2.23. Konfiguracja karty sieciowej

3. Uruchom maszynę wirtualną Metasploitable 2 i zaloguj się w niej, wpisując **msfadmin** w polach nazwy użytkownika i hasła. Wykonaj polecenie **ip addr**, aby sprawdzić, czy maszyna wirtualna otrzymała adres IP w sieci 172.30.1.0/24, tak jak na rysunku 2.24.



Rysunek 2.24. Sprawdzanie połączenia z siecią

4. Gdy skończysz pracę w systemie Metasploitable 2, wykonaj polecenie `sudo halt`, aby wyłączyć zasilanie maszyny wirtualnej.

Po przeczytaniu tego podrozdziału wiesz, jak skonfigurować maszynę wirtualną z podatnym na ataki systemem Metasploitable 2, dodając ją do laboratorium do testów penetracyjnych. W dalszych częściach książki będziesz rozbudowywać to laboratorium, dodając nowe systemy z podatnościami. W następnym podrozdziale dowiesz się, jak za pomocą Vagranta zaimplementować system Metasploitable 3 w środowisku laboratorium.

Implementacja systemu Metasploitable 3 za pomocą Vagranta

W tym podrozdziale zobaczysz, jak za pomocą Vagranta utworzyć maszyny wirtualne z dwiema wersjami podatnego na ataki systemu Metasploitable 3. Jest to najnowsza wersja podatnych na ataki maszyn wirtualnych z linii Metasploitable, opracowanych przez Rapid7. Można w nich ćwiczyć przeprowadzanie testów penetracyjnych i ocenę podatności. Dostępne są wersje dla systemów Windows oraz Linux.

Zaczynamy!

Część 1. Konfigurowanie wersji dla systemu Windows

Wykonaj następujące kroki, aby skonfigurować Metasploitable 3 w systemie Windows.

1. Otwórz stronę <https://www.vagrantup.com/downloads>, pobierz program **Vagrant 2.2.17** i zainstaluj go na komputerze.
2. Po zainstalowaniu Vagranta zostaniesz poproszony o ponowne uruchomienie systemu; zrób to.
3. Po ponownym uruchomieniu systemu otwórz program Windows Command Prompt i wykonaj następujące polecenia, aby zainstalować dodatki Vagrant Reload i vbguest:

```
C:\Users\Slayer> vagrant plugin install vagrant-reload
```

```
C:\Users\Slayer> vagrant plugin install vagrant-vbguest
```

Rysunek 2.25 przedstawia zrzut ekranu z oczekiwanym wynikiem po zainstalowaniu dodatków.

```
C:\Users\Slayer>vagrant plugin install vagrant-reload
Installing the 'vagrant-reload' plugin. This can take a few minutes...
Fetching vagrant-reload-0.0.1.gem
Installed the plugin 'vagrant-reload (0.0.1)!'

C:\Users\Slayer>vagrant plugin install vagrant-vbguest
Installing the 'vagrant-vbguest' plugin. This can take a few minutes...
Fetching micromachine-3.0.0.gem
Fetching vagrant-vbguest-0.30.0.gem
Installed the plugin 'vagrant-vbguest (0.30.0)!'
```

Rysunek 2.25. Instalowanie dodatków Vagranta

4. Wykonaj teraz następujące polecenia, aby za pomocą Vagranta zainstalować Metasploitable 3 z systemem Windows Server 2008:

```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-win2k8
```

5. Następnie wybierz opcję 1, jak na rysunku 2.26, aby wybrać hipernadzorcę VirtualBox.

```
C:\Users\Slayer>vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
      box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
```

Wpisz 1 i naciśnij Enter

Rysunek 2.26. Wybieranie hipernadzorczy

Vagrant pobierze Metasploitable 3 dla systemu Windows z repozytorium online, co widać na rysunku 2.27.

```
C:\Users\Slayer>vagrant box add rapid7/metasploitable3-win2k8
==> box: Loading metadata for box 'rapid7/metasploitable3-win2k8'
      box: URL: https://vagrantcloud.com/rapid7/metasploitable3-win2k8
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

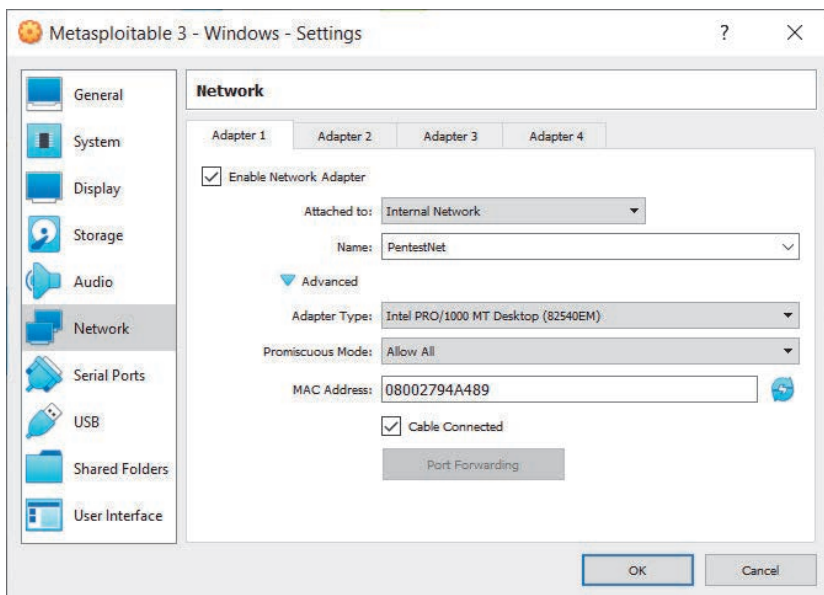
1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
==> box: Adding box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for provider: virtualbox
      box: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-win2k8/versions/0.1.0-weekl
y/providers/virtualbox.box
==> box: Box download is resuming from prior download progress
      box:
==> box: Successfully added box 'rapid7/metasploitable3-win2k8' (v0.1.0-weekly) for 'virtualbox'!
```

Rysunek 2.27. Pobieranie systemu Metasploitable 3

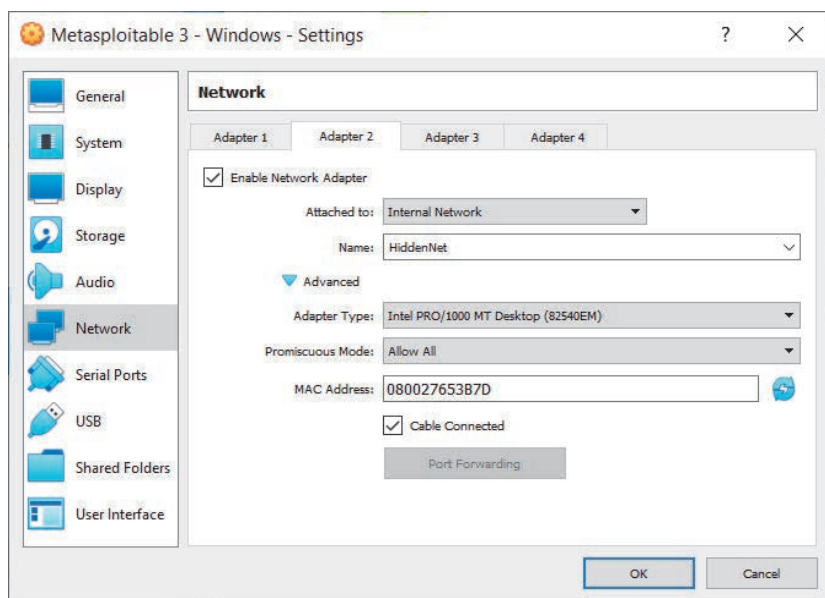
6. Otwórz program Windows Explorer, przejdź do folderu `C:\Users\username\.vagrant.d\boxes` i zmień nazwę folderu `rapid7-VAGRANTSLASH-metasploitable3-win2k8` na `metasploitable3-win2k8`.
7. Wróć do programu Windows Command Prompt, przejdź do folderu, do którego został pobrany Metasploitable 3 dla systemu Windows, i uruchom inicjalizację za pomocą następujących poleceń:

```
C:\Users\Slayer> cd .vagrant.d\boxes  
C:\Users\Slayer\.vagrant.d\boxes> vagrant init metasploitable3-win2k8  
C:\Users\Slayer\.vagrant.d\boxes> vagrant up
```
8. Metasploitable 3 dla systemu Windows po zakończeniu konfiguracji będzie dostępny w programie VirtualBox Manager. Zmień nazwę maszyny wirtualnej, połącz ją z siecią wirtualną PentestNet i upewnij się, że opcja *Promiscuous Mode* ma wartość *Allow All* (patrz rysunek 2.28).



Rysunek 2.28. Ustawienia sieciowe systemu Metasploitable 3

9. Włącz kartę sieciową *Adapter 2* i połącz ją z siecią wirtualną *HiddenNet* oraz ustaw opcję *Promiscuous Mode* na *Allow All*, jak pokazano na rysunku 2.29. Ponieważ ta maszyna wirtualna ma połączenie typu dual-homed, tworzy most między sieciami 172.30.1.0/24 i 10.11.12.0/24.



Rysunek 2.29. Połączenie sieciowe typu dual-homed

10. Na koniec upewnij się, że maszyna wirtualna z systemem Kali Linux jest połączona z maszyną wirtualną z systemem Metasploitable 3 dla systemu Windows. W tym celu wyślij komunikat ping między tymi systemami.

Ważna uwaga

Więcej informacji o lukach w zabezpieczeniach systemu Metasploitable 3 znajdziesz w oficjalnym repozytorium GitHub, dostępnym pod adresem <https://github.com/rapid7/metasploitable3/wiki/Vulnerabilities>.

Oto nazwy użytkowników i hasła dostępu do maszyny wirtualnej Metasploitable 3:

- użytkownik: Administrator, hasło: vagrant,
- użytkownik: vagrant, hasło: vagrant.

Teraz dowiesz się, jak za pomocą Vagranta wdrożyć Metasploitable 3 dla Linuksa.

Część 2. Konfiguracja wersji dla Linuksa

Wykonaj następujące kroki, aby skonfigurować Metasploitable 3 dla Linuksa w naszym laboratorium.

1. Upewnij się, że wykonałeś(-łaś) na komputerze kroki 1. – 3. z poprzedniego punktu.
2. Wykonaj następujące polecenia, aby za pomocą Vagranta zainstalować w swoim systemie Metasploitable 3 dla Linuksa.

```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-ub1404
```

3. Wybierz opcję 1, jak pokazano na rysunku 2.30, aby wybrać hipernadzorcę VirtualBox.

```
C:\Users\Slayer> vagrant box add rapid7/metasploitable3-ub1404
==> vagrant: A new version of Vagrant is available: 2.2.18 (installed version: 2.2.17)!
==> vagrant: To upgrade visit: https://www.vagrantup.com/downloads.html

==> box: Loading metadata for box 'rapid7/metasploitable3-ub1404'
      box: URL: https://vagrantcloud.com/rapid7/metasploitable3-ub1404
This box can work with multiple providers! The providers that it
can work with are listed below. Please review the list and choose
the provider you will be working with.

1) virtualbox
2) vmware
3) vmware_desktop

Enter your choice: 1
```

Wpisz 1 i naciśnij Enter

Rysunek 2.30. Wybór hipernadzorki

Vagrant rozpocznie pobieranie systemu Metasploitable 3 dla Linuksa z repozytorium online.

4. Otwórz program Windows Explorer, przejdź do folderu `C:\Users\username\.vagrant.d\boxes` i zmień nazwę folderu `rapid7-VAGRANTSLASH-metasploitable3-ub1404` na `metasploitable3-ub1404`.

Wskazówka

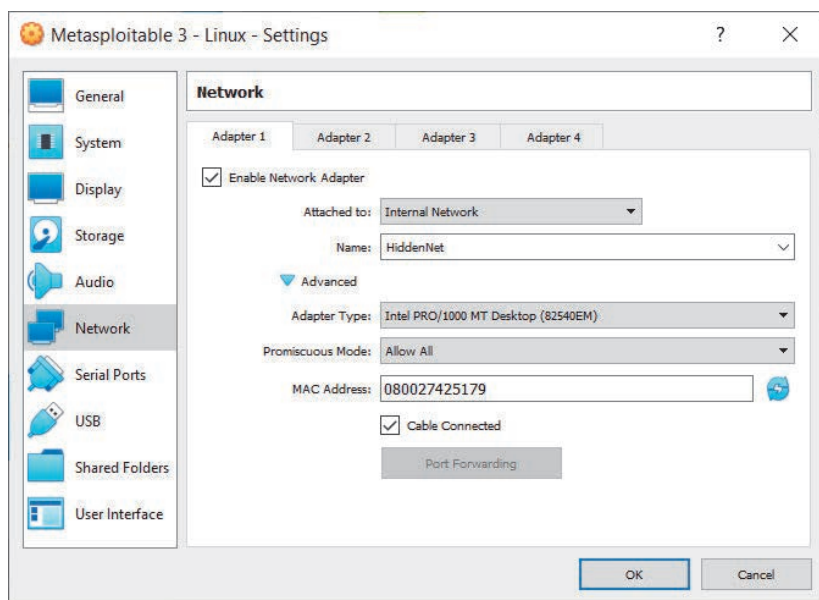
Możliwe, że zanim przejdiesz do następnego kroku, będziesz musiał(a) otworzyć program Virtual Manager.

5. Otwórz program Windows Command Prompt i przejdź do folderu, do którego Vagrant pobrał system Metasploitable dla Linuksa. Wykonaj następujące polecenia:

```
C:\Users\Slayer> cd .vagrant.d
C:\Users\Slayer\.vagrant.d> del Vagrantfile
C:\Users\Slayer\.vagrant.d> vagrant init metasploitable3-ub1404
C:\Users\Slayer\.vagrant.d> vagrant up
```

Jeśli podczas wykonywania polecenia `vagrant up` pojawią się błędy, spróbuj powtórzyć to polecenie.

W programie VirtualBox Manager po zakończeniu konfiguracji będzie dostępny system Metasploitable 3 dla Linuksa. Zmień nazwę maszyny wirtualnej, połącz ją z siecią wirtualną HiddenNet i upewnij się, że opcja *Promiscuous Mode* ma wartość *Allow All* (patrz rysunek 2.31).



Rysunek 2.31. Podłączanie do sieci wirtualnej HiddenNet

6. Na koniec upewnij się, że obydwie wersje systemu Metasploitable 3 mogą się ze sobą połączyć. W tym celu wyślij między nimi komunikat ping.

Po przeczytaniu tego podrozdziału wiesz, jak skonfigurować obydwie wersje systemu Metasploitable 3 w środowisku laboratorium. Metasploitable 3 zawiera nowsze podatności niż poprzednie wersje systemu. W dalszej części książki dowiesz się, jak je wykorzystać. W następnym podrozdziale nauczysz się wdrażać podatne na ataki aplikacje WWW do celów testów penetracyjnych.

Konfigurowanie systemów z aplikacjami WWW podatnymi na ataki

Umiejętność symulacji rzeczywistych cyberataków za pomocą systemu Kali Linux jest niewystarczająca. Trzeba też wiedzieć, jak wykrywać i wykorzystywać podatności aplikacji WWW. **Open Web Application Security Project (OWASP)** jest organizacją,

która działa na rzecz zwiększania bezpieczeństwa oprogramowania, również aplikacji internetowych. Organizacja ta publikuje znaną listę **OWASP Top 10**, na której uwzględnione są najbardziej krytyczne luki w zabezpieczeniach aplikacji internetowych.

Ważna uwaga

W czasie pisania tej książki lista OWASP Top 10 była dostępna w wersji 2017. Więcej informacji na ten temat znajduje się na stronie <https://owasp.org/www-project-top-ten/2017/>.

Aspirujący pentester powinien wiedzieć, jak zidentyfikować każdą podatność z listy OWASP Top 10. Organizacja OWASP przygotowała kilka projektów, na podstawie których można ćwiczyć techniki obronne w bezpiecznym środowisku. Korzystając z tych projektów, można się uczyć wykrywania i wykorzystywania podatności aplikacji WWW. W tym podrozdziale wdrożysz w swoim laboratorium projekty **OWASP Juice Shop** i **OWASP Broken Web Applications (BWA)**.

Zacznijmy więc wdrażać OWASP Juice Shop i OWASP BWA!

Część 1. Wdrażanie projektu OWASP Juice Shop

Wykonaj następujące kroki, aby poprawnie skonfigurować podatną na ataki aplikację internetową OWASP Juice Shop.

1. Ponieważ musisz pobrać kilka komponentów, upewnij się, że Kali Linux jest połączony z internetem.
2. Otwórz Terminal w systemie Kali Linux i wykonaj następujące polecenia, aby pobrać klucz Dockera **Pretty Good Privacy (PGP)**:

```
curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor |  
sudo tee /usr/share/keyrings/docker-archive-keyring.gpg >/dev/null
```

Na rysunku 2.32 pokazany jest oczekiwany wynik wspomnianego polecenia.

3. Wykonaj następujące polecenia, aby skonfigurować repozytorium APT Dockera w systemie Kali Linux:

```
echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-  
keyring.gpg] https://download.docker.com/linux/debian buster stable' |  
sudo tee /etc/apt/sources.list.d/docker.list
```

Rysunek 2.33 pokazuje wykonywanie tych poleceń w Terminalu.

```
File Actions Edit View Help
(kali@kali)-[~]
$ curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor
| sudo tee /usr/share/keyrings/docker-archive-keyring.gpg >/dev/null

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for kali:
(kali@kali)-[~]
$
```

Rysunek 2.32. Instalacja kluczy PGP Dockera

```
File Actions Edit View Help
(kali@kali)-[~]
$ echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian buster stable' | sudo tee
/etc/apt/sources.list.d/docker.list
deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/debian buster stable
(kali@kali)-[~]
$
```

Rysunek 2.33. Konfigurowanie repozytorium Dockera

4. Wykonaj następujące polecenie, aby uaktualnić listę źródłową repozytorium w systemie Kali Linux:

```
sudo apt-get update
```

5. Można już zainstalować Dockera w systemie Kali Linux. Wykonaj następujące polecenie:

```
sudo apt install -y docker-ce docker-ce-cli containerd.io
```

Na rysunku 2.34 pokazane są oczekiwane wyniki wspomnianych poleceń.

6. Na tym etapie Docker jest zainstalowany w systemie Kali Linux. Wykonaj to polecenie, aby pobrać kontener Dockera z aplikacją OWASP Juice Shop:

```
sudo docker pull bkimminich/juice-shop
```

Na rysunku 2.35 widać, że kontener Dockera z aplikacją OWASP Juice Shop został pobrany.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install -y docker-ce docker-ce-cli containerd.io
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  docker-ce-rootless-extras docker-scan-plugin libslirp0 pigz slirp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras
  docker-scan-plugin libslirp0 pigz slirp4netns
0 upgraded, 8 newly installed, 0 to remove and 93 not upgraded.
Need to get 108 MB of archives.
```

Rysunek 2.34. Instalowanie Dockera w systemie Kali Linux

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
ddad3d7c1e96: Pull complete
3a8370f05d5d: Pull complete
71a8563b7fea: Pull complete
119c7e14957d: Pull complete
cc14223d9a87: Pull complete
1b6803f21605: Pull complete
3dbea8a23ca4: Pull complete
4a9468a1f264: Pull complete
Digest: sha256:9dde4f70f060d58dc83a3fa53f4f9ad89cf7a38858ecffdc1d74289a14c61465
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
(kali@kali)-[~]
$
```

Pobieranie może
potrwać kilka minut

Rysunek 2.35. Kontener Dockera z aplikacją OWASP Juice Shop

- Wykonaj następujące polecenie, aby uruchomić w Dockerze aplikację OWASP Juice Shop:

```
sudo docker run --rm -p 3000:3000 bkimminich/juice-shop
```

Na rysunku 2.36 widać, że Docker uruchamia kontener OWASP Juice Shop.

Aby w dowolnym czasie zatrzymać działanie kontenera, użyj skrótu *Ctrl+Q* lub samego klawisza *Q*.

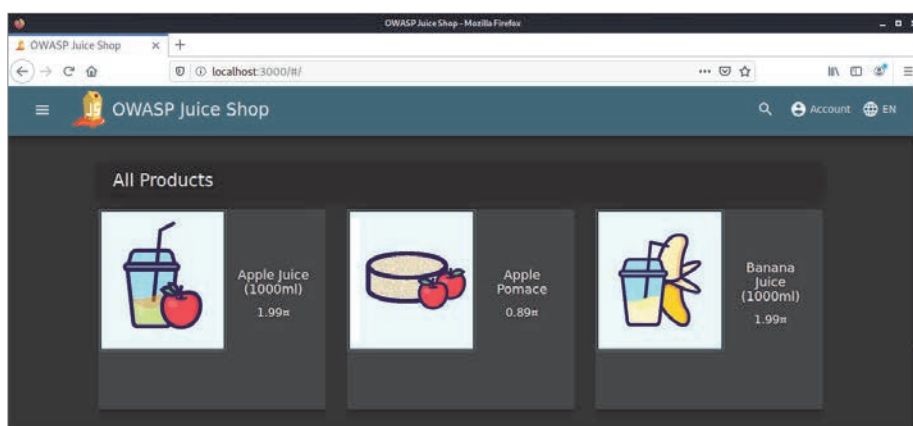
- Aby wyświetlić interfejs aplikacji OWASP Juice Shop, otwórz przeglądarkę internetową w systemie Kali Linux i przejdź pod adres *http://localhost:3000/*, jak na rysunku 2.37.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

> juice-shop@12.8.0 start /juice-shop
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v12.22.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file styles.css is present (OK)
info: Required file main-es2018.js is present (OK)
info: Required file tutorial-es2018.js is present (OK)
info: Required file polyfills-es2018.js is present (OK)
info: Required file runtime-es2018.js is present (OK)
info: Required file vendor-es2018.js is present (OK)
info: Required file main-es5.js is present (OK)
info: Required file tutorial-es5.js is present (OK)
info: Required file polyfills-es5.js is present (OK)
info: Required file runtime-es5.js is present (OK)
info: Required file vendor-es5.js is present (OK)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```

Rysunek 2.36. Uruchamianie kontenera Dockera z aplikacją OWASP Juice Shop



Rysunek 2.37. Interfejs użytkownika aplikacji OWASP Juice Shop

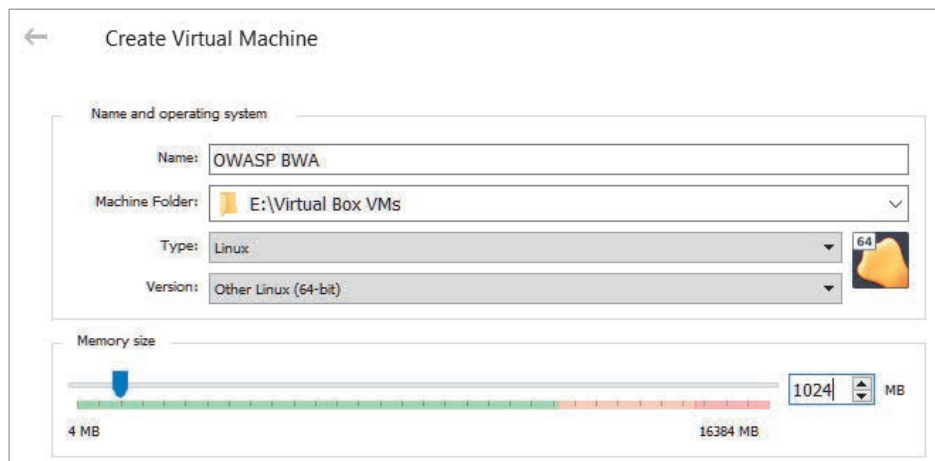
Następnie utworzysz maszynę wirtualną z projektem OWASP Broken Web Applications w laboratorium do testów penetracyjnych.

Część 2. Konfigurowanie projektu OWASP Broken Web Applications

Wykonaj następujące kroki, aby wdrożyć maszynę wirtualną z systemem OWASP Broken Web Applications, czyli dodatkową platformę z podatnościami, w której będziesz ćwiczyć swoje umiejętności:

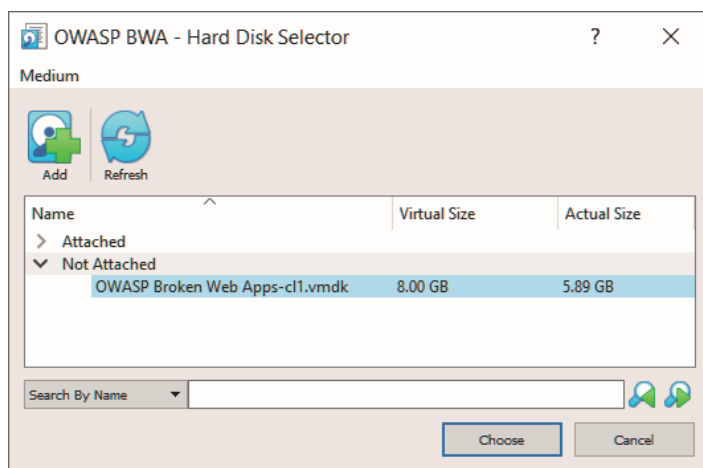
1. Otwórz stronę <https://sourceforge.net/projects/owaspbwa/files/> i pobierz system **OWASP Broken Web Applications** w wersji 1.2.
2. Rozpakuj plik *OWASP_Broken_Web_Apps_VM_1.2.7z* za pomocą aplikacji 7-Zip. Skopiuj wyodrębnioną zawartość (wirtualny dysk twardy) do katalogu z pozostałymi maszynami wirtualnymi.
3. Utwórz środowisko wirtualne, w którym wdrożysz maszynę wirtualną OWASP Broken Web Applications. Otwórz program VirtualBox Manager i kliknij *New*.
4. W oknie *Create Virtual Machine* kliknij *Expert Mode*, aby zmienić podgląd konfiguracji.
5. Wprowadź następujące ustawienia środowiska wirtualnego:
 - *Name*: OWASP BWA,
 - *Type*: Linux,
 - *Version*: Other Linux (64-bit),
 - *Memory size*: 1024 MB.

Rysunek 2.38 pokazuje gotowe ustawienia.



Rysunek 2.38. Maszyna wirtualna OWASP BWA

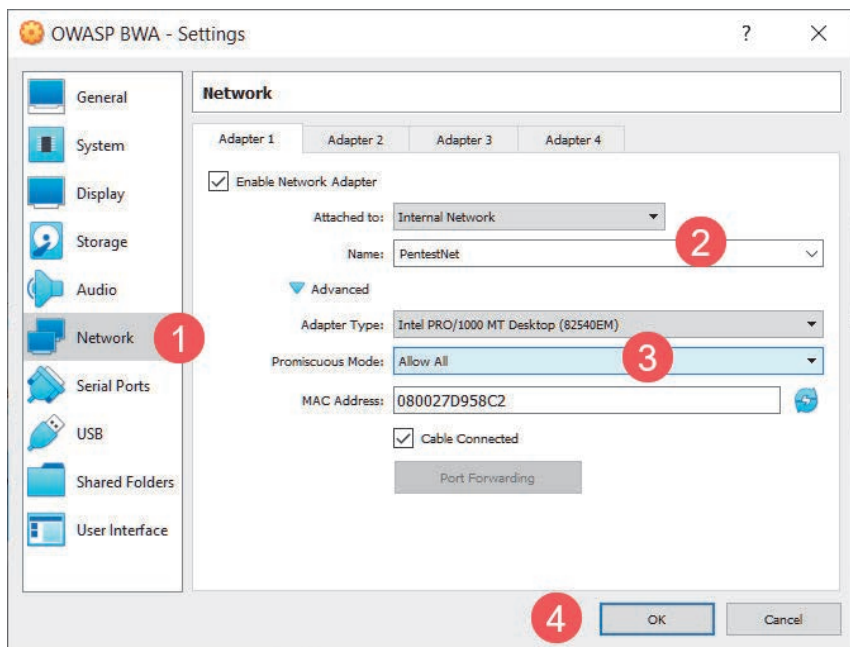
6. W tym samym oknie *Create Virtual Machine* zmień wartość opcji *Hard disk* na *Use an existing virtual hard disk file* i kliknij ikonę folderu z prawej strony, aby otworzyć okno *Hard Disk Selector*.
7. Kliknij *Add* i przejdź do folderu, w którym znajdują się rozpakowane pliki z kroku 2. Wybierz plik dysku twardego *OWASP Broken Web Apps-cl1* i kliknij *Open*.
8. Zaznacz plik *OWASP Broken Web Apps-cl1.vmdk* i kliknij *Choose*, jak na rysunku 2.39.



Rysunek 2.39. Wybieranie pliku dysku wirtualnego

9. Powrócisz do okna *Create Virtual Machine* z dołączonym wirtualnym dyskiem twardym. Kliknij *Create*.
10. Zaznacz nową maszynę wirtualną OWASP BWA w programie VirtualBox Manager i kliknij ikonę *Settings*.
11. Przejdź do sekcji *Network*, włącz kartę sieciową *Adapter 1* i wprowadź następujące ustawienia, aby dodać tę kartę do sieci PentestNet z naszego laboratorium:
 - *Attached to: Internal Network*,
 - *Name: PentestNet*,
 - *Promiscuous Mode: Allow All*.

Rysunek 2.40 pokazuje gotową konfigurację sieciową.



Rysunek 2.40. Konfiguracja karty sieciowej

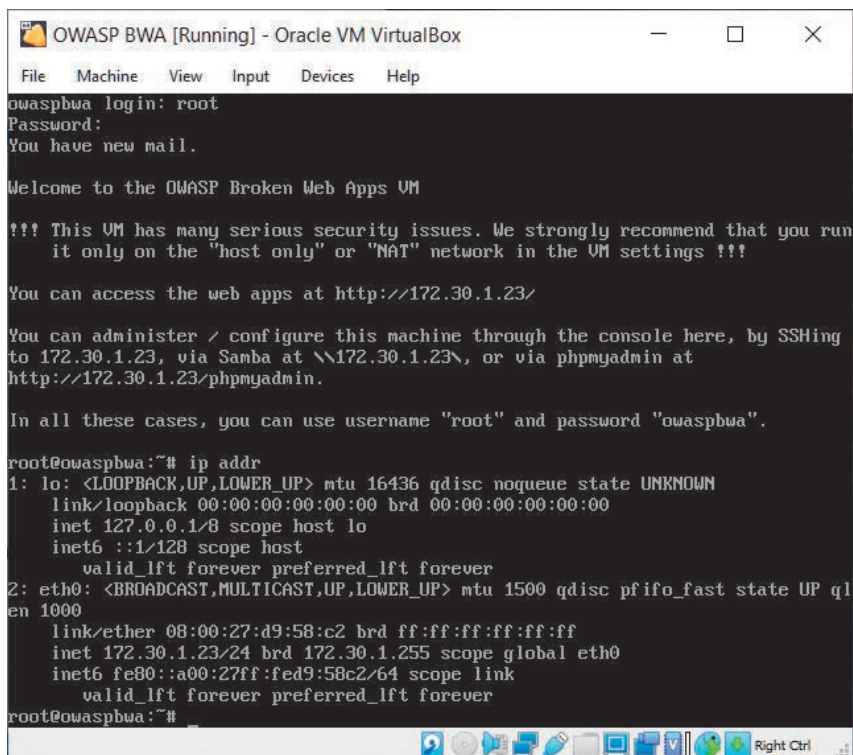
12. Uruchom maszynę wirtualną OWASP BWA; użyj nazwy użytkownika root i hasła owaspbwa. Wykonaj polecenie `ip addr`, aby sprawdzić, czy maszyna wirtualna otrzymała adres IP z sieci 172.30.1.0/24, tak jak na rysunku 2.41.

13. Na koniec wyłącz maszynę wirtualną OWASP BWA poleceniem `sudo halt`.

Po przeczytaniu tego podrozdziału wiesz, jak skonfigurować środowiska z podatnymi na ataki aplikacjami WWW i dodać je do laboratorium. Skorzystasz z nich podczas nauki testów penetracyjnych aplikacji internetowych.

Podsumowanie

W tym rozdziale dowiedziałeś(-łaś) się, jak ważne jest zbudowanie laboratorium do testów penetracyjnych na swoim komputerze. Nauczyłeś(-łaś) się korzystać z hipernadzorczy w celu wirtualizacji zasobów sprzętowych w systemie. Dzięki temu może z nich korzystać wiele systemów operacyjnych uruchomionych jednocześnie w tym samym systemie. Ponadto skonfigurowałeś(-łaś) maszynę z systemem Kali Linux, aby służyła do przeprowadzania testów penetracyjnych w podatnych na ataki systemach, np. Metasploitable 2, oraz w platformie z aplikacjami WWW, takimi jak OWASP Juice Shop i OWASP BWA.



```
OWASP BWA [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
owaspbwa login: root
Password:
You have new mail.

Welcome to the OWASP Broken Web Apps VM

!!! This VM has many serious security issues. We strongly recommend that you run
it only on the "host only" or "NAT" network in the VM settings !!!

You can access the web apps at http://172.30.1.23/

You can administer / configure this machine through the console here, by SSHing
to 172.30.1.23, via Samba at \\172.30.1.23\\, or via phpmyadmin at
http://172.30.1.23/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP ql
en 1000
    link/ether 08:00:27:d9:58:c2 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.23/24 brd 172.30.1.255 scope global eth0
        inet6 fe80::a00:27ff:fed9:58c2/64 scope link
            valid_lft forever preferred_lft forever
root@owaspbwa:~#
```

Rysunek 2.41. Sprawdzanie połączenia sieciowego

Mam nadzieję, że w tym rozdziale zdobyłeś(-łaś) wiele informacji, które pomogą Ci w nauce testów penetracyjnych, symulacji rzeczywistych cyberataków w celu wykrywania luk w zabezpieczeniach oraz wykonywaniu exploitów za pomocą systemu Kali Linux. W rozdziale 3., „Konfiguracja dla zaawansowanych technik hakerskich”, nauczysz się konfiguracji środowiska laboratorium czerwonego zespołu i poznasz zaawansowane techniki testów penetracyjnych.

Dalsza lektura

Więcej informacji o poruszanych zagadnieniach znajdziesz pod następującymi adresami:

- *Why secure web-based applications with Kali Linux?*:
<https://hub.packtpub.com/why-secure-web-based-applications-with-kali-linux/>,
- informacje o wersji 2021.2 systemu Kali Linux:
<https://www.kali.org/blog/kali-linux-2021-2-release/>.

Skorowidz |

A

- Active Directory, AD, 86, 314, 372
 - atak z użyciem protokołu LLMNR, 393
 - NetBIOS-NS, 393
 - SMB i NTLMv2, 399
- atak z wykorzystaniem Bloodhound, 387
- CME, 418
- Kerberos, 421
- Mimikatz, 423, 425
- mitm6, 412, 414, 417
- PowerView, 378
- ataki
 - na usługę, 371
 - zaawansowane, 408
- enumerowanie, 376
- eskalacja
 - pionowa, 421
 - pozioma, 418, 423
- klucz szkieletowy, 433
- konfigurowanie usług, 95
- luka
 - w zabezpieczeniach protokołu IPv6, 412
- modele zaufania, 375
- przejmowanie kontroli, 427
- przyłączanie klientów do domeny, 103
- srebrny bilet, 431
- złoty bilet, 428
- administrator domeny, 98
- adres
 - IP
 - zmienianie, 201
 - MAC, 192, 289
 - zmienianie, 192, 201
- agent, 450, 466
 - tworzenie, 454
- Aircrack-ng, 517
 - łamanie hasła, 497
- Airgeddon, 474, 499, 504, 508
- Airmon-ng, 482
- akceptowanie dostępu sieci, 634
- aktualizacja stanu HTTP, 571
- algorytm ROT13, 576
- anonimizacja ruchu sieciowego
 - łańcuchy proxy, 127
 - TOR, 130
 - VPN, 125
- API, Application Programming Interface, 378
- aplikacja internetowa OWASP Juice Shop, 78
- aplikacje
 - internetowe podatne na atak, 53, 77, 78
 - WWW, 545
- APT, Advanced Persistent Threat, 439
- ARP, 289
- atak
 - AP-less, 492
 - cross-site request forgery, CSRF, 607, 608
 - cross-site scripting, XSS, 606, 607
 - dnia zerowego, 32
 - downgrade, 513, 514
 - doxing, 532
 - eksploit, 32, 206, 271
 - MITM, 364, 367
 - NTLM Relay, 401, 412
 - pharming, 530
 - phishing, 530
 - przez anulowanie uwierzytelnienia, 487, 516
 - przez wstrzykiwanie SQL, 561, 562
 - ransomware WannaCry, 304
 - reflected XSS, 607, 608, 611
 - server-side request forgery, SSRF, 595
 - słownikowy, 294, 497, 514
 - SMB, 104
 - smishing, 531
 - spear phishing, 530
 - stored XSS, 607, 611, 613
 - Toll Fraud, 293
 - vishing, 531
 - water hole, 531
 - whaling, 530
- ataki
 - na hasła offline, 294
 - na hasła online, 294
 - po stronie klienta, 613
 - wykorzystujące błędy w mechanizmach kontroli dostępu, 569
 - wykorzystujące hasła, 293
 - cele, 293
 - lista hasel, 297
 - lista słów, 299

ataki

- protokół RDP, 295
 - rodzaje, 294
 - z wykorzystaniem komputerów, 530
 - taktyki wodopoju, 328
 - urządzeń mobilnych, 531
- automatyzacja ataków przez wstrzykiwanie SQL, 599
- AzureHound, 387

B

- Bash Bunny, 628
- baza danych
- SAM, 399, 420
 - WHOIS, 133
- beamforming, 477
- BeEF, 614
- bezpieczeństwo, 578
- aplikacji internetowych, 544
 - sieci bezprzewodowych, 479
- biała skrzynka, white box, 38
- biały wywiad, *Patrz* OSINT
- bind shell, 255
- tworzenie powłoki, 259
- Bloodhound, 387
- błąd otwarcia pliku, 586
- błędna konfiguracja zabezpieczeń, 578, 581
- błędy
- SQL, 565, 566
 - w mechanizmach kontroli dostępu, 569
- botnet, 439
- brute force, 294
- BSSID, Basic Service Set Identifier, 483
- Burp Suite, 551, 556
- konfiguracja pakietu, 554

C

- C2, Command and Control, 48, 438
- konfiguracja serwera Empire, 442
 - operacji, 440
 - zarządzanie użytkownikami, 445
 - zasady operacji, 439
- Censys, 157
- CeWL, 298
- chmury obliczeniowe, 212
- CME, CrackMapExec, 418, 420
- Command Prompt, 98
- CrackMapExec, 421
- Crunch, 299
- Cyber Kill Chain, 44, 120
- Command and Control, C2, 48, 438
 - dostarczanie, 46
 - działanie, 49
 - eksploatacja, 48
 - instalacja, 48
 - rekonesans, 45, 120
 - zbrojenia, 46
- cyberbezpieczeństwo
- atak dnia zerowego, 32
 - eksploit, 32
 - podatność, 31
 - ryzyko, 32
 - zagrożenie, 31
 - zasób, 31
- czarna skrzynka, black box, 39

D

- DC, Domain Controller, 86
- DNS, Domain Name System, 166, 174
- enumeracja, 177
 - odpowiedź, 175
 - rekordy, 181
 - transfer stref, 178
 - wyciek danych, 176
 - zapytanie, 175
 - zmiana ustawień, 358
- DNSEnum, 180, 181
- DNSmap, 186

DNSRecon, 177

- dołączanie do sieci, 633
- domena, 373
- struktura, 373
 - Windows, 88
 - konta użytkowników, 88
- dostęp
- do menu programu FoxyProxy, 553
 - do powłoki Windows Command Prompt, 315
 - do zdalnych systemów, 317
 - do zdalnych udziałów, 312
 - stały do hosta, 457
 - za pośrednictwem usługi SSH, 318
- doxing, 532
- drzewo, 374

E

- eksfiltracja danych, 357, 358
- eksploit, 32
- ekstrakcja danych, 361
- Empire
- emulacja zagrożeń, 455
 - konfiguracja serwera, 442
 - stałego dostępu, 457
 - nasłuchiwanie, 448
- korzystanie z agentów, 450
- model klient-serwer, 441
- posteksploatacja, 447
- tworzenie
- agenta, 454
 - stagera, 449
- zarządzanie użytkownikami, 445
- Empire 4, 440
- enumerowanie, 624
- Active Directory, 376
 - informacji SNMP, 328
 - serwerów nazw, 179
 - subdomen, 186

- DNSmap, 186
- Sublist3r, 187
- usługi, 203
- DNS, 177
- SMB, 205, 207
- SSH, 208
- użytkowników, 209
- eskalacja uprawnień, 341, 345
- ESSID, Extended Service Set Identifier, 484
- Ettercap, 367
- exe2hex, 354
- EyeWitness, 189, 190

F

- filtrowanie wyzwań, 563
- footprinting, 120, 121
- FoxyProxy, 551, 552
 - konfigurowanie programu, 552
- FreeRadius, 474
 - konfigurowanie programu, 110
- FreeRDP, 317
- FTP, File Transfer Protocol, 299

G

- generator haseł, 299, 521
- generowanie żądania HTTP, 610
- Google
 - hacking, 168–174
 - Hacking Database, 173
- GPO, Group Policy Object, 372
- GPU, Graphics Processing Unit, 631
- Greenbone Vulnerability Manager, GVM, 237

H

- Hack The Box, 635
- hakowanie
 - enumeracja, 42
 - etapy, 41

- etyczne, 25
- skanowanie, 42
- utrzymanie dostępu, 43
- uzyskanie dostępu, 43
- zacieranie śladów, 44
- zbieranie informacji, 42
- Hashcat, 308, 309, 398
- hasła
 - do sieci WPA/WPA2, 492
 - rodzaje ataków, 294
 - wymagania, 520
- High Gain Wireless B/G/N, 251
- hipernadzorca, 53
 - konfiguracja, 54
 - Oracle VM VirtualBox, 54
- honeypot, 496
 - beprzewodowy
 - tworzenie, 508
- host zainfekowany
 - eksfiltracja danych, 358
 - ekstrakcja danych, 361
 - konfiguracja środowiska, 357
 - zmiana ustawień DNS, 358
- hostapd, 494
- hunter.io, 137
- Hydra, 295, 297

I

- identyfikator
 - BSSID, 483
 - ESSID, 484
 - SID, 380
 - SSID, 483, 484
- Impacket, 316, 400, 405
- implementowanie serwera RADIUS, 107
- Instagram, 150
- instalowanie systemu
 - Windows Server 2019, 89
 - Windows 10 Enterprise, 93
- interfejs graficzny użytkownika, 458
- internet rzeczy, IoT, 153

- inżynieria społeczna, 149, 525
- ataki
 - oparte na interakcjach z ludźmi, 529
 - z wykorzystaniem komputerów, 530
 - z wykorzystaniem urządzeń mobilnych, 531
- elementy, 527
- fałszywe witryny społecznościowe, 532
- narzędzia, 535
- obrona, 533
- planowanie ataków, 534
- techniki, 535
- tworzenie urządzeń infekujących, 539
- witryny phishingowej, 536
- zasady, 526
- IoT, Internet of Things, 153
- IR, incident response, 33

J

- John the Ripper, 303

K

- kabel USB Ninja, 47
- Kali Linux
 - konfiguracja systemu, 57
- karta graficzna dedykowana, 631
- karta sieciowa, 251, 474
 - beprzewodowa, 272, 482, 489, 509
 - konfiguracja, 62, 71, 84
 - podłączanie, 274, 277
 - RTL8812AU, 277
 - sprawdzanie adresu IP, 66
 - tryby działania, 280

Kerberos
 skrót biletu TGS, 422
 zasada działania, 409
 klucz szkieletowy
 tworzenie, 433
 kodowanie plików, 354
 komunikat HTTP GET, 597
 konfigurowanie
 bezprzewodowego
 routera, 114
 hipernadzorczy, 54
 karty sieciowej, 62
 nasłuchiwanie, 448
 Nessusa, 219
 operacji C2, 440
 pakietu Burp Suite, 554
 programu FoxyProxy,
 552
 proxy, 553
 reverse shell, 261
 routera
 bezprzewodowego,
 488
 serwera Empire, 442
 systemu Kali Linux, 57
 udostępniania plików,
 101
 usług Active Directory,
 95
 zdalnego dostępu, 631
 kontroler domeny, DC, 86,
 96, 314, 372
 kradzież tokenów, 342

L

laboratorium, 52
 bezprzewodowej sieci
 firmowej, 498
 czerwonego zespołu
 Active Directory, 87
 topologia, 88, 376
 do bezprzewodowych
 testów
 penetracyjnych, 105
 komponenty, 53
 konfiguracja
 sieci wirtualnej, 56
 hipernadzorczy, 54
 systemów
 z aplikacjami
 WWW, 77

systemu agresora, 57
 systemu ofiary, 68, 72
 topologia, 54, 335
 LAN Turtle, 629
 LDAP, Lightweight
 Directory Access
 Protocol, 373
 lista OWASP, 549
 LLMNR, 393
 LSA, Local Security
 Authority, 420
 luka
 EternalBlue, 304, 305
 w usłudze
 Elasticsearch, 325
 SNMP, 328
 WinRM, 324
 w zabezpieczeniach
 protokołu IPv6, 412

Ł

ładunki
 program MSFvenom,
 263
 program Shellter, 266
 uruchamianie, 348
 łamanie hasła, 294, 308,
 309, 606
 do sieci WPA/WPA2,
 492
 programem
 aircrack-ng, 497
 łańcuchy proxy, 125–128

M

MAC Changer, 192, 193
 Maltego, 158
 maszyna wirtualna
 Ubuntu Server, 107
 Alice-PC, 403
 Bob-PC, 378, 394
 Kali Linux
 aktualizacja, 66
 dostosowanie, 60
 konfiguracja karty
 sieciowej, 62
 lista narzędzi, 65
 podłączanie
 bezprzewodowej

karty sieciowej,
 274, 277
 tworzenie, 57
 uruchamianie
 systemu, 64
 zagnieżdżanie
 wirtualizacji, 60
 Metasploitable 2
 konfigurowanie
 ustawień
 sieciowych, 70
 tworzenie, 68
 OWASP BWA
 wdrażanie, 82
 Windows 10
 Enterprise, 93
 Windows Server 2019,
 89
 kontroler domeny, 96
 tworzenie kont
 użytkowników, 98
 wyłączanie
 zabezpieczeń, 99
 media społecznościowe,
 149
 Medusa, 320
 Metasploit, 204, 244
 skanowanie, 204
 Metasploitable 2
 konfigurowanie
 ustawień sieciowych,
 70
 wdrażanie systemu, 68
 Metasploitable 3
 implementacja
 systemu, 72
 konfiguracja
 dla Linuksa, 75
 dla Windowsa, 72
 Meterpreter
 posteksploatacja, 334
 mikrokontroler ESP8266,
 627
 Mimikatz, 423
 mitm6, 412
 modyfikowanie
 nagłówka, 571
 żądania HTTP, 580
 MSFvenom, 404
 kodowanie ładunków,
 263

N

nagłówek
 odpowiedzi HTTP, 548
 żądania HTTP, 546
najlepsze praktyki, 620
narzędzia w systemie Kali
 Linux, 65
nasłuchiwanie, 448, 463
Ncrack, 295, 296
Nessus, 219
 analiza wyników, 225
 eksportowanie
 wyników, 230
 konfiguracja, 219
 skanowanie, 223
NetBIOS, 290
NetBIOS-NS, 393
Netcat, 257
 konfigurowanie
 zdalnych powłok, 257
Netcraft, 163
Netdiscover, 195, 288
niezabezpieczony katalog,
 586
Nikto, 247
Nmap, 195–203, 243, 289,
 318
 wykrywanie
 podatności, 232
Nmap Scripting Engine,
 201, 232, 399
 kategorie skryptów,
 232
NTLM, New Technology
 LAN Manager, 372, 409

O

obrona przed inżynierią
 społeczną, 533
odgadywanie hasła, 294
Open Web Application
 Security Project, 53
OpenVAS, 236
operacje C2, 49, 440
oprogramowanie
 wywiadowcze, 122
OSINT, Open Source
 Intelligence, 123

bazy danych WHOIS,
 133
Censys, 157
dane pracowników,
 136
Hunter.io, 137
Maltego, 158
media
 społecznościowe, 149
Netcraft, 163
Osintgram, 150
pacynka, 124
Recon-ng, 139
Sherlock, 152
Shodan, 153
Spiderfoot, 181–86
theHarvester, 147
ukrywanie swojej
 tożsamości, 125
wewnętrzna
 infrastruktura
 sieciowa, 133, 153
witryny rekrutacyjne,
 134
źródła danych, 123
Osintgram, 150
OWASP, 549
 Broken Web
 Applications, BWA,
 52, 53, 82, 600, 609
 Juice Shop, 78, 586
 Top 10, 78, 549

P

Packet Squirrel, 628
PacketWhisper, 357
pacynka, sock puppet, 124
pakiet
 Burp Suite, 551
 epilogue-js, 587
 Oracle VM VirtualBox
 Extension Pack, 55
pharming, 530
phishing, 530
pisanie raportów, 625
platforma Cyber Kill Chain,
 44
plik SAM, 306, 373
PNL, Preferred Network
 List, 484

pobieranie
 samych kolumn, 605
 tabel, 604
podatne usługi, 299
podatność, 31
podszywanie się, 342, 344
polecenia SSH, 635
polecenie
 agents, 450, 455
 aircrack-ng, 492
 airmon-ng, 482, 494,
 515
 airodump-ng, 483, 485,
 491
 arp, 350
 aws configure, 213
 back, 142, 447
 background, 307, 337,
 347, 352
 bypassuac, 451
 cat, 188, 215, 363
 cd .., 189
 cd, 339, 340
 cewl, 298
 chmod, 459
 clearev, 353
 create_user, 446
 crunch, 299
 dashboard, 144
 dir, 340
 dirb, 573
 disable_user, 446
 dnsenum
 zonetransfer.me, 180
 dnsrecon, 177
 execute, 448
 exit, 340
 exploit, 206, 271
 Find, 386
 generate, 449
 get, 313
 Get-DomainPolicy, 380
 Get-DomainSID, 380
 Get-NetComputer, 381
 Get-NetDomain
 ↪ Controller, 381
 Get-NetForest, 384
 Get-NetForestCatalog,
 385
 Get-NetGPO, 384
 Get-NetGroup, 383

- Get-NetLocalGroup, 383
- Get-NetUser, 381
- getsystem, 341, 344
- getuid, 272, 336, 341, 343
- git clone, 189
- hashcat, 397
- hashdump, 306, 336
- hashid, 307
- help, 271, 447
- host zonetransfer.me, 179
- ifconfig, 192, 193, 276
- impersonate_token, 343
- info, 141, 451
- interact, 451
- Invoke, 386
- Invoke-Bloodhound, 389
- Invoke-ShareFinder, 384
- ip addr, 65, 71, 84, 181, 194
- ipconfig, 350
- iwconfig, 276, 278, 281, 285
- keys add, 143
- keys list, 143
- keyscan_dump, 338
- keyscan_start, 338
- keyscan_stop, 338
- klist, 430
- list, 151
- list_tokens, 343
- listeners, 448, 456
- load wmap, 244
- locate proxychains, 128
- ls output, 151
- lsusb, 277
- macchanger, 192
- main, 447
- man medusa, 321
- mitm6, 413
- mkdir, 102, 215
- modules load, 141
- modules search bing, 142
- modules search report, 144
- modules search, 140, 141
- msfconsole, 205, 325
- nc, 258, 260
- net group, 99
- net user, 99
- nikto, 247
- nmap, 196, 197, 200, 296
- nslookup, 213
- option unset, 142
- options, 311, 448, 457
- passwd kali, 66
- ping, 66
- proxychains4 firefox, 130
- psinject, 454
- pth-winexe, 315
- pwd, 188, 339
- python, 260, 413
- python3 sherlock, 152
- recon-web, 146
- record_mic, 339
- route, 351
- run, 142, 206
- s3scanner, 213
- screenshare, 338
- screenshot, 338
- search, 204, 205, 339
- search elastic, 325
- search snmp_enum, 327
- search vsftpd, 301
- search winrm, 323
- searchsploit, 234
- sessions, 307, 320, 347, 541
- set Name, 448
- set Port, 448
- setspn, 102
- shell, 311, 340, 452, 455
- show contacts, 144
- show info, 235
- show options, 206
- show, 144
- slmgr, 359
- smbmap, 207
- sqlmap, 603, 604, 605
- sublist3r, 187
- sudo airgeddon, 509
- sudo bloodhound, 387
- sudo crackmapexec, 419
- sudo ettercap, 367
- sudo halt, 72
- sudo mousepad, 401
- sudo msfconsole, 404
- sudo responder, 394, 401
- sudo spiderfoot, 182
- sysinfo, 336
- theHarvester, 148
- tracert, 197
- use priv, 341
- uselistener, 448
- vagrant plugin install, 72
- vagrant up, 76
- webcam_list, 339
- webcam_snap, 339
- webcam_stream, 339
- whatweb, 242
- whoami, 311, 430
- whois, 133
- wmap_run, 246
- wmap_sites, 245
- wordlists, 295
- workspaces create, 140
- workspaces load, 140
- wpscan, 248
- posteksploatacja, 334
 - eskalacja pozioma, 349
 - eskalacja uprawnień, 341
 - główne operacje, 335
 - kradzież tokenów, 342
 - operacje w interfejsie użytkownika, 338
 - podszycanie się, 342
 - przesyłanie plików, 339
 - utrwalanie dostępu, 345
 - używanie hosta pośredniczącego, 349
 - za pomocą platformy Empire, 447
 - zacieranie śladów, 353
- PowerView, 378
- powłoka
 - pseudo-Terminala, 302

profilowanie
 systemu docelowego, 291
 systemu operacyjnego, 198
 witryn WWW
 EyeWitness, 189
programy antywirusowe
 omijanie zabezpieczeń, 262
protokół
 ARP, 195
 FTP, 198
 HTTP, 545
 zasady, 546
 ICMP, 289
 IPv6, 411
 Kerberos, 409
 LDAP, 373
 LLMNR, 393
 NetBIOS-NS, 393
 RDP, Remote Desktop Protocol, 295, 317
 SMB, Server Message Block, 156, 199, 399
 SNMP, 326
 TCP/IP, 199, 411
 WinRM, 321
proxy, 125, 127
 konfigurowanie, 553
proxychains, 130
przechwytywanie
 komunikatu HTTP
 POST, 564, 567
 pakietów, 364
 sesji zwrotnej, 348
 zadań HTTP, 570, 580
przeglądanie danych, 575
przejęcie lokalnego konta, 104
przekazywanie wartości
 skrótów, 314, 316
PsExec, 310
PTH-WinExe, 315
punkt kontaktu, point-of-contact, 141

R

ransomware, 26
raporty, 625

reagowanie na incydenty,
 IR, 33
Recon-ng, 139
rekonesans, 42, 45
 aktywny, 120
 DNS, 174
 automatyzacja
 zbierania danych, 181
 enumerowanie DNS, 177
 transfer stref DNS, 178
 footprinting, 120
 pasywny, 120
 sieci bezprzewodowej, 481
 zbieranie informacji
 aktywne, 166
 pasywne, 122
Responder, 393, 394, 402
reverse shell, 256, 404
 konfiguracja, 261
 powłoki, 406
 uzyskiwanie powłoki, 404
router bezprzewodowy
 konfiguracja, 488
rozkodowanie skrótu
 Base64, 576
rozpylanie haseł,
 password spraying, 138, 294
rozszyfrowywanie
 algorytmem ROT13, 576
ryzyko, 32

S

S3Scanner, 213, 214
SAM, Security Account Manager, 373
SDN, Software Defined Networking, 631
Server Manager, 95
serwer
 BeEF, 615
 DNS, 174, 357
 Empire, 442
 RADIUS, 107

konfigurowanie
 bezprzewodowego routera, 114
serwery
 proxy, 127
 VPN, 126
SharpHound, 387
Shellter
 kodowanie ładunków, 266
Sherlock, 152
Shodan, 153
sieci bezprzewodowe, 474
 atak AP-less, 492
 konfiguracja, 498
 określanie celu, 500
 pobieranie danych
 dostępowych, 505
 rozpoczynanie, 503
 filtrowanie, 485
 firmowe, 497, 521
 informacje, 483
 kanały, 475
 monitorowanie, 483
 rekonesans, 481
 standard
 bezpieczeństwa, 479
 WPA3, 513
 standardy, 475
 transmisja
 MIMO, 477
 MU-MIMO, 478
 SISO, 476
 SU-MIMO, 478
 tryb bezpieczeństwa
 WPA2-PSK, 488
 WPA-PSK, 488
 ustalanie klientów, 486
 włamywanie się, 488, 497
 wykrywanie ataków, 513
 zabezpieczanie, 518, 521
sieć
 TOR, 130
 wirtualna
 konfiguracja, 56
 ZeroTier, 632
skanery aplikacji
 internetowych, 242

skanowanie, 190–203
 platforma Metasploit, 204
 portów, 204, 352
 programem
 Nessus, 223
 Netdiscover, 195
 Nmap, 195
 S3Scanner, 214
 sieci, 623
 z ukrycia, 202, 203
 za pomocą komunikatów TCP SYN, 205
 zaawansowane, 198
 skrót, 314
 Base64, 576
 biletu TGS Kerberos, 422
 NTLM, 372
 NTLMv2, 397
 SMB, Server Message Block, 156, 199, 399
 SMBclient, 312
 SMBMap, 208
 smishing, 531
 SNMP, Simple Network Management Protocol, 326
 spear phishing, 530
 Spiderfoot, 181–186
 spoofing adresów MAC, 192
 sprawdzanie
 podatności, 602
 zawartości ukrytej lokalizacji, 574
 srebrny bilet
 tworzenie, 431
 SSH, 208
 SSID, Service Set Identifier, 483, 484
 SSO, Single Sign-On, 409
 stager, 449, 464
 standardy sieci
 bezprzewodowych, 475
 Starkiller, 458, 459
 dane dostępne, 468
 korzystanie z agentów, 466
 moduły, 462
 raportowanie, 468

tworzenie
 listenerów, 463
 stagerów, 464
 uruchamianie programu, 459
 zarządzanie użytkownikami, 459
 Sublist3r, 187
 switch, 630
 Sysinternals, 310
 szara skrzynka, gray box, 39
 szukanie poufnych plików, 575

Ś

świadczenie usług doradczych, 35

T

tablica trasowania, 352
 TCP
 uzgadnianie trójetapowe, 202
 Tcpdump, 366
 technika CSMA/CA, 478
 telnet, 253
 test penetracyjny, 33
 analiza podatności, 37
 aplikacji internetowych, 39
 mobilnych, 40
 bezprzewodowy, 473
 chmury, 41
 eksploatacja, 37
 etapy, 34
 faza wstępna, 35
 kontrakt, 621
 lista kontrolna, 622
 modelowanie zagrożeń, 36
 pisanie raportu, 38
 podejścia, 38
 posteksploatacja, 38
 przygotowanie, 35
 urządzeń fizycznych, 41
 witryn internetowych, 584
 z wykorzystaniem inżynierii społecznej, 40

zasady zaangażowania, 35, 622
 zbieranie informacji, 36
 testy penetracyjne sieci, 40, 251
 ataki z wykorzystaniem hasła, 293
 taktyki wodopoj, 328
 bezzprzewodowych, 272
 cele, 254
 omijanie zabezpieczeń, 262
 posteksploatacja, 333
 profilowanie systemów, 291
 technologia bind shell, 255
 reverse shell, 255
 wykrywanie systemów, 288
 zarządzanie trybami bezzprzewodowymi, 280
 znajdowanie podatności, 299
 theHarvester, 147, 148
 token delegacji, 342
 personifikacji, 342
 TOR, The Onion Router, 125, 130
 trasowanie, 352
 tryb monitorowania ręczne konfigurowanie, 280
 użycie pakietu Aircrack-ng, 283
 tryby bezzprzewodowe, 280
 TryHackMe, 635
 tworzenie agenta, 454
 bezzprzewodowego honeypota, 508
 fałszywego zdjęcia profilowego, 124

fałszywej karty
 kredytowej, 124
 fałszywej tożsamości,
 124
 klucza szkieletowego,
 434
 kont użytkowników, 98
 listenerów, 463
 listy haseł, 297
 listy słów, 299
 ładunków, 263, 266
 nowego użytkownika,
 346
 powłoki, 310
 powłoki bind shell, 259
 przybornika hakera,
 626
 sieci, 633
 sieci wirtualnych, 56
 srebrnego biletu, 431
 stagera, 449, 464
 urządzeń infekujących,
 539
 witryny phishingowej,
 536
 złotego biletu, 428

U

Ubuntu Server
 instalowanie systemu,
 107
 udostępnianie plików, 101
 umowa o zachowaniu
 poufności, 35
 unikanie wykrycia, 199
 upychanie poświadczeń,
 credential stuffing, 138,
 294
 uruchamianie ładunku, 348
 USB Rubber Ducky, 47
 usługa
 BeEF, 615
 DNS, 177
 Elasticsearch, 325
 FTP, File Transfer
 Protocol, 299
 HTTP, Hypertext
 Transfer Protocol,
 321
 LSA, 420

S3, Simple Storage
 Service, 212
 SMB, 205, 303, 304
 SSH, 208, 318
 vsFTPD, 302
 WinRM, 321
 usterki
 kryptograficzne, 573
 w integralności
 oprogramowania
 i danych, 594
 w monitorowaniu
 i rejestracji zdarzeń,
 594
 w identyfikacji, 588
 w uwierzytelnianiu,
 588, 589
 uwierzytelnianie, 101, 589
 hałaśliwe, 209
 uzyskiwanie dostępu, 568,
 624

V

Vagrant
 implementacja systemu
 Metasploitable 3, 72
 VirtualBox, 53
 Guest Additions, 91
 Manager, 377
 pakiet rozszerzeń, 55
 vishing, 531
 VPN, Virtual Private
 Network, 125, 126, 631

W

wabiki, 200
 wartość hakowania, 30
 water hole, 531
 wczytywanie złośliwej
 strony, 617
 whaling, 530
 WhatWeb, 242
 WHOIS, 133
 WiFi Pineapple Nano, 626
 Windows 10 Enterprise
 instalowanie systemu,
 93
 Windows Server 2019

 instalowanie systemu,
 89
 WinRM, Windows Remote
 Management, 321
 Wireshark, 203, 366
 wirtualna sieć prywatna,
 VPN, 125, 126, 631
 witryny rekrutacyjne, 134
 własne serwery proxy,
 127
 WPA, 488
 WPA2, 488
 WPA3
 atak typu downgrade,
 514
 nowe funkcje
 i technologie, 513
 WPSscan, 248
 wstrzykiwanie SQL, 567,
 599
 wyciek
 danych w chmurze,
 212
 danych z witryn
 rekrutacyjnych, 134
 DNS, 176
 wykrywanie
 aktywne działających
 systemów, 289
 ataków stored XSS, 611
 ataków reflected XSS,
 608
 baz danych, 599, 603
 działających systemów,
 288
 otwartych portów, 197,
 290
 pasywne hosta, 289
 podatności, 232, 603
 podatnych
 komponentów, 585
 przestarzałych
 komponentów, 585
 udostępnionych
 dysków, 207
 ukrytych katalogów,
 573
 uruchomionych
 hostów, 193
 systemów, 193
 usług, 196, 300

- wykrywanie
 - usterek
 - kryptograficznych, 572
- wyłączanie
 - Windows Defendera, 99
 - zapory sieciowej domeny, 99
- wyszukiwarka Shodan, 153
- wywoływanie błędu SQL, 565

Z

- zabezpieczenia, 578
- zacieranie śladów, 625
- zagrożenie, 31
- zaporą sieciową, 191
- zasady bezpieczeństwa, 578
- zasób, 31
- zaufanie
 - dwukierunkowe, 375
 - jednokierunkowe, 375
 - lasu, 375
 - nieprzechodnie, 375
 - przechodnie, 375
- zbieranie informacji, 623,
Patrz także OSINT
 - aktywne, 166–216
 - o organizacji, 121
 - o sieci, 121
 - o systemie, 121
 - pasywne, 122–165
 - sposoby, 121

- zdalna powłoka, 257
- zdalne wykonanie kodu, 304
- ZeroTier, 632
- złośliwy aktor, 26
 - biały kapelusz, 28
 - czarny kapelusz, 28
 - haktywista, 27
 - przestępca
 - zorganizowany, 28
 - skryptowy dzieciak, script kiddie, 27
 - sponsorowany przez państwo, 28
 - szary kapelusz, 29
 - wtajemniczony, 28
- złoty bilet, 430
 - tworzenie, 428
- zmiana ustawień DNS, 358

Ź

- źródła danych OSINT, 123

Ż

- żądania HTTP, 570, 598, 610
 - GET, 602
 - POST, 564, 567

PROGRAM PARTNERSKI

— GRUPY 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
Helion

Poznaj Kali Linux — najsilniejszą sojuszniczkę w sieciowych wojnach!

Test penetracyjny jest ostatecznym sprawdzianem mechanizmów obronnych. Umożliwia też ocenę skutków fazy powłamaniowej eksploracji skompromitowanego systemu. Najlepsi pentesterzy korzystają w tym celu z Kali — zaawansowanej dystrybucji systemu Linux przeznaczonej właśnie do przeprowadzania testów penetracyjnych, wykrywania podatności, a także prowadzenia analiz informatyki śledczej i inżynierii wstecznej.

Dzięki temu wyczerpującemu przewodnikowi, napisanemu z myślą o początkujących użytkownikach systemu Kali Linux i pentesterach, szybko zdobędziesz potrzebne umiejętności. Najpierw skompletujesz i skonfigurujesz laboratorium, a potem poznasz najważniejsze koncepcje testów penetracyjnych. Skupisz się na zbieraniu informacji i poznasz różne narzędzia do oceny podatności dostępne w systemie Kali Linux. Nauczysz się wykrywać docelowe systemy w sieci, identyfikować błędy i wykorzystywać luki w zabezpieczeniach urządzeń, uzyskiwać dostęp do sieci, konfigurować operacje Command and Control (C2), a także przeprowadzać testy penetracyjne aplikacji internetowych. Opanujesz umiejętności potrzebne, aby włamać się do usługi Active Directory i do sieci korporacyjnych. Wreszcie — poznasz najlepsze praktyki w zakresie prowadzenia zaawansowanych testów penetracyjnych sieci w doskonale zabezpieczonym środowisku.

Z książki dowiesz się:

- czym jest etyczne hakowanie
- jak przygotować system Kali Linux do pracy
- jakie są techniki wykrywania zasobów i sieci, a także prowadzenia ocen podatności
- w jaki sposób wykorzystywać zaufanie w usługach Active Directory Domain Services
- na czym polega eksploatacja za pomocą operacji C2
- jak korzystać z zaawansowanych technik hakowania bezprzewodowego
- jak wykorzystywać luki w zabezpieczeniach aplikacji internetowych

Glen D. Singh zajmuje się cyberbezpieczeństwem, taktykami obronnymi i sieciami korporacyjnymi. Zdobył liczne certyfikaty, między innymi CEH, CHFI, PAWSP, a także trzy certyfikaty CCNA (CyberOps, Security, Routing and Switching). Napisał wiele książek dotyczących wykrywania i wykorzystywania podatności, analizy włamań, reakcji na incydenty i implementowania zabezpieczeń.

	KOD KORZYŚCI Sięgnij po więcej!  
 helion.pl  HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	ISBN 978-83-283-9835-1  9 788328 398351
Cena: 149,00 zł	

Packt