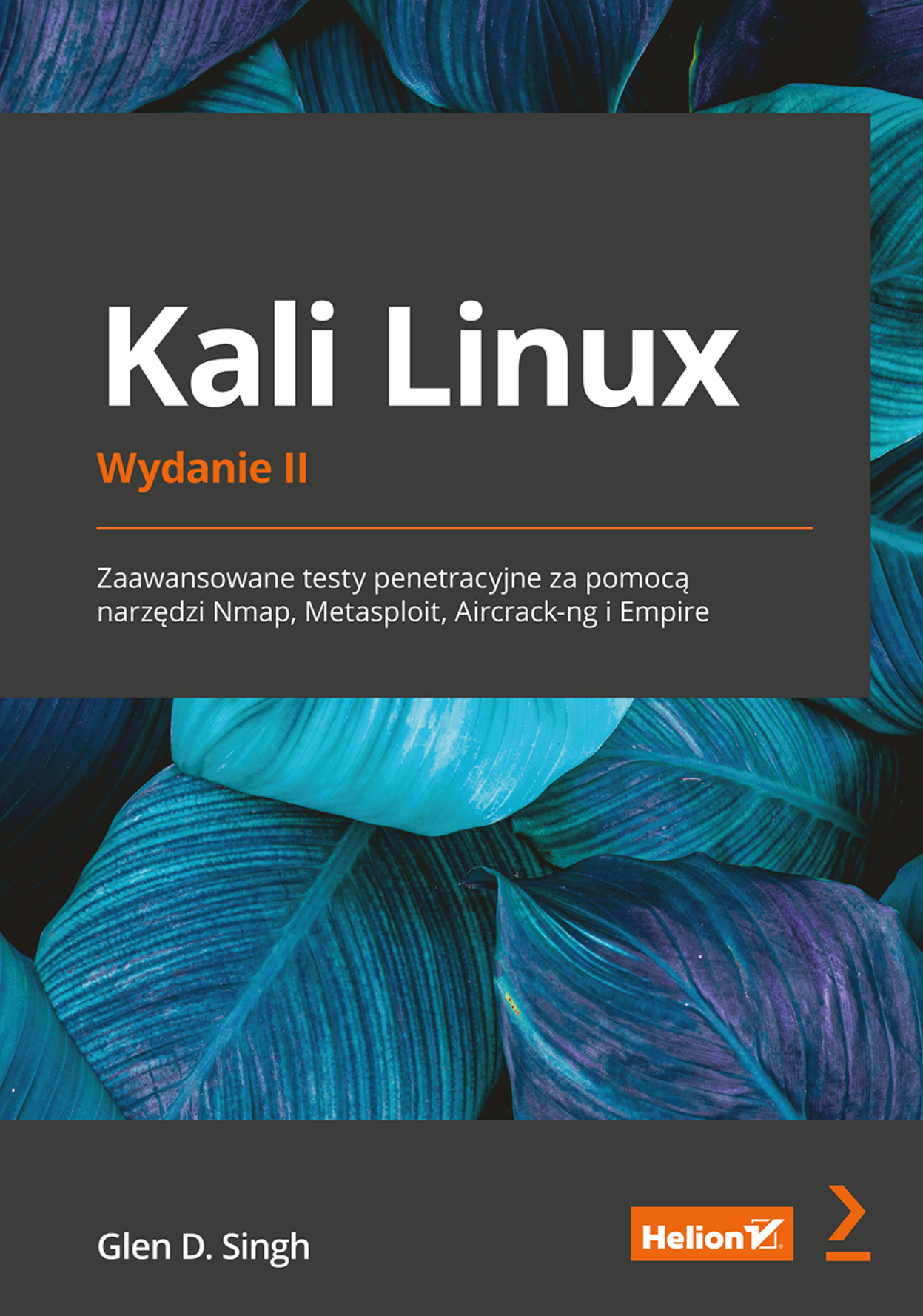


Kali Linux

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

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.

Spis treści

CZĘŚĆ 3. Techniki czerwonego zespołu

CZĘŚĆ 4. Inżynieria społeczna i ataki na aplikacje internetowe

Rozdział 2
Tworzenie laboratorium do testów penetracyjnych

Będąc kandydatem na etycznego hakera lub pentestera, należy pamiętać, że podczas testowania eksploitów, ładunków lub ćwiczenia umiejętności hakerskich nie można zakłócać pracy ani powodować żadnych szkód w systemach i infrastrukturze sieciowej innych osób i organizacji. Chociaż 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 uniknieszprzypadkowego 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. switche 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.

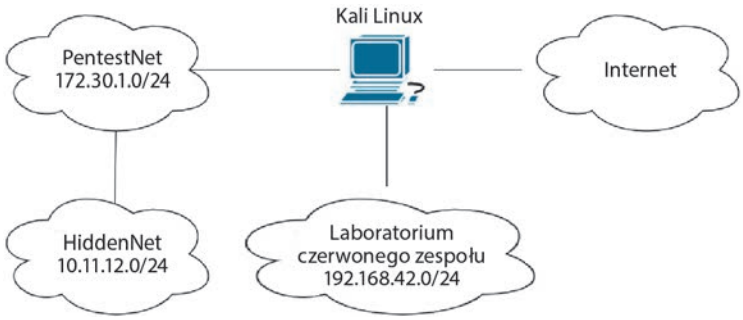
To tylko kilka problemów, z którymi styka się wielu studentów i początkujących informatyków. W licznych przypadkach początkujący ma tylko jeden komputer stacjonarny lub laptop. Technologie wirtualizacji, które rozwinęły się w reakcji na wspomniane problemy, otworzyły nowe możliwości w branży IT. Dzięki 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 eksploitów.

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.

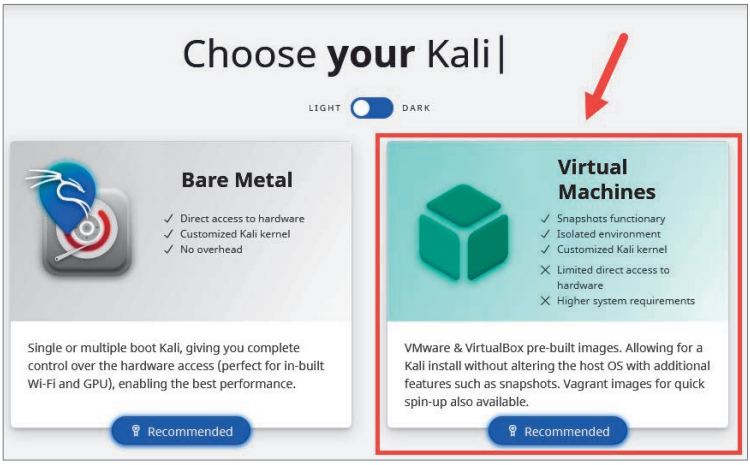
Zaczynamy!

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:

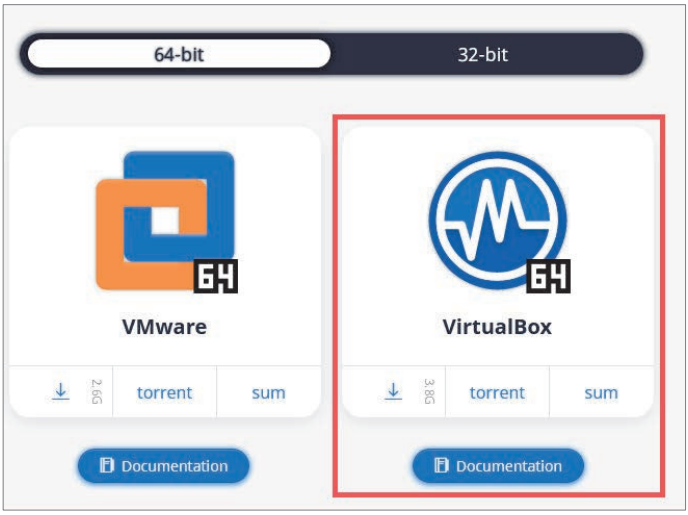
1. Aby pobrać oficjalny obraz wirtualny najnowszej wersji systemu Kali Linux, przejdź na stronę *https://www.kali.org/get-kali/*[2] i kliknij kartę *Virtual Machines*, widoczną na zrzucie ekranu przedstawionym na rysunku 2.4.

[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.*



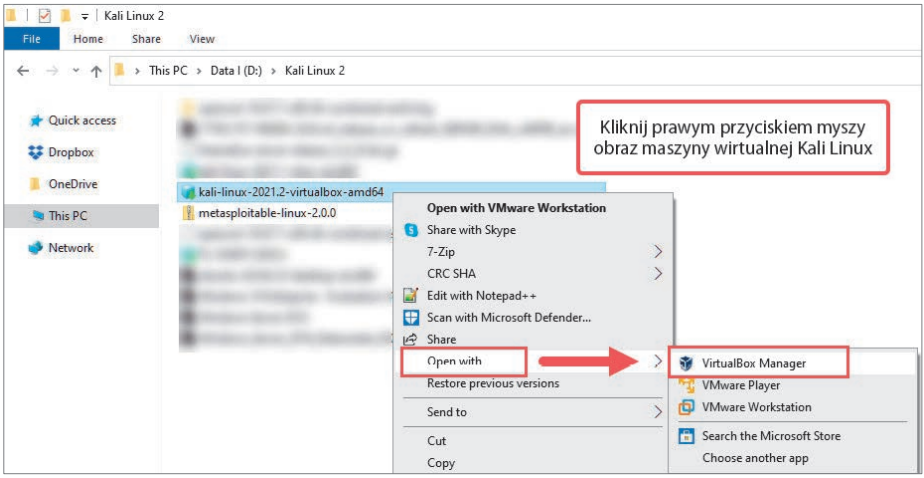
Rysunek 2.4. Obraz wirtualny systemu Kali Linux

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



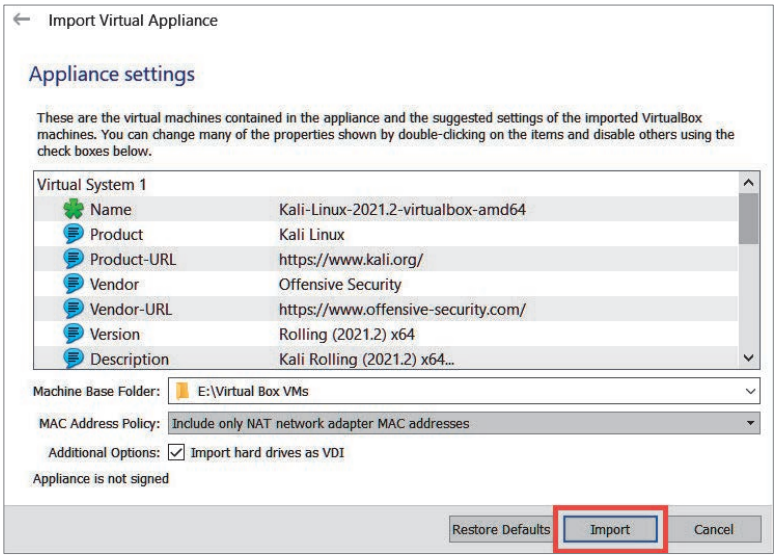
Rysunek 2.5. Pobieranie systemu Kali Linux

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**:

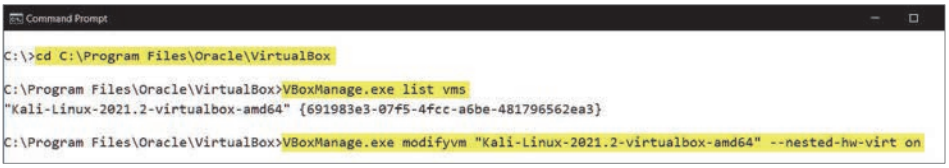
   ```
   C:\> cd C:\Program Files\Oracle\VirtualBox
   C:\Program Files\Oracle\VirtualBox> VBoxManage.exe list vms
   ```

   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:

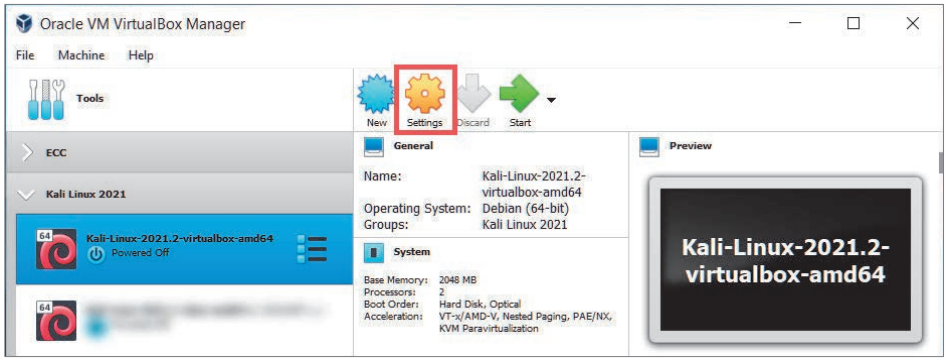
   ```
   C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "Nazwa
   maszyny wirtualnej" --nested-hw-virt on
   ```

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

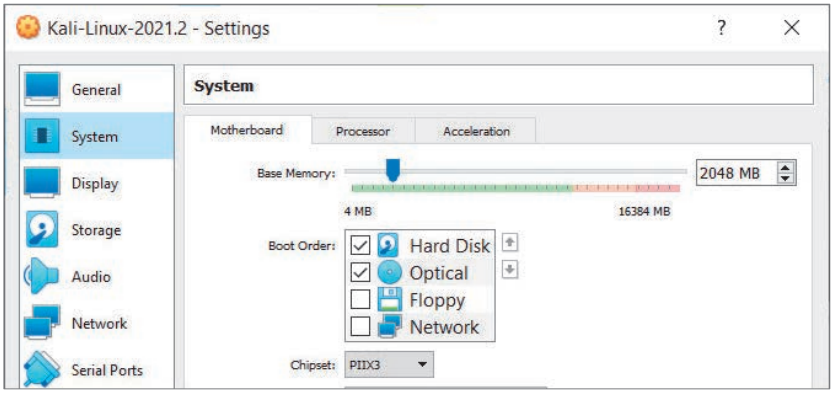


Rysunek 2.8. Włączanie zagnieżdżonej wirtualizacji na maszynie wirtualnej

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

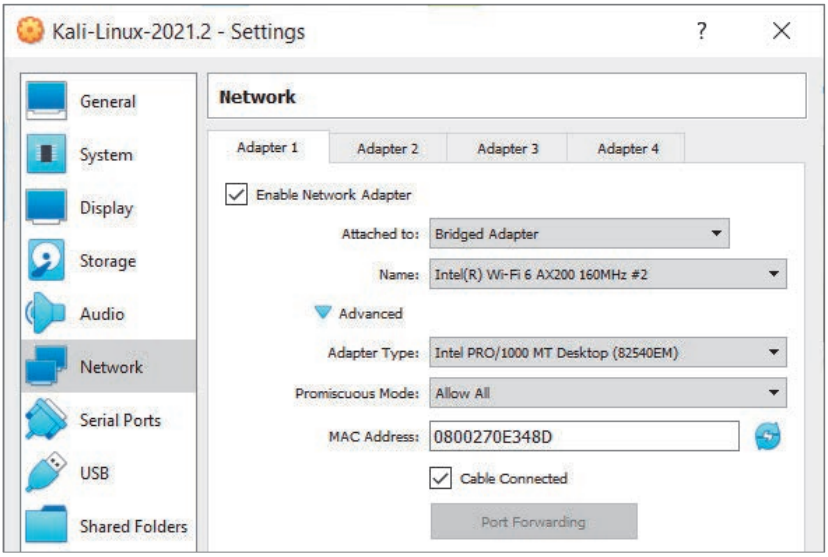
Nie zaleca się przydzielania ilości pamięci z pomarańczowego i czerwonego zakresu. Kali Linux może skutecznie działać, korzystając z 2 GB pamięci RAM; jeśli jednak w systemie masz do dyspozycji ponad 8 GB pamięci, możesz przydzielić 4 GB pamięci RAM.

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.

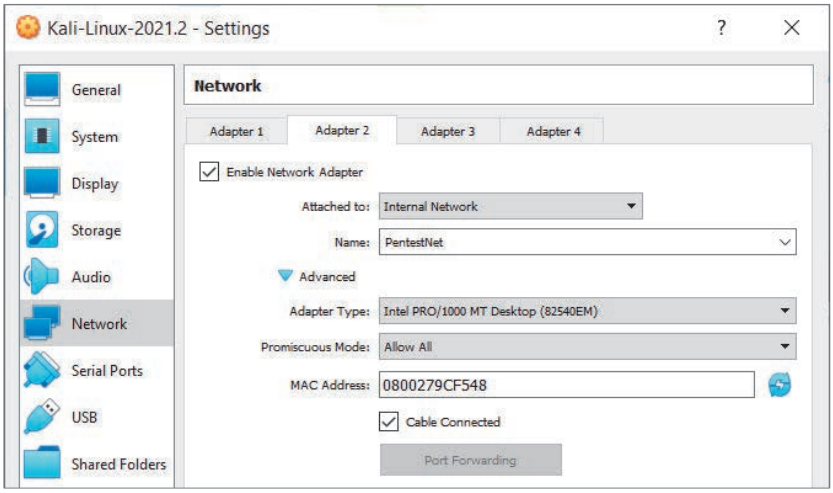


Rysunek 2.11. Karta sieciowa służąca do łączenia się z internetem

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.

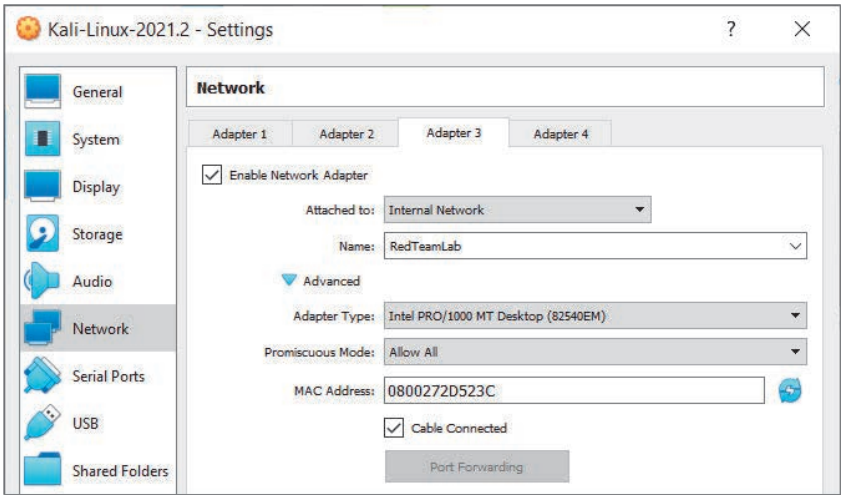
   Po skonfigurowaniu zakładki *Adapter 2* usuń zaznaczenie opcji *Enable Network Adapter*, aby wyłączyć kartę. Ponieważ w programie VirtualBox będziemy korzystać z wirtualnego serwera DHCP, czasem mogą się pojawiać konflikty podczas próby połączenia jednej maszyny wirtualnej z kilkoma sieciami wirtualnymi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

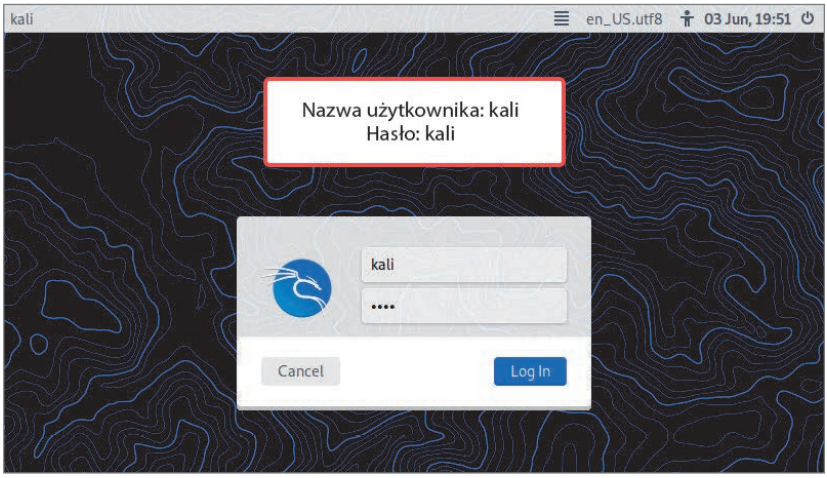
Po skonfigurowaniu zakładki *Adapter 3* usuń zaznaczenie opcji *Enable Network Adapter*, aby wyłączyć kartę sieciową. Kliknij *OK*, aby zapisać ustawienia maszyny wirtualnej.

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 linuksowego, 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.

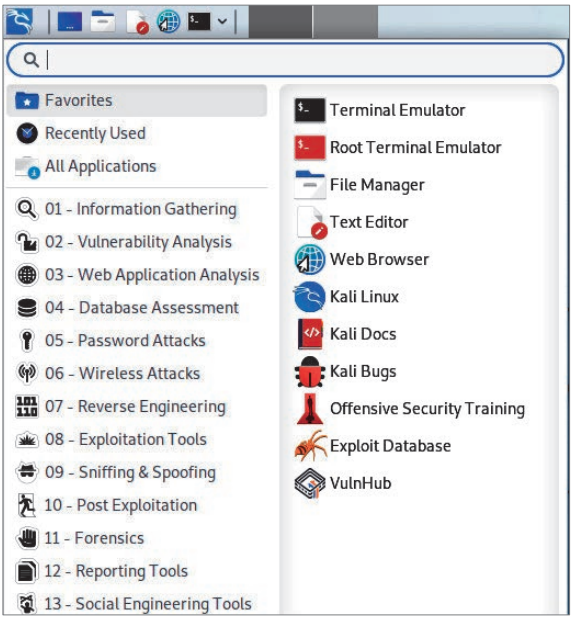


Rysunek 2.14. Okno logowania w systemie Kali Linux

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.



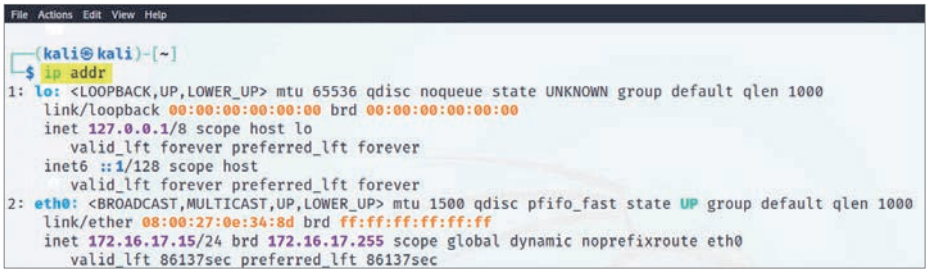
Rysunek 2.15. Lista narzędzi w systemie Kali Linux

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.

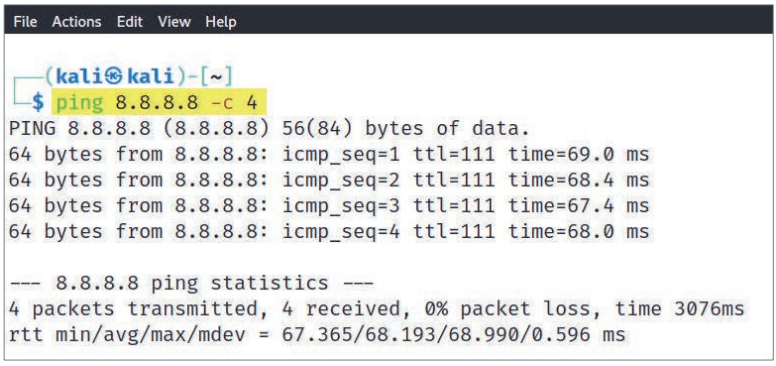
4. Sprawdź teraz, czy do maszyny wirtualnej systemu Kali Linux zostanie automatycznie przydzielony adres IP z naszej sieci za pośrednictwem karty sieciowej *Adapter 1* (*Bridge*). Otwórz Terminal i wykonaj polecenie `ip addr`, jak na rysunku 2.16.

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.



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.



Rysunek 2.17. Testowanie połączenia z internetem

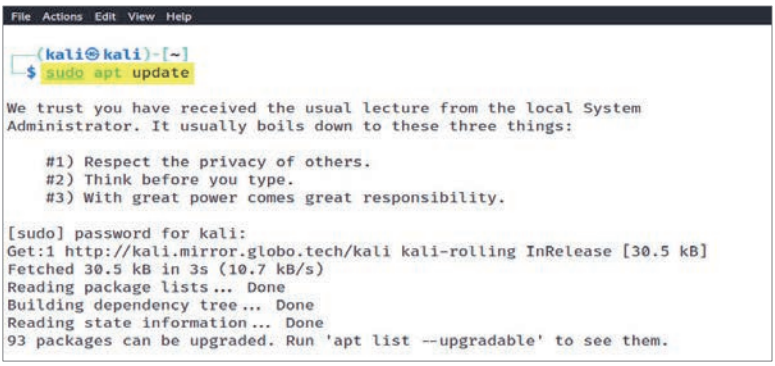
Jak widać na rysunku 2.17, Kali Linux otrzymał odpowiedzi z adresu `8.8.8.8`. Oznacza to, że system agresora ma dostęp do internetu.

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.

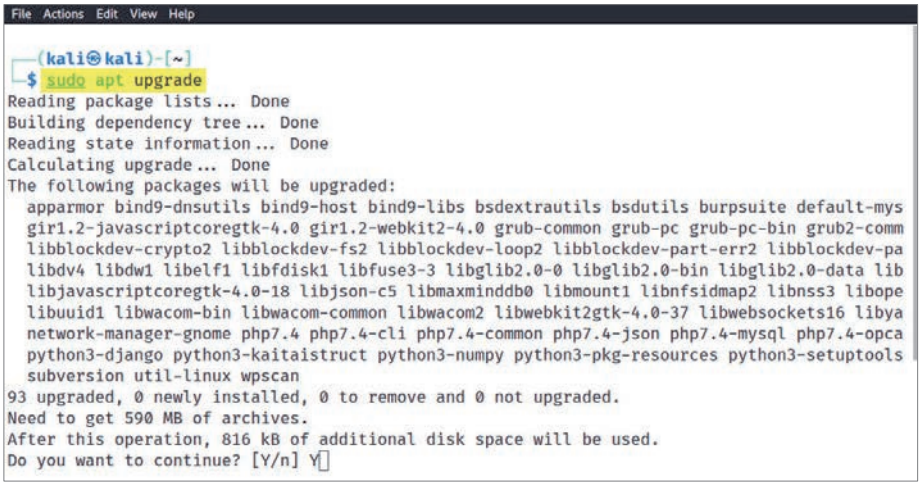


Rysunek 2.18. Aktualizacja źródeł

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.



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!

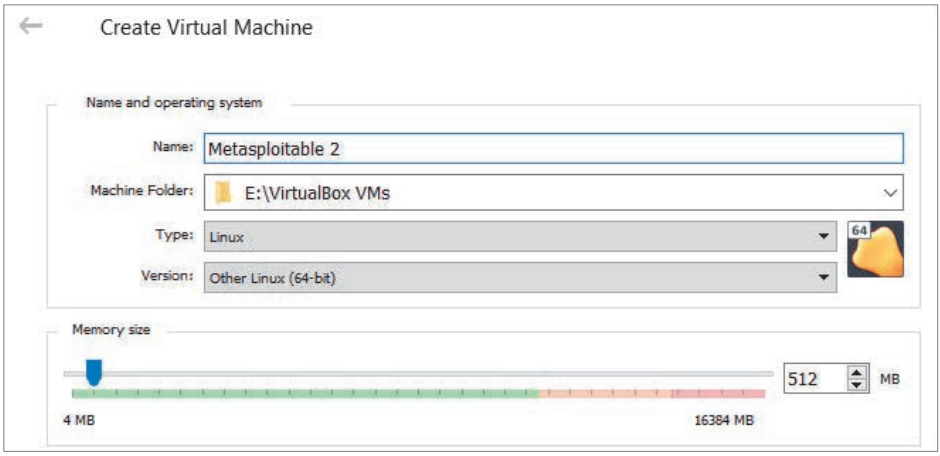
Część 1. Wdrażanie systemu Metasploitable 2

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*,

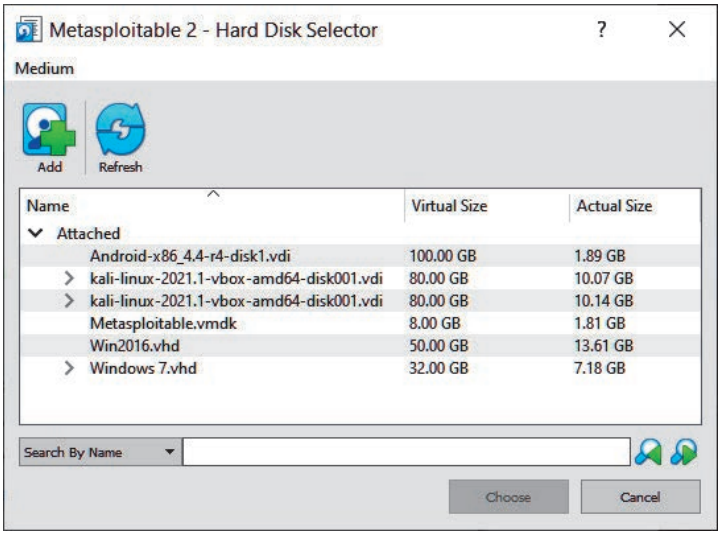
- *Version* (*Wersja*): *Other Linux (64-bit)*,
- *Memory size* (*Rozmiar pamięci*): 512 MB.

Szczegóły te są widoczne na rysunku 2.20.



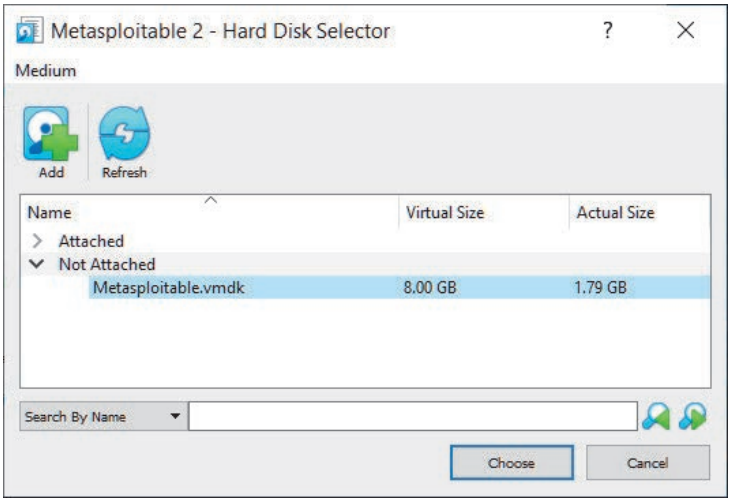
Rysunek 2.20. Tworzenie maszyny wirtualnej

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 wyodrębnione 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

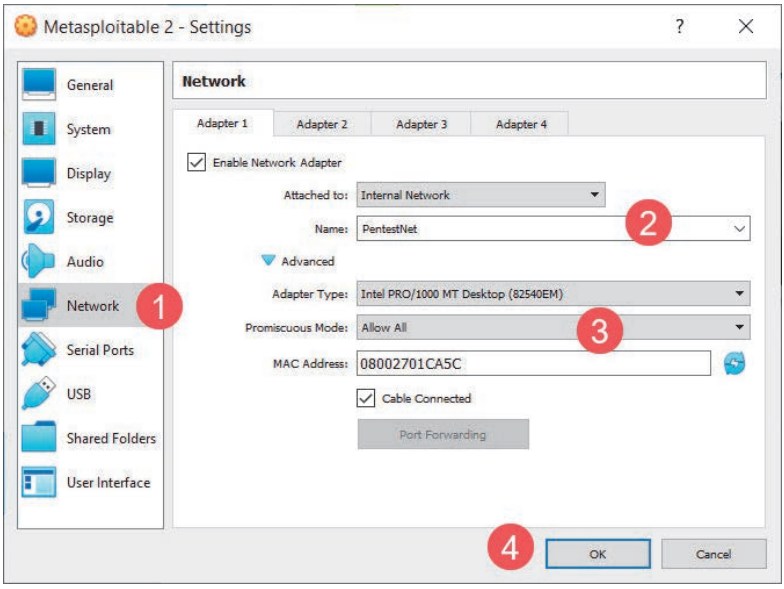
9. Powrócisz do okna *Create Virtual Machine* z dołączonym wirtualnym dyskiem twardym. Kliknij *Create* (*Utwórz*).

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:

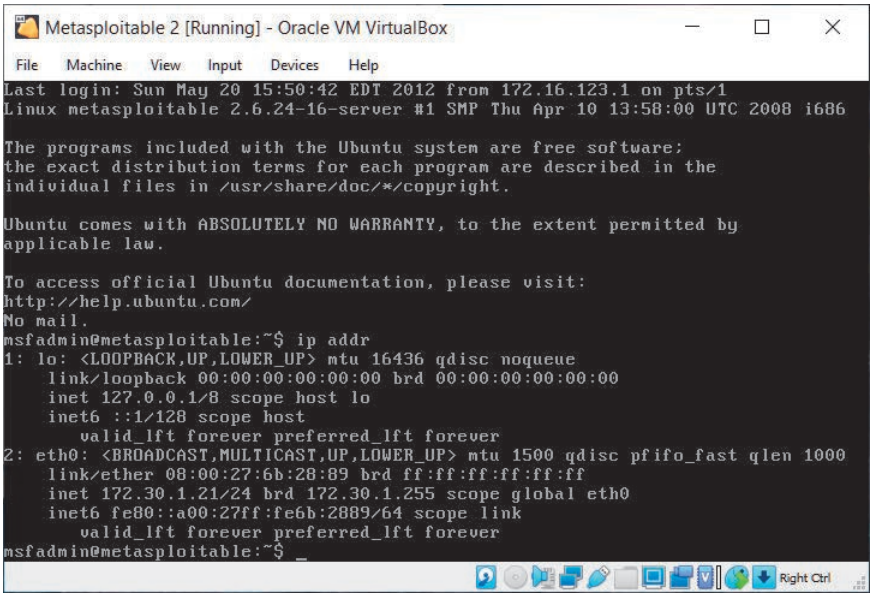
1. Aby skonfigurować ustawienia sieciowe, zaznacz maszynę wirtualną Metasploitable2 w programie VirtualBox Manager i kliknij *Settings*.
2. Przejdź do sekcji *Network* i zakładki *Adapter 1*, włącz kartę sieciową i wprowadź następujące ustawienia, aby dodać ją do sieci `PentestNet` należącej do laboratorium: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

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'!
```

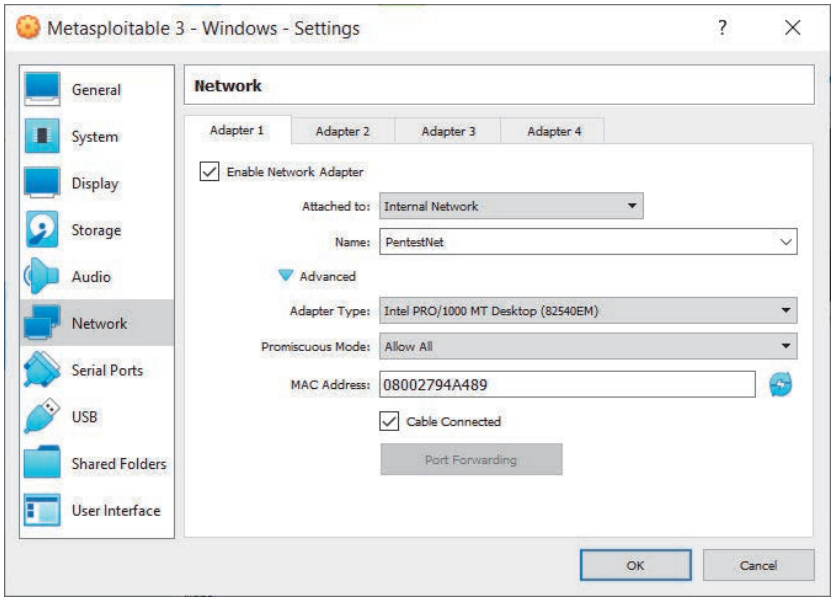
Rysunek 2.27. Pobieranie systemu Metasploitable 3

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
```

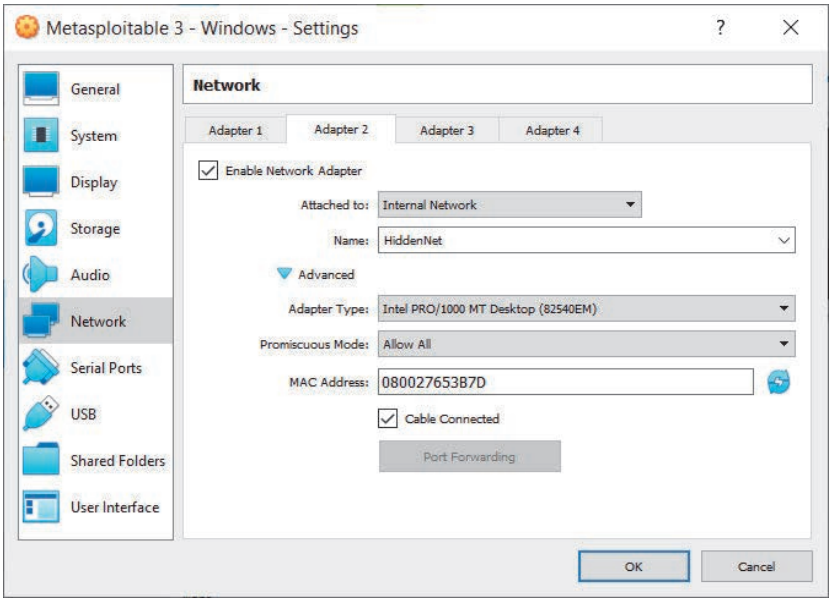
8. Metasploitable 3 dla systemu Windows po zakończeniu konfiguracji będzie dostępny w programie VirtualBox Manager. Zmień nazwę maszyny wirtualnej, połącz ją z siecią wirtualną `PentestNet` i upewnij się, że opcja *Promiscuous Mode* ma wartość *Allow All* (patrz rysunek 2.28).



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.

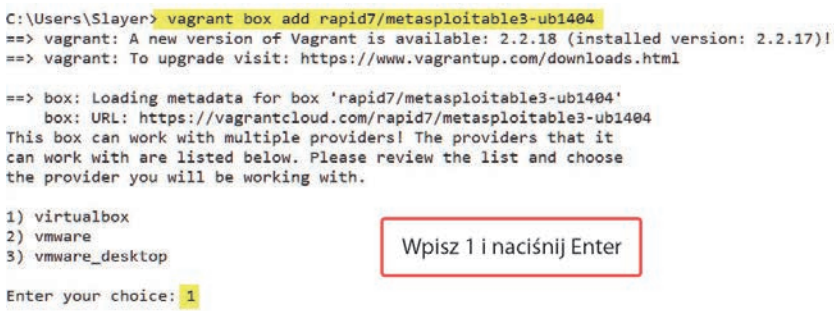
Część 2. Konfiguracja wersji dla Linuksa

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.



Rysunek 2.30. Wybór hipernadzorcy

   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

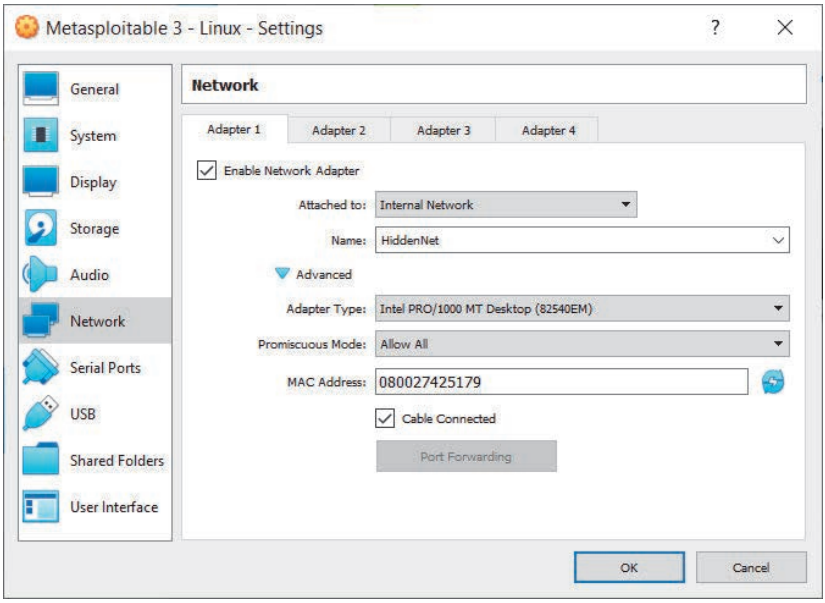
Możliwe, że zanim przejdziesz do następnego kroku, będziesz musiał(a) otworzyć program Virtual Manager.

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 Metasloitable 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.

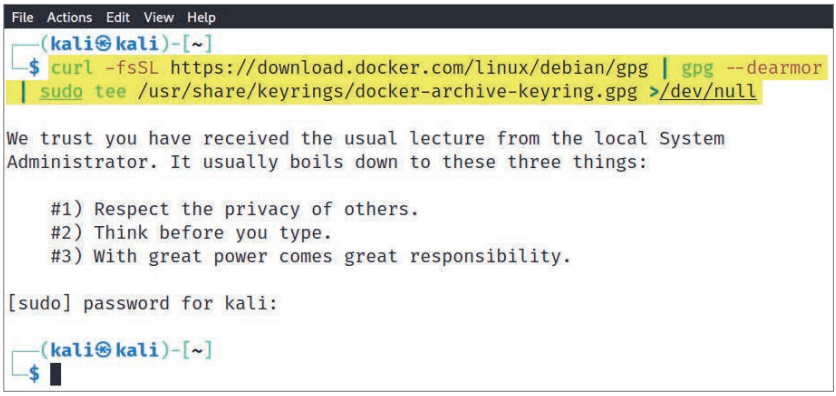
1. Ponieważ musisz pobrać kilka komponentów, upewnij się, że Kali Linux jest połączony z internetem.
2. Otwórz Terminal w systemie Kali Linux i wykonaj następujące polecenia, aby pobrać klucz Dockera **Pretty Good Privacy** (**PGP**):

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

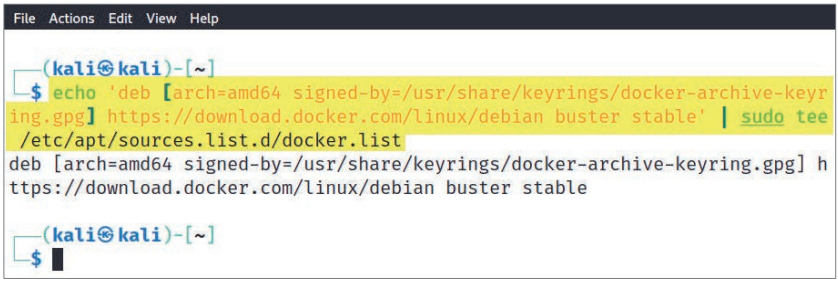
   Na rysunku 2.32 pokazany jest oczekiwany wynik wspomnianego polecenia.
3. Wykonaj następujące polecenia, aby skonfigurować repozytorium APT Dockera w systemie Kali Linux:

   ```
   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.



Rysunek 2.32. Instalacja kluczy PGP Dockera



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:

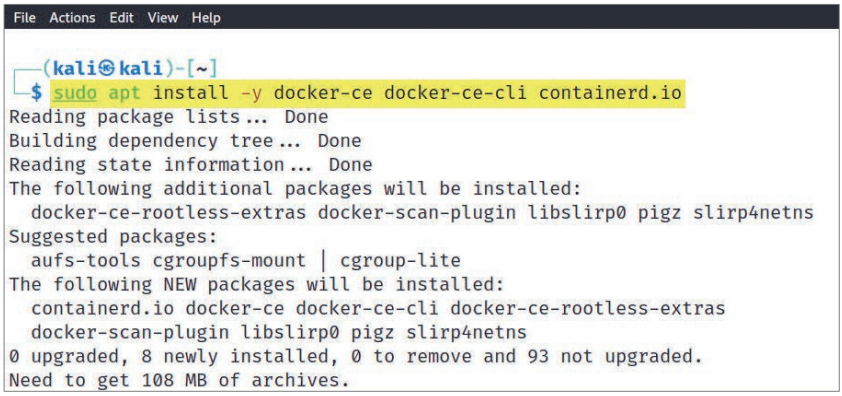
   ```
   sudo apt install -y docker-ce docker-ce-cli containerd.io
   ```

   Na rysunku 2.34 pokazane są oczekiwane wyniki wspomnianych poleceń.

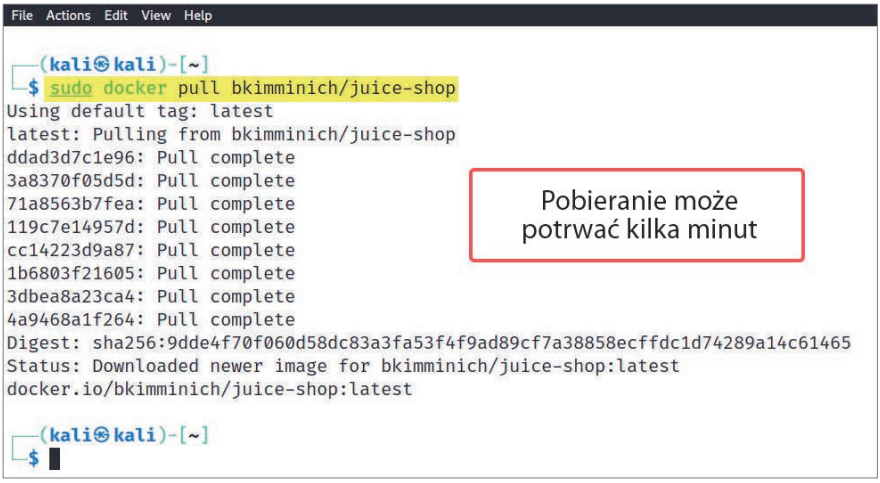
6. Na tym etapie Docker jest zainstalowany w systemie Kali Linux. Wykonaj to polecenie, aby pobrać kontener Dockera z aplikacją OWASP Juice Shop:

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

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



Rysunek 2.34. Instalowanie Dockera w systemie Kali Linux



Rysunek 2.35. Kontener Dockera z aplikacją OWASP Juice Shop

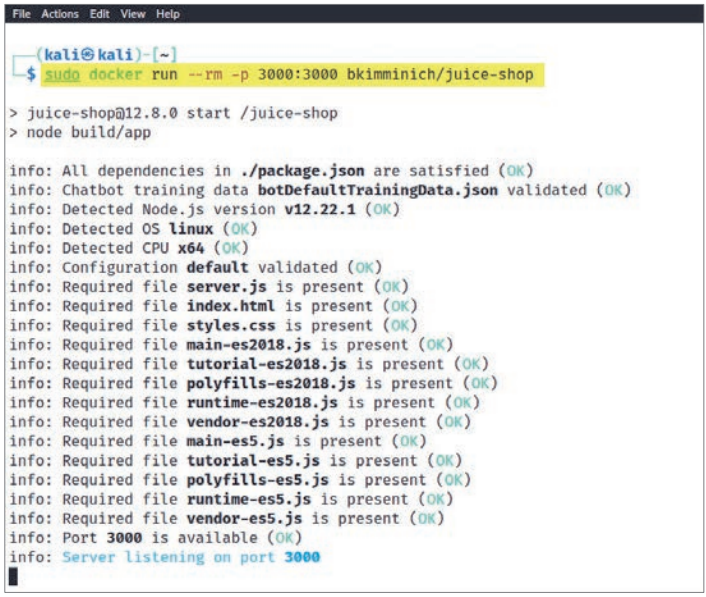
7. Wykonaj następujące polecenie, aby uruchomić w Dockerze aplikację OWASP Juice Shop:

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

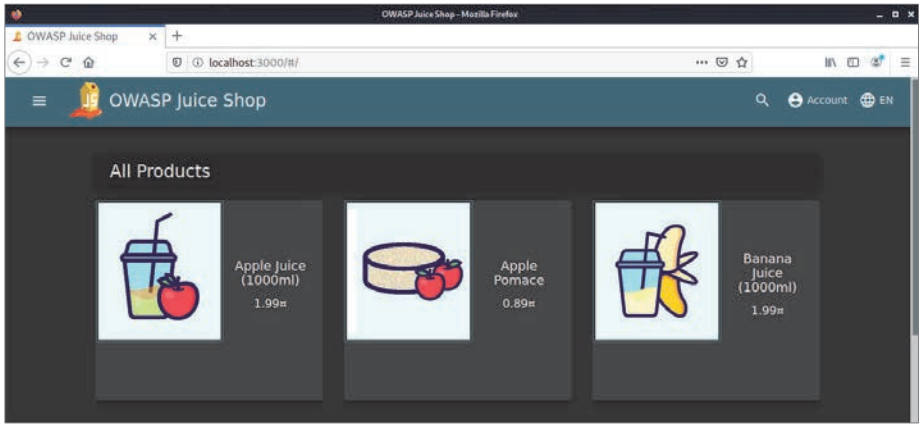
   Na rysunku 2.36 widać, że Docker uruchamia kontener OWASP Juice Shop.

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

8. 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.



Rysunek 2.36. Uruchamianie kontenera Dockera z aplikacją OWASP Juice Shop



Rysunek 2.37. Interfejs użytkownika aplikacji OWASP Juice Shop

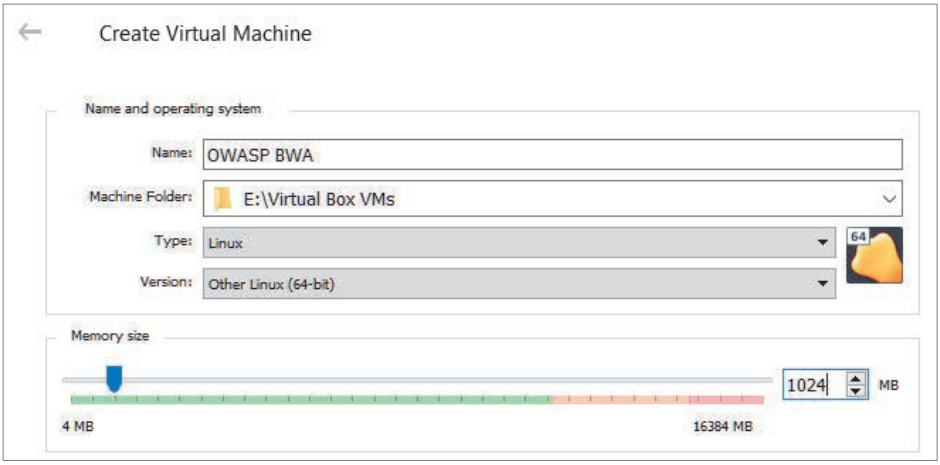
Następnie utworzysz maszynę wirtualną z projektem OWASP Broken Web Applications w laboratorium do testów penetracyjnych.

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:

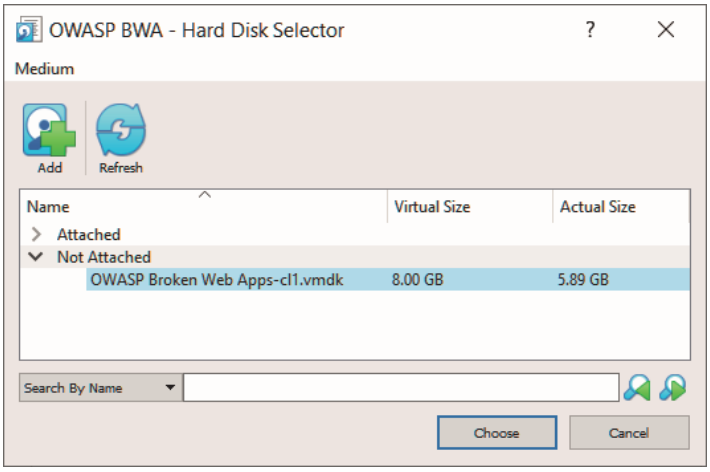
1. Otwórz stronę *https://sourceforge.net/projects/owaspbwa/files/* i pobierz system **OWASP Broken Web Applications** w wersji 1.2.
2. Rozpakuj plik *OWASP_Broken_Web_Apps_VM_1.2.7z* za pomocą aplikacji 7-Zip. Skopiuj wyodrębnioną zawartość (wirtualny dysk twardy) do katalogu z pozostałymi maszynami 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

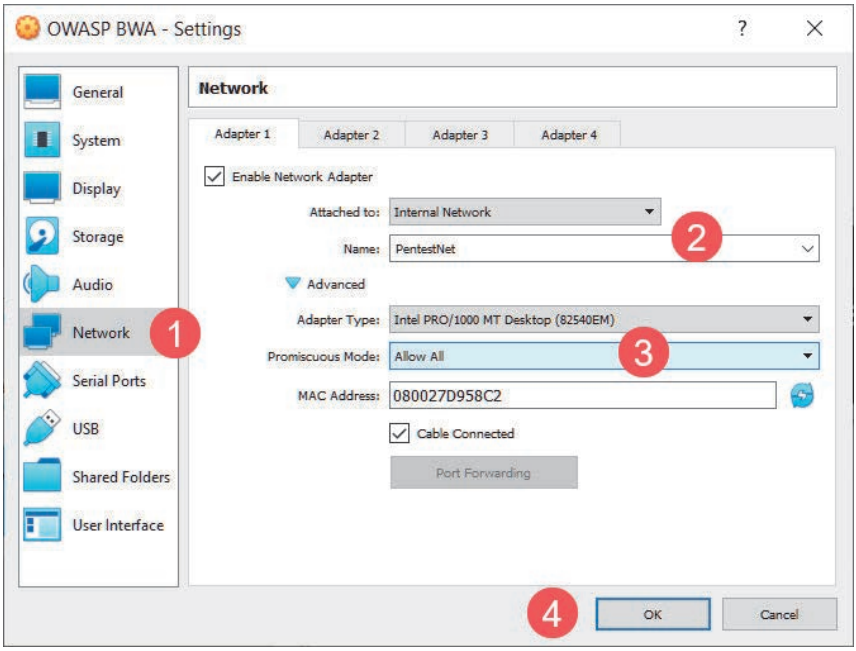
6. W tym samym oknie *Create Virtual Machine* zmień wartość opcji *Hard disk* na *Use an existing virtual hard disk file* i kliknij ikonę folderu z prawej strony, aby otworzyć okno *Hard Disk Selector*.
7. Kliknij *Add* i przejdź do folderu, w którym znajdują się rozpakowane pliki z kroku 2. Wybierz 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.



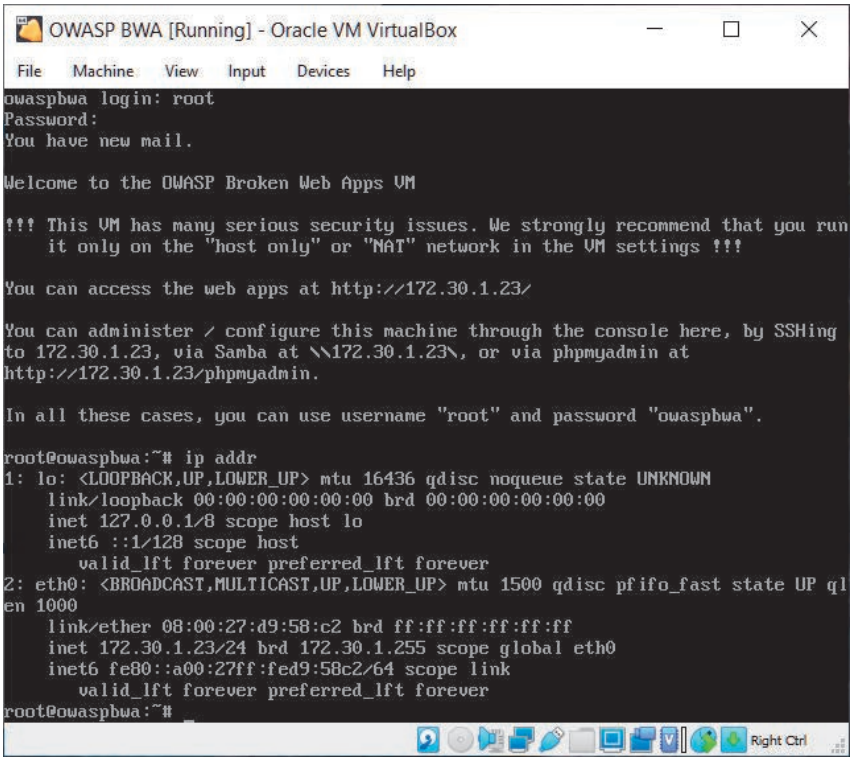
Rysunek 2.40. Konfiguracja karty sieciowej

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 hipernadzorcy 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.



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 eksploitów 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

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

z

ź

ż

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.

Helion

helion.pl

HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-283-9835-1

9 788328 398351

Cena: 149,00 zł

Packt›