Vijay Kumar Velu

Kali Linux

Testy penetracyjne i bezpieczeństwo sieci dla zaawansowanych

Wydanie II

Helion

Packt›

Tytuł oryginału: Mastering Kali Linux for Advanced Penetration Testing - Second Edition

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-4037-4

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

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/kalit2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 1

Testy penetracyjne ukierunkowane na osiągnięcie celu

„Istnieją tylko dwa rodzaje ludzi: ci, którzy hakują, i ci, którzy zostaną zhakowani”

Wszystko rozpoczyna się od wyznaczenia celu, który chcesz osiągnąć. Z tego względu w tym rozdziale będziemy omawiać znaczenie testów penetracyjnych ukierunkowanych na osiągnięcie celu oraz wyjaśnimy, dlaczego bez wyznaczenia takiego celu przeprowadzanie skanowania w poszukiwaniu podatności (ang. *vulnerability scanning*), testy penetracyjne czy inne działania zespołów Red Team[1] mogą zakończyć się spektakularnym niepowodzeniem. W tym rozdziale omówimy również szereg zagadnień związanych z przeprowadzaniem testów bezpieczeństwa, tworzeniem i konfigurowaniem środowiska testowego oraz używaniem systemu Kali Linux do przeprowadzania zaawansowanych testów penetracyjnych. Po przeczytaniu tego rozdziału będziesz wiedział:

- Na czym polegają testy bezpieczeństwa systemów informatycznych.
- Dlaczego skanowanie w poszukiwaniu podatności, testy penetracyjne i inne działania zespołu Red Team mogą zakończyć się niepowodzeniem.
- Jak aktualizować i konfigurować system Kali Linux.
- Jak za pomocą skryptów powłoki *bash* dostosowywać system Kali Linux do własnych potrzeb.

[1] Red Team — zespół czerwony, ofensywny, w scenariuszach testów cyberbezpieczeństwa odpowiedzialny za przeprowadzanie kontrolowanych ataków mających na celu przełamywanie zabezpieczeń środowiska komputerowego chronionego przez zespół defensywny (Blue Team; zespół niebieski) — *przyp. tłum.*

- Jak wyznaczać cele działania.
- Jak zbudować środowisko testowe.

Koncepcyjny przegląd testów bezpieczeństwa

Praktycznie każda firma czy organizacja na świecie może się obawiać różnych zagrożeń związanych z cyberprzestrzenią, takich jak wycieki wrażliwych danych, złośliwe oprogramowanie czy cyberterroryzm. Każda próba przeciwdziałania musi rozpocząć się od przygotowania ogólnego zarysu i koncepcji planowanych zabezpieczeń. Jeżeli stu różnym konsultantom zadasz pytanie: „Czym jest testowanie bezpieczeństwa środowiska teleinformatycznego?", to z dużą dozą prawdopodobieństwa możesz założyć, że otrzymasz bardzo wiele różnych odpowiedzi. Najprościej mówiąc, testowanie bezpieczeństwa to proces polegający na sprawdzaniu, czy dane środowisko teleinformatyczne i poszczególne działające w nim systemy są odpowiednio chronione i czy mogą funkcjonować zgodnie z oczekiwaniami.

Zmierzch klasycznych testów penetracyjnych, skanowania w poszukiwaniu podatności i działań zespołów Red Team

W tym podrozdziale skoncentrujemy się na omawianiu ograniczeń tradycyjnych bądź, jak kto woli, klasycznych metod przeprowadzania testów penetracyjnych, wyszukiwania podatności i działań zespołów Red Team. Najpierw jednak spróbujemy w prostych słowach objaśnić obecne znaczenie tych trzech zagadnień i pokazać ich ograniczenia.

- **Skanowanie w poszukiwaniu podatności** (ang. *vulnerability scanning*) — jest to proces mający na celu identyfikację podatności na ataki i luk w zabezpieczeniach atakowanego środowiska i działających w nim systemów. Poważnym ograniczeniem takiego skanowania jest fakt, że jego wyniki to lista potencjalnych podatności, z których duża część może być fałszywie pozytywna. Dla właściciela danego biznesu może to stanowić poważny problem z oszacowaniem ryzyka, ponieważ w takiej sytuacji nie mamy jasnego obrazu tego, która z podatności stanowi rzeczywiste zagrożenie dla funkcjonowania środowiska, a która jest tylko fałszywie potencjalnym zagrożeniem niemającym odzwierciedlenia w rzeczywistości.
- **Testy penetracyjne** (ang. *penetration testing*) — jest to proces mający na celu dokonanie próby bezpiecznego wykorzystania wykrytych wcześniej podatności i luk w zabezpieczeniach do przeprowadzenia kontrolowanego ataku na badane

środowisko bez wprowadzania poważnych zagrożeń dla jego normalnego funkcjonowania. Przeprowadzenie takich testów daje znacznie mniejszy odsetek wyników fałszywie pozytywnych, ponieważ pentesterzy próbują użyć każdej ze znalezionych podatności. Poważnym ograniczeniem testów penetracyjnych może być to, że z reguły są one zawężane tylko do publicznie znanych podatności i exploitów. Co więcej, podczas przeprowadzania testów penetracyjnych często słyszymy słowa: „Bingo! Mamy roota!", ale bardzo rzadko pada pytanie: „Co robimy dalej?". Dzieje się tak z wielu bardzo różnych powodów, takich jak narzucone z góry ograniczenia zakresu przeprowadzanych testów penetracyjnych, konieczność raportowania tylko podatności wysokiego ryzyka czy ograniczenie przez klienta zakresu testów tylko do wybranych systemów czy segmentów sieci.

- **Ćwiczenia zespołów Red Team** (ang. *Red Team Exercises*) — jest to proces szacowania efektywności ochrony badanego środowiska przed zagrożeniami z cyberprzestrzeni i poprawiania zaimplementowanych zabezpieczeń. Podczas takich ćwiczeń z reguły stosowanych jest wiele różnych sposobów atakowania badanego środowiska, wykorzystujących metody socjotechniczne, kampanie phishingowe, ataki na sieci bezprzewodowe czy fizyczne testy penetracyjne. Ograniczeniem takich ćwiczeń mogą być ramy czasowe, restrykcje budżetowe, postępowanie według z góry ustalonych scenariuszy czy pomijanie niektórych działań, które mogą być zbyt niebezpieczne do przeprowadzenia w rzeczywistym środowisku produkcyjnym.

Bardzo często wszystkie trzy opisane procesy powiązane są z określeniami takimi jak *hacking* czy *łamanie zabezpieczeń*. Możemy co prawda powiedzieć klientowi, że spróbujemy włamać się do jego sieci i pokazać słabe strony jej zabezpieczeń, ale czy tak naprawdę klient czy właściciel środowiska rozumie, na czym takie „hakowanie" czy „łamanie zabezpieczeń" będzie polegało? Jak możemy je zmierzyć? Jakie są kryteria „hakowania"? Skąd możemy wiedzieć, że „hakowanie" czy „łamanie zabezpieczeń sieci" zostało zakończone? Wszystkie tego typu pytania w prostej mierze prowadzą do jednego, fundamentalnego zagadnienia — jaki jest podstawowy cel przeprowadzania danej operacji?

Podstawowym celem przeprowadzania testów penetracyjnych czy ćwiczeń zespołów Red Team jest określenie stopnia podatności danego środowiska na cyberataki, wyznaczenie zagrożeń dla jego poszczególnych elementów składowych (poszczególnych segmentów sieci i działających w nim systemów) oraz oszacowanie ryzyka, jakie stanowią dla funkcjonowania całego środowiska firmy czy organizacji. Z reguły nie jest to jednak kwestia ilości podatności znalezionych na poszczególnych hostach, ale to, jak bardzo eksponowany jest dany system i jak jego działanie jest krytyczne dla funkcjonowania całego środowiska. Nie każda znaleziona podatność i luka w zabezpieczeniach jest istotna i nie zawsze musi się ona wiązać z poważnym zagrożeniem. Na przykład znaleziona podatność na ataki typu *Cross-Site Scripting* (*XSS*) na odseparowanym, informacyjnym serwerze WWW nie musi stanowić poważnego zagrożenia dla funkcjonowania całej firmy; nie zmienia to jednak faktu, że po wykryciu takiej luki właściciel systemu może podjąć decyzję o minimalizacji zagrożenia poprzez zaimplementowanie takich rozwiązań jak WAF (ang. *Web Application Firewall*), zapobiegających przeprowadzaniu ataków typu XSS.

Metodologia przeprowadzania testów

Niestety metodologia przeprowadzania testów penetracyjnych bardzo często nie obejmuje powodów, dla których klient zlecił przeprowadzenie takich testów, ani nie zawiera listy danych, które są krytyczne dla biznesu i powinny być chronione w szczególny sposób. Pominięcie tak istotnych informacji już na samym początku procesu może spowodować, że właściwy cel przeprowadzania takiego testu penetracyjnego ulegnie rozmyciu.

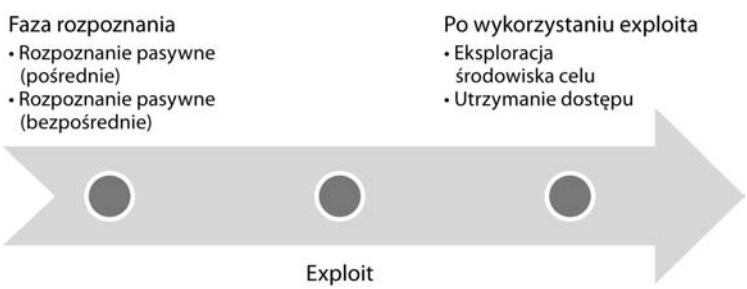
Bardzo wielu pentesterów niechętnie podchodzi do z góry wyznaczonych metodologii postępowania, obawiając się, że może to w jakiś sposób ograniczać ich kreatywność w wyszukiwaniu podatności i luk w zabezpieczeniach, a następnie w ich efektywnym wykorzystywaniu. Testy penetracyjne często nie odzwierciedlają sposobu, w jaki może postępować potencjalny napastnik. Na przykład klient zlecający test chce sprawdzić, czy pentester będzie w stanie w nieautoryzowany sposób uzyskać dostęp na poziomie administratora do atakowanego systemu, podczas gdy intencją prawdziwego napastnika może być skopiowanie z tego systemu wrażliwych danych w sposób, który ani nie wymaga uzyskania takiego dostępu, ani nie spowoduje awarii systemu.

Aby można było poradzić sobie z ograniczeniami wynikającymi z formalnych metod testowania, testy penetracyjne muszą być zintegrowane w ramach, które pozwalają spojrzeć na atakowaną sieć z punktu widzenia napastnika i w uporządkowany sposób przeprowadzić skuteczny atak.

W roku 2009 Mike Cloppert, pracujący w zespole CERT firmy Lockheed Martin, opracował koncepcję znaną obecnie jako atak cybernetyczny (ang. *Attacker Kill Chain*), która opisywała poszczególne kroki, jakie musi podjąć napastnik w celu przeprowadzenia efektywnego cyberataku na system sieciowy. Ataki takie nie zawsze mają przebieg liniowy, ponieważ niektóre z ich faz mogą być przeprowadzane równolegle. W danym okresie ten sam cel może być atakowany wielokrotnie, przy czym niektóre równoległe fazy ataku mogą być przeprowadzane w tym samym czasie.

W tej książce zmodyfikowaliśmy nieco oryginalny koncept cyberataku opracowany przez Mike'a Clopperta, aby jeszcze dokładniej odzwierciedlić poszczególne operacje podejmowane przez potencjalnego napastnika podczas atakowania całych sieci komputerowych oraz funkcjonujących w nich systemów, aplikacji i usług sieciowych.

Na rysunku przedstawionym poniżej pokazano, jak wygląda typowy atak cybernetyczny:



Typowy atak cybernetyczny może wyglądać tak:

- **Faza rozpoznania** — twierdzenie, że „rekonesans nigdy nie jest stratą czasu", przyjęte i powszechnie stosowane przez wojsko na całym świecie, jest prostym potwierdzeniem tego, że przed rozpoczęciem ataku zawsze dobrze jest zebrać jak największą ilość informacji o nieprzyjacielu. Z tego samego powodu hakerzy przed rozpoczęciem cyberataku przeprowadzają zakrojone na szeroką skalę rozpoznanie celu. W praktyce szacuje się, że na przeprowadzenie odpowiedniego rozpoznania środowiska celu cyberprzestępcy (jak również profesjonalni pentesterzy) zużywają nawet 70 procent czasu i zasobów całego ataku! Ogólnie rzecz biorąc, cyberprzestępcy najczęściej wykorzystują dwa scenariusze fazy rozpoznania:
  - **Rozpoznanie pasywne** — w takim scenariuszu napastnik nie wchodzi w bezpośrednią interakcję ze środowiskiem celu, lecz korzysta na przykład z zawartości publicznie dostępnych stron internetowych, materiałów konferencyjnych, informacji dostępnych w mediach i serwisach sieciowych (a zwłaszcza w serwisach społecznościowych). Bazując na pozyskanych informacjach, stara się wyznaczyć odpowiednią **płaszczyznę ataku** (ang. *attack surface*). Jedną z operacji często wykonywanych podczas rozpoznania pasywnego jest przygotowywanie listy obecnych i poprzednich pracowników atakowanej firmy, która może stanowić dobrą bazę do łamania haseł metodą brute-force lub może być wykorzystana do przeprowadzania ataków socjotechnicznych. Rozpoznanie przeprowadzane w sposób pasywny jest bardzo trudne, a często wręcz niemożliwe do wykrycia.
  - **Rozpoznanie aktywne** — aktywność napastnika związana z aktywnym rozpoznawaniem środowiska celu może zostać wykryta, ale w praktyce bardzo trudno ją odróżnić od tego, z czym większość firm czy organizacji styka się na co dzień. Rozpoznanie aktywne może obejmować skanowanie portów, zdalne skanowanie systemów w poszukiwaniu podatności i luk w zabezpieczeniach, a nawet fizyczne odwiedziny w siedzibie firmy pod pozorem udawania klienta, dostawcy pizzy czy serwisanta.
- **Faza dostawy** — w tej fazie dokonywany jest wybór i opracowanie narzędzia, które zostanie użyte do wykorzystania danego exploita podczas przeprowadzania ataku. To, jakie narzędzie zostanie finalnie wybrane, zależy zarówno od intencji atakującego, jak i od planowanego sposobu dostarczenia narzędzia do atakowanego celu (na przykład za pomocą wiadomości poczty elektronicznej, sieci bezprzewodowej czy usługi sieci WWW). Znaczenie fazy dostawy i jej wpływ na przeprowadzanie ataku zostaną szczegółowo omówione w drugiej połowie książki.
- **Faza penetracji (faza ataku)** — jest to faza, w której określony exploit zostaje pomyślnie wykorzystany, co pozwala napastnikowi na osiągnięcie zaplanowanego celu. Skompromitowanie celu mogło wystąpić w jednej fazie (na przykład napastnik wykorzystał dobrze znaną podatność danego systemu na ataki z przepełnianiem bufora), ale równie dobrze mogło wymagać przeprowadzenia operacji wielofazowej (na przykład napastnik, wykorzystując metody socjotechniczne, przedostał się na teren firmy i skradł egzemplarz firmowej książki telefonicznej. Znajdujące się tam informacje zostały wykorzystane do utworzenia słownika danych użytego następnie

do przeprowadzenia ataku typu brute-force na portal firmy. Dodatkowo na pozyskane poprzez kradzież książki adresy poczty elektronicznej pracowników napastnik porozsyłał wiadomości mające na celu skłonić użytkowników do kliknięcia osadzonego łącza i pobrania odpowiednio spreparowanego, złośliwego dokumentu PDF, za pomocą którego napastnik mógłby przejąć kontrolę nad zainfekowanymi systemami). Ataki wielofazowe są powszechnie wykorzystywane w scenariuszach, gdzie celem ataku jest określona firma czy organizacja.

- **Faza *post-exploit* (eksploracja środowiska celu)** — faza eksploracji środowiska celu bardzo często bywa niepoprawnie nazwana **fazą eksfiltracji** (ang. *exfiltration phase*), ponieważ dość powszechnie takie ataki postrzegane są niemal wyłącznie jako metody kradzieży poufnych i wrażliwych danych (takich jak listy użytkowników i haseł dostępu, dane osobowe czy informacje finansowe). W praktyce jednak napastnicy mają często zupełnie inne cele. Na przykład nieuczciwa firma może być zainteresowana przeprowadzeniem ataku typu DoS na internetową sieć usług swojego konkurenta, czego efektem będzie potencjalne zwiększenie zainteresowania klientów swoimi rozwiązaniami. Z tego względu faza eksploracji środowiska celu musi skupiać się na wielu potencjalnie możliwych czynnościach napastnika. Jedne z najczęściej obserwowanych działań związanych z exploitami mają miejsce wtedy, gdy napastnicy próbują zwiększyć swoje uprawnienia do najwyższego możliwego poziomu (eskalacja pionowa) i uzyskać dostęp do jak największej liczby kont i systemów (eskalacja pozioma).
- **Faza *post-exploit* (utrzymanie dostępu)** — przełamanie zabezpieczeń i uzyskanie dostępu do atakowanego systemu może być dla napastnika bardzo wartościowe, ale z pewnością ta wartość znacząco wzrośnie, jeżeli napastnikowi uda się utworzyć przyczółek i zachować stały dostęp do skompromitowanego systemu, dzięki czemu będzie mógł w dowolnym momencie powrócić do zaatakowanego systemu. Z punktu widzenia zespołu odpowiedzialnego za ochronę systemu ten element cyberataku jest zazwyczaj najłatwiejszy do wykrycia.

Przebieg ataku cybernetycznego (ang. *kill chain*) jest swego rodzaju metamodelem zachowania napastnika próbującego przełamać zabezpieczenia atakowanego celu i uzyskać do niego nieautoryzowany dostęp. Jako metamodel atak cybernetyczny może zawierać dowolną, otwartą lub komercyjną metodologię przeprowadzania testów penetracyjnych. W przeciwieństwie jednak do metodologii cyberatak pokazuje przebieg ataku na środowisko celu z perspektywy strategicznej. Układ i zawartość naszej książki zostały dobrane tak, aby odzwierciedlić czynności wykonywane przez napastnika podczas przeprowadzania ataku.

Wprowadzenie do systemu Kali Linux — jego historia i przeznaczenie

System Kali Linux jest następcą znanego i bardzo popularnego niegdyś systemu BackTrack. W środowisku pentesterów Kali Linux jest swego rodzaju standardem wśród narzędzi i pakietów wspomagających przeprowadzanie testów penetracyjnych sieci komputerowych. Autorami

systemu są Mati Aharoni oraz Devon Kearns z firmy Offensive Security. Poniżej przedstawiamy krótką historię systemu Kali Linux od momentu jego powstania:

- W marcu 2013 roku system BackTrack został zastąpiony systemem Kali Linux, wykorzystującym nową architekturę opartą na systemie Debian GNU/Linux.
- **Kali 1.1.0 (data wydania: 9 lutego 2015)** — kolejna wersja systemu Kali Linux pojawiła się dopiero po dwóch latach od jego premiery i przyniosła aktualizację jądra systemu do wersji 3.18, poprawki modułów wspomagających ataki ze wstrzykiwaniem ramek do sieci Wi-Fi oraz obsługę nowych sterowników bezprzewodowych kart sieciowych; w sumie w tym wydaniu poprawionych zostało ponad 58 błędów. W następnych wydaniach tej wersji, takich jak Kali 1.1.0a, poprawione zostały również drobne błędy i inne problemy instalatora.
- **Kali 2.0 (data wydania: 11 sierpnia 2015)** — wersja 2.0 była bardzo poważną aktualizacją, zawierającą m.in. duże zmiany w interfejsie użytkownika; stała się tzw. dystrybucją ciągłą systemu Kali Linux (ang. *rolling distribution*). Począwszy od wersji 2.0, można dokonywać aktualizacji systemu Kali Linux ze starszej do nowszej wersji.
- **Kali 2016.1 (data wydania: 21 stycznia 2016)** — pierwsze ciągłe wydanie systemu Kali Linux, które przyniosło aktualizację jądra do wersji 4.3 oraz nowe środowisko GNOME w wersji 3.18.
- **Kali 2016.2 (data wydania: 31 sierpnia 2016)** — kolejne ciągłe wydanie systemu Kali Linux, wyposażone w jądro 4.6, środowisko GNOME 3.20.2 oraz wiele poprawek i aktualizacji.

System Kali Linux w wersji 2.0 (i w kolejnych aktualizacjach) posiada między innymi następujące cechy:

- Ponad 300 narzędzi wspomagających przeprowadzanie testów penetracyjnych oraz ekspertyz z informatyki śledczej. W kolejnych wydaniach systemu poszczególne narzędzia są sukcesywnie aktualizowane bądź zastępowane nowymi wersjami. Wiele z tych narzędzi współpracuje z bezprzewodowymi kartami sieciowymi i pozwala na przeprowadzanie testów penetracyjnych w sieciach Wi-Fi.
- Obsługa wielu środowisk desktopowych, takich jak KDE, GNOME, Xfce, Mate, e17, lxde czy i3wm.
- Narzędzia zgodne z dystrybucją Debian są synchronizowane z repozytoriami co najmniej cztery razy dziennie, co pozwala na ich aktualizację oraz instalację poprawek niemal natychmiast po ich opublikowaniu.
- Obsługa środowiska Secure Development Environment oraz pakietów i repozytoriów podpisanych kluczem GPG.
- Wsparcie dla użytkowników chcących przygotować indywidualne, dostosowane do własnych potrzeb dystrybucje ISO systemu Kali Linux. Funkcja bootstrap znakomicie ułatwia instalowanie systemu również w dużych środowiskach korporacyjnych, gdzie proces instalacji może być zautomatyzowany przy użyciu predefiniowanych plików konfiguracyjnych (ang. *Linux preseed files*).

- Ze względu na rosnącą popularność (i spadające ceny) systemów z procesorami ARM w systemie zaimplementowana została również obsługa architektur ARMEL i ARMHF, dzięki czemu Kali Linux można instalować na takich urządzeniach jak rk3306 mk/ss808, Raspberry Pi, ODROID U2/X2, Samsung Chromebook, EfikaMX, Beaglebone Black, CuBox czy Galaxy Note 10.1.
- Mimo rosnącej popularności Kali Linux nadal pozostaje systemem klasy open source, dostępnym bezpłatnie dla każdego i co najważniejsze — aktywnie wspieranym przez ogromną społeczność użytkowników.

Celem systemu Kali Linux jest zebranie wszystkich najważniejszych narzędzi wspomagających przeprowadzanie testów bezpieczeństwa i testów penetracyjnych w jednej, elastycznej i bardzo uniwersalnej platformie systemowej.

Instalowanie i aktualizowanie systemu Kali Linux

W poprzednich wydaniach tej książki koncentrowaliśmy się głównie na procesie instalacji systemu Kali Linux w maszynach wirtualnych VMware, zatem tym razem postaramy się nieco bardziej zagłębić w różne inne techniki instalowania i aktualizowania systemu Kali Linux.

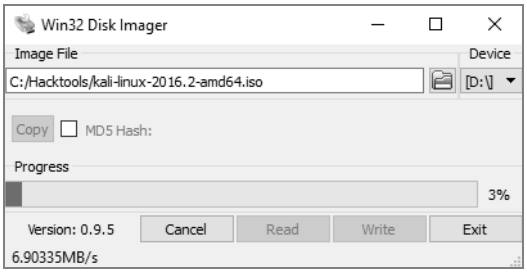
Uruchamianie systemu Kali Linux z urządzenia przenośnego

Proces instalowania systemu Kali Linux na urządzeniu przenośnym jest całkiem prosty. W niektórych sytuacjach klienci nie zezwalają na podłączanie i używanie „obcych" laptopów w ich sieci — klient dostarcza wtedy pentesterowi odpowiednie komputery, przy użyciu których ma on przeprowadzić testowanie. Przeprowadzanie testów penetracyjnych przy użyciu systemu Kali Linux uruchomionego z urządzenia przenośnego ma wiele zalet, na przykład:

- Wszystko zmieścisz w kieszeni (pamięci USB czy zewnętrzne dyski twarde mają małe rozmiary).
- System Kali Linux możesz uruchomić na komputerze bez konieczności wprowadzania jakichkolwiek modyfikacji w zainstalowanym systemie operacyjnym.
- Korzystając z urządzeń przenośnych, możesz utworzyć kilka osobnych wersji systemu Kali Linux, dostosowanych do określonych scenariuszy testowania i wymagań klienta.

Jeżeli pracujesz na komputerze działającym pod kontrolą systemu Windows, zainstalowanie systemu Kali Linux na urządzeniu przenośnym będzie wymagało wykonania zaledwie trzech kroków:

1. Pobierz oficjalny obraz systemu Kali Linux ze strony internetowej o adresie:
   https://docs.kali.org/introduction/download-official-kali-linux-images
2. Pobierz program Win32 Disk Imager ze strony internetowej *https://sourceforge.net/projects/win32diskimager/*.
3. Uruchom program Win32 Disk Imager jako administrator. Podłącz przenośną pamięć USB do dowolnego portu USB komputera. Na ekranie powinno pojawić się okno podobne do przedstawionego poniżej. Wybierz urządzenie, na którym chcesz zainstalować system Kali Linux, i naciśnij przycisk *Write* (zapisz):



Po zakończeniu instalowania systemu zamknij program Win32 Disk Imager i bezpiecznie odłącz pamięć USB. Kali Linux zainstalowany na tym urządzeniu jest już gotowy do użycia; możesz je na przykład podłączyć do laptopa i uruchomić z niego system Kali Linux. Jeżeli chcesz zainstalować system Kali Linux z poziomu komputera działającego pod kontrolą systemu Linux, proces instalacji jest jeszcze prostszy i wymaga wykonania z poziomu konsoli tylko dwóch poleceń. Pierwsze to `sudo fdisk -l`, które wyświetla listę wszystkich zamontowanych napędów dyskowych, a drugie to `dd if=kali linux.iso of=/dev/`*`nazwa_urządzenia`* `bs=512k`. To wszystko. Polecenie `dd` pobiera instalacyjny plik ISO i zapisuje jego zawartość na podanym urządzeniu. Polecenie pobiera kilka argumentów wywołania, gdzie `if` to nazwa wejściowego pliku ISO, `of` to nazwa urządzenia docelowego, a `bs` to rozmiar zapisywanych bloków.

Instalowanie systemu Kali Linux w maszynie wirtualnej

W tej sekcji szczegółowo omówimy sposób instalowania systemu Kali Linux w maszynach wirtualnych działających pod kontrolą oprogramowania VMware Workstation Player oraz Oracle VirtualBox.

VMware Workstation Player

VMware Workstation Player (starsze wersje nosiły nazwę VMware Player) to oprogramowanie wirtualizacyjne, pozwalające na uruchamianie maszyn wirtualnych działających pod kontrolą innych systemów operacyjnych, które jest bezpłatne dla zastosowań osobistych. Dla zastosowań komercyjnych wymagane jest zakupienie odpowiedniej licencji. Oprogramowanie można pobrać ze strony internetowej o następującym adresie URL:

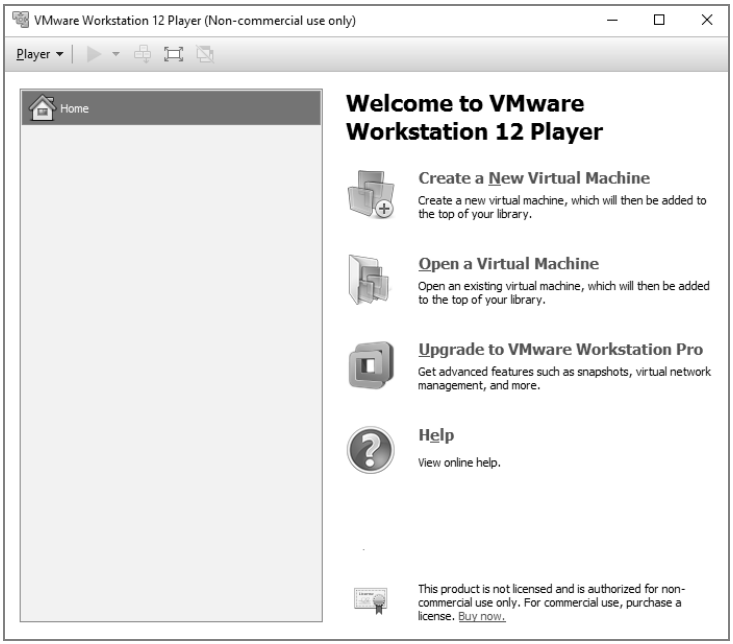
https://www.vmware.com/products/player/playerpro-evaluation.html

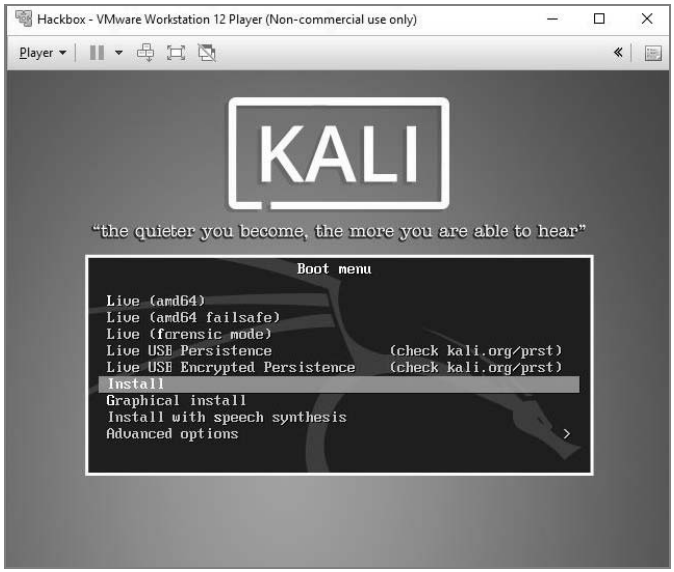
Poniżej przedstawiamy krok po kroku procedurę instalacji systemu Kali Linux w maszynie wirtualnej VMware Workstation Player.

Po pobraniu pliku instalacyjnego VMware Workstation Player uruchom go, a na ekranie pojawi się pierwszy ekran kreatora instalacji, tak jak to zostało pokazane poniżej. Naciśnij przycisk *Next* (dalej).

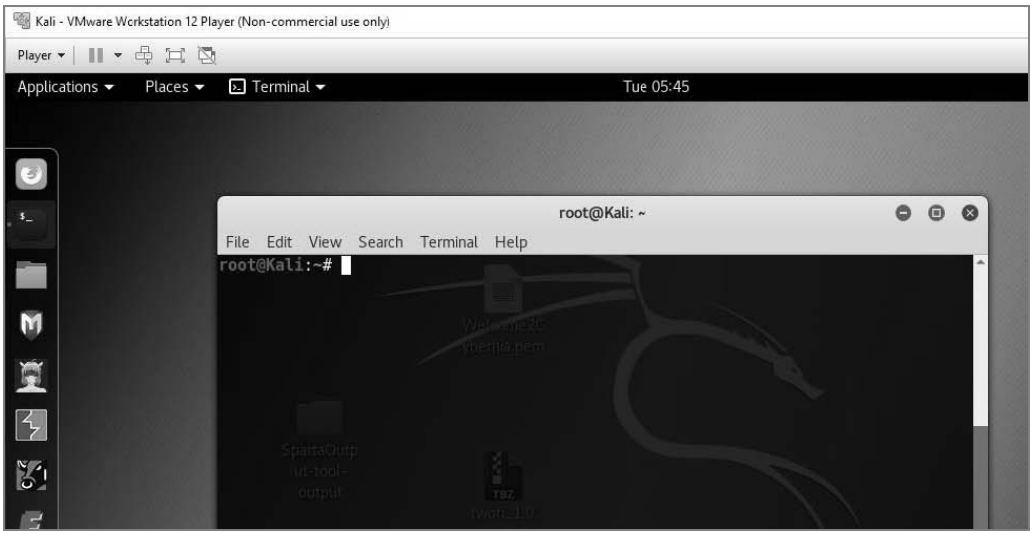
Na ekranie pojawi się okno z warunkami licencji. Naciśnij przycisk *Accept* (akceptuję), a następnie na kolejnych ekranach naciskaj przycisk *Next* — aż do momentu, kiedy pojawi się ekran przedstawiony na pierwszym rysunku na następnej stronie, sygnalizujący, że proces instalacji programu VMware Workstation Player został zakończony pomyślnie.

Kolejnym krokiem będzie utworzenie maszyny wirtualnej i zainstalowanie w niej systemu Kali Linux, którego instalacyjny obraz ISO pobraliśmy już wcześniej z oficjalnej strony internetowej. Naciśnij przycisk *Create a New Virtual machine* (utwórz nową maszynę wirtualną), a następnie wybierz opcję *Installer disc image file (iso)* (plik obrazu ISO dysku instalacyjnego), wskaż odpowiedni plik ISO i naciśnij przycisk *Next*. Wpisz nazwę tworzonej maszyny wirtualnej (na przykład *HackBox*) i wybierz miejsce, w którym będą przechowywane jej pliki. Naciśnij przycisk *Next*, określ rozmiar dysku maszyny wirtualnej dla systemu Kali Linux (rekomendowany rozmiar to 10 GB), naciskaj przycisk *Next* na kolejnych ekranach kreatora aż do utworzenia maszyny wirtualnej. Po jej uruchomieniu powinieneś zobaczyć następujący ekran (patrz drugi rysunek na następnej stronie).





Z poziomu menu uruchomieniowego możesz wybrać opcję instalacji systemu Kali Linux na dysku lub uruchomienia go w wersji Live (bez konieczności instalacji). Po zakończeniu instalacji system Kali Linux powinien uruchamiać się w maszynie wirtualnej VMware bez żadnych problemów, tak jak to zostało pokazane na rysunku:



Począwszy od wersji 2016.2, z systemu Kali Linux zostały usunięte repozytoria Sana. *Sana* to nazwa kodowa wersji systemu Kali Linux, która używała repozytoriów zawierających pakiety. Z tego powodu pierwszym, zdecydowanie zalecanym krokiem, jaki powinieneś wykonać po zainstalowaniu i uruchomieniu systemu Kali Linux, powinno być wykonanie polecenia `apt-get update`, dzięki któremu zaktualizowana zostanie zawartość pliku *sources.lst*.

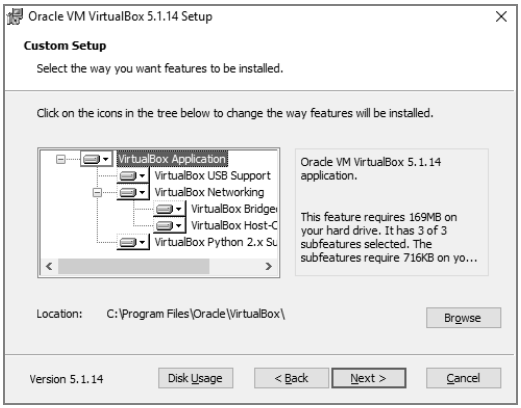
VirtualBox

Program VirtualBox jest rozwiązaniem bardzo podobnym do VMware Workstation Player. Jest to oprogramowanie pozwalające na tworzenie i uruchamianie maszyn wirtualnych, które jest bezpłatnie udostępniane w wersji open source. Pakiet VirtualBox możesz pobrać z następującej strony internetowej:

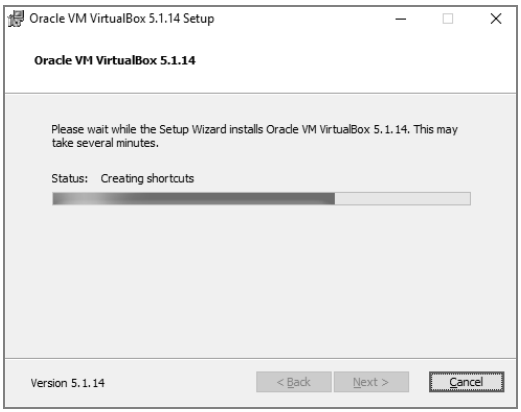
https://www.virtualbox.org/wiki/Downloads

Teraz pokażemy sposób instalacji systemu Kali Linux w maszynie wirtualnej działającej pod kontrolą oprogramowania VirtualBox. Podobnie jak to miało miejsce w przypadku VMware, najpierw musimy zainstalować sam pakiet VirtualBox. Aby to zrobić, uruchom pobrany program instalacyjny; na ekranie powinieneś zobaczyć pierwsze okno kreatora instalacji (patrz pierwszy rysunek na następnej stronie).

Naciśnij przycisk *Next* (dalej), a na ekranie pojawi się lista opcji konfiguracyjnych pakietu. W naszym przypadku wybierzemy domyślną opcję *VirtualBox Application* (patrz drugi rysunek na następnej stronie).

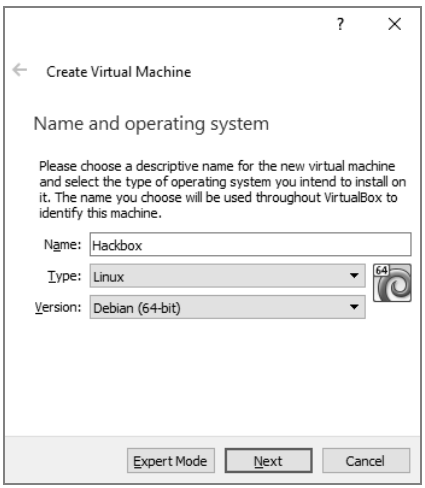


Naciśnij przycisk *Next*, a na ekranie pojawi się kolejne okno kreatora, pokazujące postęp procesu instalacji, tak jak to zostało pokazane na rysunku poniżej:

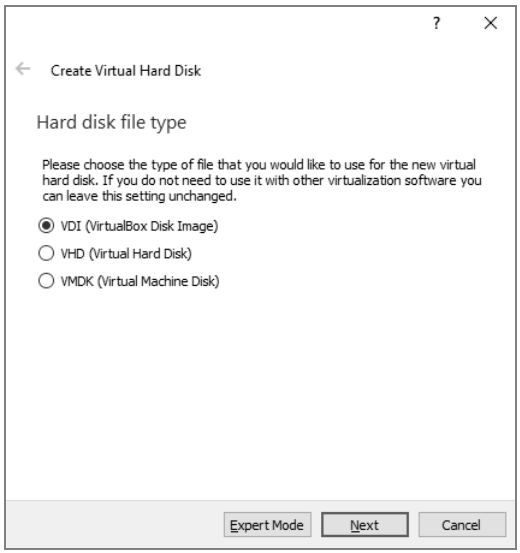


Jeżeli proces instalacji pakietu Oracle VirtualBox zakończy się pomyślnie, po uruchomieniu programu ekran powinien wyglądać tak, jak to zostało pokazane poniżej:

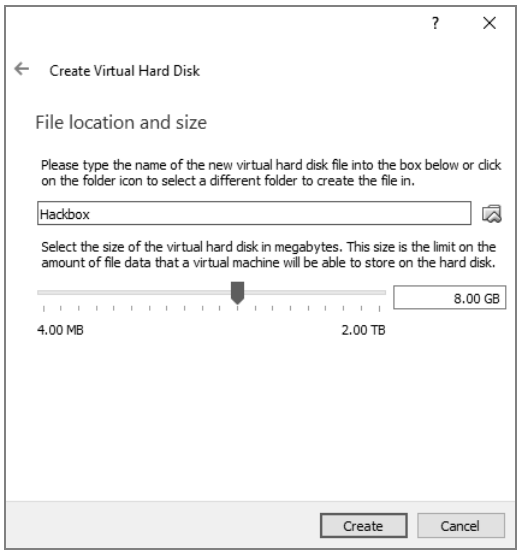
Kolejnym krokiem będzie utworzenie maszyny wirtualnej i zainstalowanie w niej systemu Kali Linux. Aby to zrobić, naciśnij przycisk *New* (nowy), znajdujący się na pasku narzędzi programu VirtualBox. Na ekranie powinno się pojawić okno kreatora tworzenia nowej maszyny wirtualnej. W polu *Name* (nazwa) wpisz żądaną nazwę maszyny (na przykład *HackBox*), a następnie w zależności od pobranej wersji systemu Kali Linux wybierz odpowiedni typ maszyny wirtualnej, na przykład *Debian (64-bit)* albo *Debian (32-bit)* (zobacz rysunek poniżej).



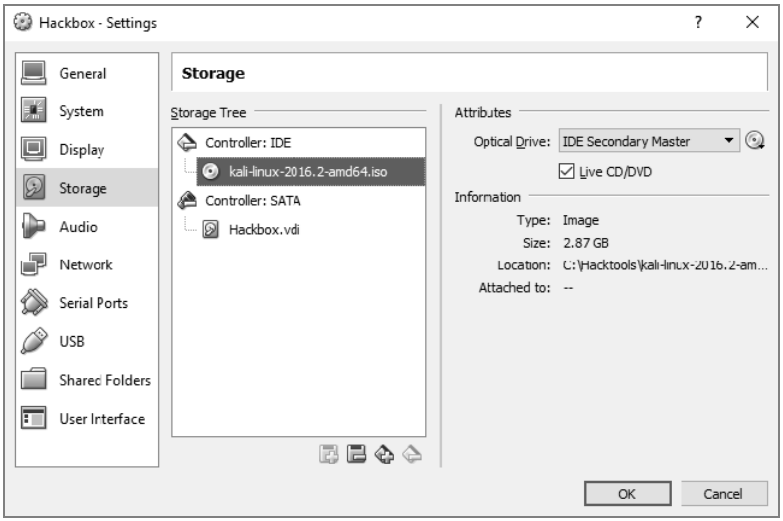
Naciśnij przycisk *Next* i podaj żądany rozmiar pamięci RAM dla systemu Kali Linux. Rekomendowana wielkość to co najmniej 1 GB. W kolejnym kroku utworzymy wirtualny dysk twardy dla instalowanego systemu. Naciśnij przycisk *Next* i wybierz typ dysku; w większości przypadków będziemy korzystać z domyślnej opcji *VDI (VirtualBox Disk Image)*, tak jak to zostało pokazane na pierwszym rysunku na następnej stronie.



Naciśnij przycisk *Next* i w kolejnym oknie kreatora wybierz rozmiar dysku twardego, który zostanie utworzony (zobacz rysunek poniżej):



Na koniec musimy przejść do ustawień maszyny wirtualnej *HackBox* (opcja *Settings*) i podłączyć instalacyjny obraz ISO systemu Kali Linux jako dysk zewnętrzny, tak jak to zostało pokazane na pierwszym rysunku na następnej stronie.



Gotowe. Po uruchomieniu maszyny wirtualnej na ekranie powinno się pojawić okno, w którym z menu uruchomieniowego możesz wybrać opcję uruchomienia wersji Live lub zainstalowania systemu Kali Linux na dysku (zobacz rysunek poniżej):

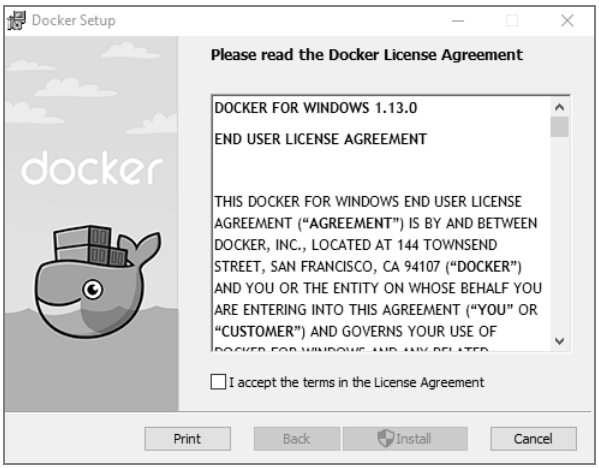
Instalowanie aplikacji Docker

Docker to aplikacja typu *open source* pozwalająca na tworzenie, dostarczanie i uruchamianie aplikacji w tzw. kontenerach. Docker zapewnia również dodatkową warstwę abstrakcji i automatyzacji na poziomie wirtualizacji systemu operacyjnego.

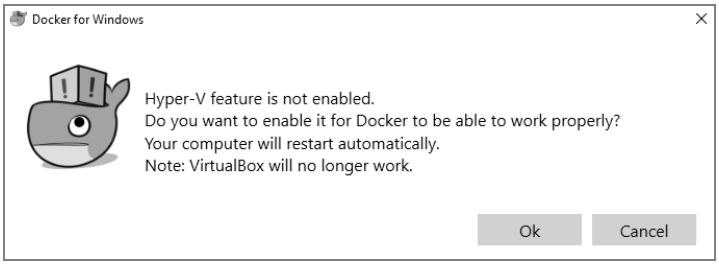
Docker jest dostępny w wersjach dla systemów Windows, macOS, AWS (ang. *Amazon Web Services*) oraz Azure. Dla systemu Windows pakiet Docker możesz pobrać z następującego adresu URL:

https://download.docker.com/win/stable/InstallDocker.msi

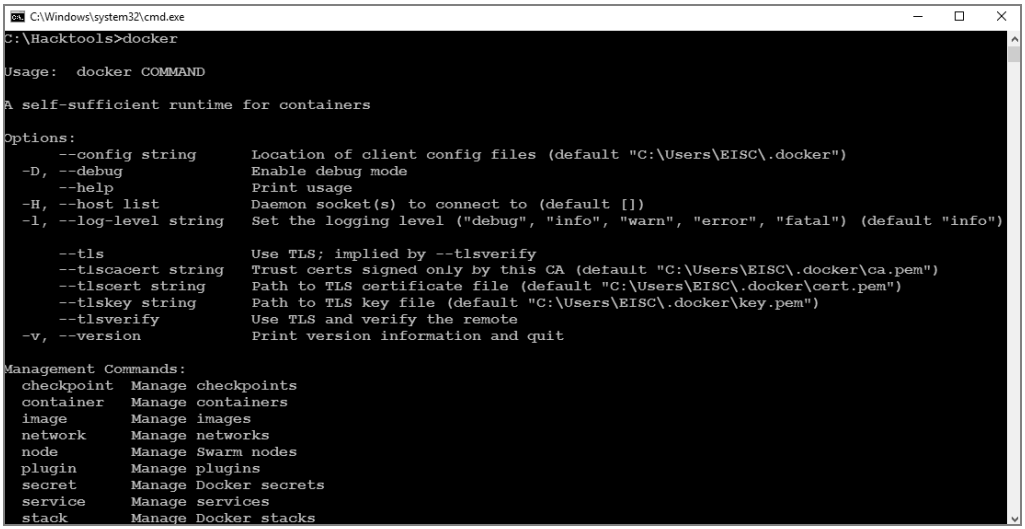
Poniżej pokażemy, w jaki sposób możesz zainstalować pakiet Docker na komputerze działającym pod kontrolą systemu Windows 10:



Docker wykorzystuje mechanizm Hyper-V systemu Microsoft Windows. Jeżeli Hyper-V nie jest włączony, to najprawdopodobniej na ekranie pojawi się następujący komunikat:



Po naciśnięciu przycisku *Ok* mechanizm Hyper-V zostanie włączony i będziesz mógł sprawdzić działanie programu Docker, uruchamiając konsolę i wykonując polecenie `docker`, tak jak to zostało pokazane na rysunku:



Na tym proces instalowania aplikacji Docker zostaje zakończony. Teraz musimy zainstalować system Kali Linux. Aby to zrobić, powinieneś z poziomu konsoli wykonać polecenie `docker pull kalilinux/kali-linux-docker`, tak jak to zostało pokazane na rysunku poniżej:

Po załadowaniu systemu Kali Linux do aplikacji Docker powinieneś być w stanie uruchomić powłokę `bash` z pobranego kontenera Kali Docker poprzez wykonanie polecenia `run -t -i kalilinux/kal-linux-docker /bin/bash`, tak jak to zostało pokazane na rysunku poniżej:

System Kali Linux możesz teraz uruchomić bezpośrednio z poziomu kontenera Docker. Zwróć uwagę, że Docker wykorzystuje pracujące w tle środowisko VirtualBox, zatem w takiej sytuacji nasza maszyna wirtualna z systemem Kali Linux działa w środowisku VirtualBox za pośrednictwem kontenera Docker.

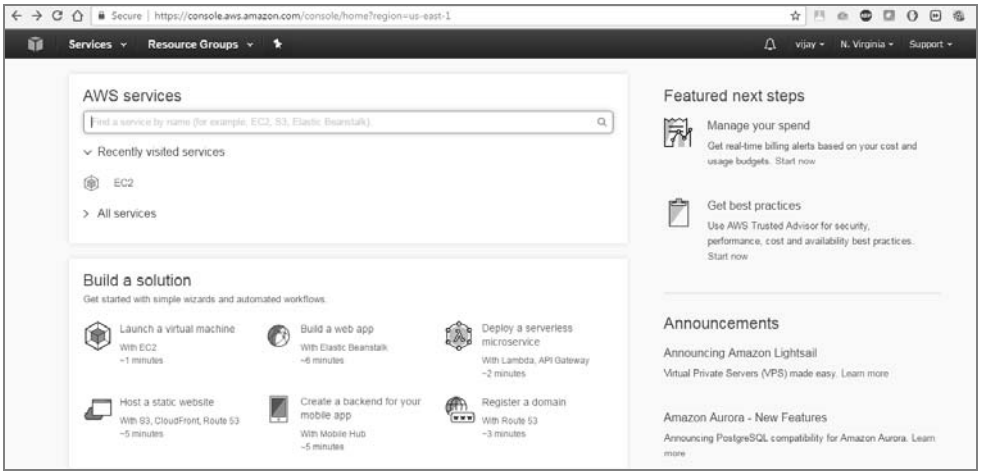
Instalowanie systemu Kali Linux w chmurze — tworzenie instancji AWS

AWS to opracowana przez firmę Amazon platforma oparta na technologii chmury, której podstawowym przeznaczeniem jest udostępnianie użytkownikom mocy obliczeniowej, przestrzeni dyskowej oraz dostarczanie treści. Jako pentester możesz wykorzystać AWS do przeprowadzania testów penetracyjnych. W tym podrozdziale pokażemy najłatwiejszą metodę zainstalowania systemu Kali Linux w chmurze AWS, co może być bardzo użyteczne w przypadku korzystania z zewnętrznych serwerów C2 (ang. *command and control*).

Najpierw musimy utworzyć swoje konto na platformie AWS. Aby to zrobić, powinieneś odwiedzić następującą stronę internetową:

https://console.aws.amazon.com/console/home

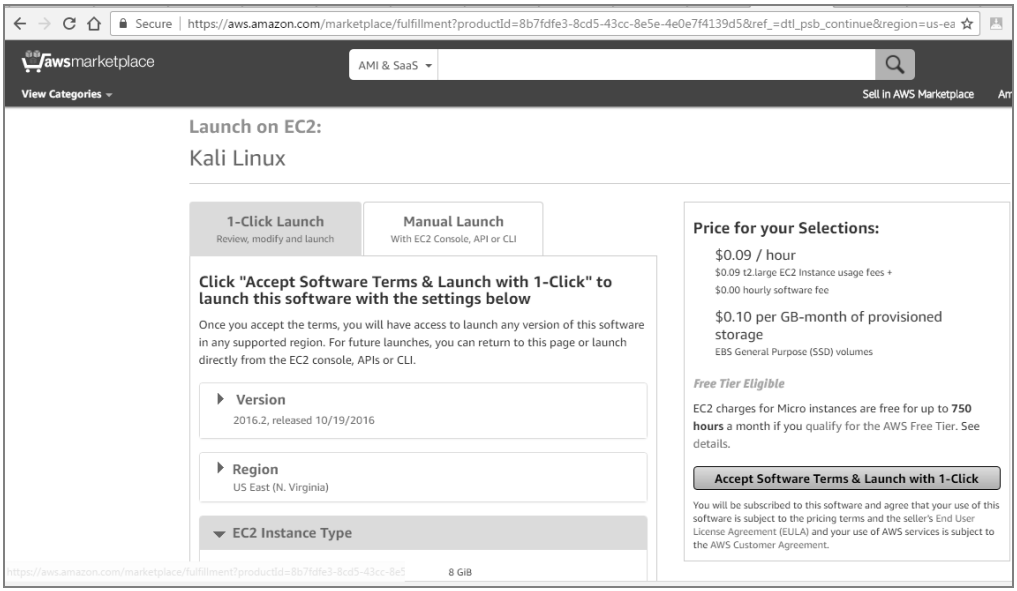
Po zalogowaniu się na konto AWS możesz zobaczyć listę wszystkich dostępnych usług, tak jak to zostało pokazane na rysunku poniżej:



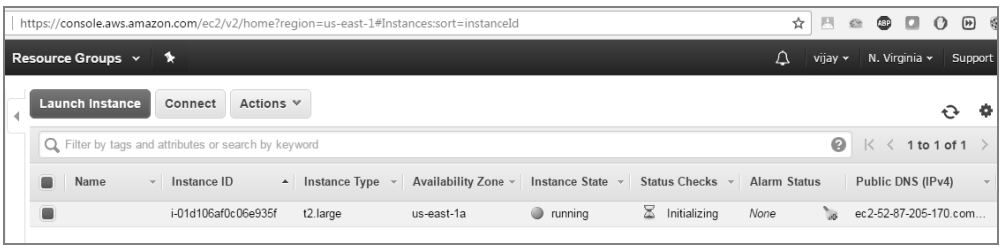
Kolejnym krokiem będzie uruchomienie systemu Kali Linux na platformie AWS. Zrobimy to, korzystając z odpowiednio dostosowanej wersji systemu Kali Linux bazującej na dystrybucji Debian. Dzięki społeczności programistów open source możemy w bardzo prosty sposób uruchomić prekonfigurowaną wersję systemu Kali Linux 2016.2 za pośrednictwem platformy Amazon Marketplace. Adres URL przedstawiony poniżej pozwoli Ci na szybkie uruchomienie systemu Kali Linux:

https://aws.amazon.com/marketplace/pp/B01M26MMTT

Po jego uruchomieniu w oknie przeglądarki powinna się pojawić strona, która będzie wyglądała mniej więcej tak:



Naciśnij przycisk *Accept Software Terms & Launch with 1-Click* (zaakceptuj warunki licencji i uruchom jednym kliknięciem), a następnie przejdź do konsoli AWS, odwiedzając stronę *https://console.aws.amazon.com/ec2/v2/home?region=us-east-1*. Teraz powinieneś być już w stanie uruchomić wybraną instancję systemu Kali Linux, wybierając odpowiedni wiersz lub identyfikator instancji (ang. *Instance ID*) i naciskając przycisk *Launch Instance* (uruchom instancję), tak jak to zostało pokazane na rysunku poniżej:



Teraz musisz utworzyć parę kluczy, co zagwarantuje, że tylko Ty będziesz miał dostęp do tej instancji systemu Kali Linux. Po utworzeniu będziesz mógł zalogować się do konta w chmurze AWS za pomocą swojego wygenerowanego wcześniej klucza prywatnego. Aby to zrobić, powinieneś z poziomu wiersza poleceń powłoki wykonać następującą komendę:

```
ssh -i klucz_prywatny.pem ec2-user@ip_serwera_DNS_Amazon
```

Pojawienie się ekranu pokazanego na następnej stronie będzie świadczyło o tym, że pomyślnie zainstalowałeś system Kali Linux w chmurze AWS:

Aby legalnie używać zasobów chmury AWS do przeprowadzania testów penetracyjnych, musisz przestrzegać wszystkich postanowień i warunków licencji. Przed rozpoczęciem jakichkolwiek testów czy ataków musisz też posiadać wszystkie wymagane prawem zgody i spełnić wszystkie inne niezbędne warunki prawne.

Dostosowywanie systemu Kali Linux

Zainstalowanie systemu Kali Linux to zaledwie początek, ponieważ równie ważnym, o ile nie ważniejszym etapem jest odpowiednie skonfigurowanie i dostosowanie systemu do własnych potrzeb i wymagań. W tym podrozdziale szczegółowo omówimy proces konfigurowania tego systemu.

Konfigurowanie i dostosowywanie systemu Kali Linux

Kali Linux to system wspomagający przeprowadzanie testów penetracyjnych. Jednak aby taki system był efektywny, pentester nie może się czuć w żaden sposób związany czy ograniczony przez domyślnie zainstalowane narzędzia czy domyślną konfigurację interfejsu użytkownika i pulpitu. Dostosowując system Kali Linux do własnych potrzeb i wymagań, pentester może polepszyć poziom zabezpieczenia danych na temat środowiska celu, zbieranych podczas testów penetracyjnych, a także znacząco ułatwić ich przeprowadzanie.

Najczęściej podczas dostosowywania systemu Kali Linux wykonywane są następujące operacje:

- Resetowanie i zmiana hasła użytkownika *root*.
- Dodawanie innych kont użytkowników, którzy nie posiadają uprawnień użytkownika *root*.
- Optymalizacja i przyspieszanie działania systemu Kali Linux.
- Udostępnianie i współużytkowanie wybranych folderów z systemem Windows.
- Tworzenie zaszyfrowanych folderów.

Zmiana hasła użytkownika root

Aby zmienić hasło użytkownika *root*, powinieneś wykonać następujące polecenie:

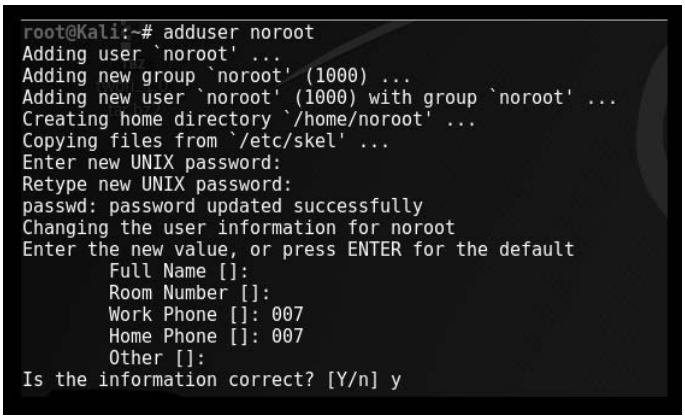
```
passwd root
```

System poprosi o wpisanie nowego hasła, tak jak to zostało pokazane na rysunku poniżej:

Dodawanie zwykłego konta użytkownika

Bardzo wiele narzędzi dostępnych w systemie Kali Linux musi być uruchamianych na prawach użytkownika *root*. Ciągła praca z uprawnieniami użytkownika *root* niesie jednak ze sobą poważne zagrożenia, na przykład prosta pomyłka czy błąd podczas wpisywania nazwy polecenia może skutkować awarią danej aplikacji czy nawet uszkodzeniem testowanego systemu. W niektórych przypadkach preferowanym rozwiązaniem jest wcześniejsze sprawdzenie działania polecenia na prawach zwykłego użytkownika. Warto zauważyć, że niektóre aplikacje wręcz wymuszają uruchamianie z poziomu użytkownika o niższych uprawnieniach niż administrator systemu.

Aby utworzyć konto zwykłego użytkownika, możesz po prostu z poziomu konsoli użyć polecenia `adduser`, a następnie postępować według poleceń pojawiających się na ekranie, tak jak to zostało pokazane na rysunku poniżej:

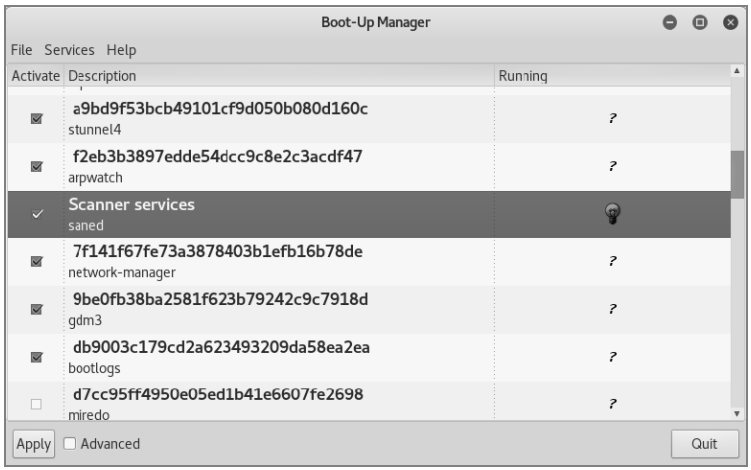


Przyspieszanie działania systemu Kali Linux

Istnieje co najmniej kilka narzędzi, których możesz używać do optymalizacji i przyspieszania działania systemu Kali Linux:

- Jeżeli korzystasz z systemu Kali Linux działającego w maszynie wirtualnej, powinieneś dodatkowo zainstalować w niej pakiet Guest Additions (VirtualBox) lub VMware Tools (VMware). Pamiętaj, aby przed instalacją dodatkowo wykonać polecenie `apt-get update`.
- Kiedy tworzysz nową maszynę wirtualną, powinieneś zamiast dysku alokowanego dynamicznie wybrać dysk twardy o stałej wielkości. Takie rozwiązanie powoduje szybsze zapisywanie plików na dysku i zmniejsza ich fragmentację.
- Aplikacja `preload` identyfikuje najczęściej wykorzystywane przez użytkownika programy i przyspiesza działanie systemu poprzez wcześniejsze buforowanie odpowiednich plików wykonywalnych i zależności. Aby ją zainstalować, powinieneś wykonać polecenie `apt-get install preload`. Po zainstalowaniu i zrestartowaniu systemu aplikacja działa całkowicie automatycznie.
- BleachBit (`apt-get install bleachbit`) to aplikacja, która optymalizuje działanie systemu poprzez zwalnianie niepotrzebnie zajętych zasobów dyskowych, usuwanie ciasteczek, czyszczenie historii przeglądania sieci internet, usuwanie plików tymczasowych, kasowanie logów oraz innych niepotrzebnych plików. Oprócz tego aplikacja posiada kilka dodatkowych, przydatnych funkcji, takich jak usuwanie plików metodą nadpisywania — co uniemożliwia ich odzyskanie — czy nadpisywanie niealokowanej przestrzeni dyskowej — co powoduje definitywne usunięcie resztek danych pozostawionych przez skasowane wcześniej pliki.

- Domyślnie Kali Linux nie wyświetla wszystkich aplikacji uruchamianych podczas ładowania systemu. Każda aplikacja ładowana i uruchamiana podczas bootowania systemu wydłuża ten proces, może zabierać cenne zasoby i wpływać na zmniejszenie wydajności działania systemu. Aby przeglądać listę takich programów i zablokować aplikacje niepotrzebnie ładowane podczas uruchamiania systemu, powinieneś zainstalować program *Boot Up Manager (BUM)*, pokazany na rysunku poniżej. Aby to zrobić, powinieneś wykonać polecenie `apt-get install bum`.



- Zainstaluj program `gnome-do` (`apt-get install gnome-do`), który pozwala na uruchamianie aplikacji bezpośrednio z poziomu klawiatury. Aby ją skonfigurować, musisz ją uruchomić z menu *Applications/Accessories* (aplikacje/akcesoria), a następnie wybrać menu *Preferences* (właściwości), aktywować opcję *Quiet Launch* (ciche uruchamianie), wybrać uruchamiającą kombinację klawiszy (na przykład *Ctrl+Shift*) i wpisać wiersz polecenia, który powinien zostać wykonany po naciśnięciu tej kombinacji.
- Pamiętaj, że do wykonywania bardziej złożonych operacji możesz używać nie tylko skrótów klawiszowych, ale też odpowiednio przygotowanych skryptów powłoki.

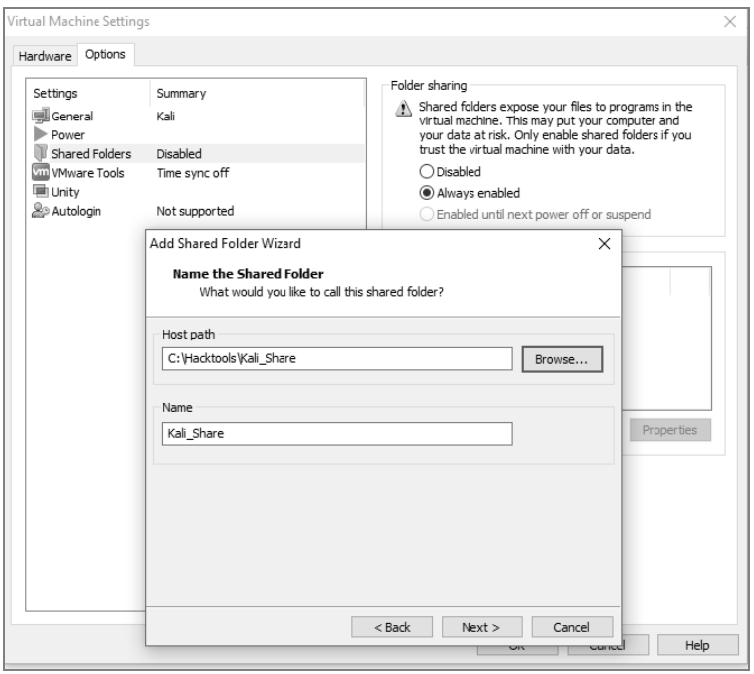
Udostępnianie i współużytkowanie folderów z systemem operacyjnym hosta

System Kali Linux pozwala na udostępnianie plików i danych aplikacjom działającym pod kontrolą innych systemów operacyjnych, a zwłaszcza systemu Microsoft Windows. Najbardziej efektywnym sposobem udostępniania danych jest utworzenie dedykowanego foldera, który będzie dostępny zarówno z poziomu systemu operacyjnego hosta, jak i z poziomu systemu Kali Linux działającego w maszynie wirtualnej.

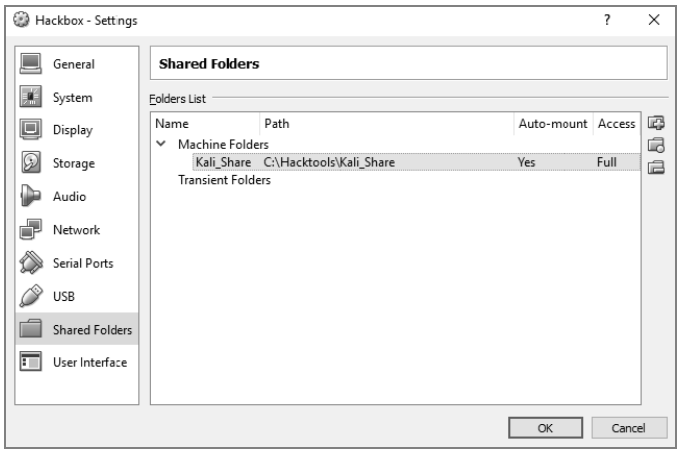
Kiedy w takim współdzielonym folderze zostaną umieszczone jakieś pliki, stają się one natychmiast dostępne dla wszystkich innych systemów korzystających z tego foldera.

Aby utworzyć taki współdzielony folder, powinieneś wykonać następujące polecenia:

1. Utwórz folder w systemie plików hosta. W naszym przypadku utworzymy folder o nazwie *Kali_Share*.
2. Kliknij nowo utworzony folder prawym przyciskiem myszy i wybierz polecenie *Sharing* (udostępnianie).
3. Włącz udostępnianie foldera i upewnij się, że dostęp będą mieli wszyscy użytkownicy (*Everyone*), a poziom uprawnień ustawiony jest na prawo odczytu i zapisu (*Read/Write*).
4. Jeżeli jeszcze tego nie zrobiłeś, zainstaluj w maszynie wirtualnej dodatki Guest Additions (dla VirtualBox) lub VMware Tools (dla VMware); więcej szczegółowych informacji na ten temat znajdziesz w dodatku, w sekcji „Instalowanie systemu Kali Linux".
5. Po zakończeniu instalacji przejdź do menu głównego VMware, wybierz polecenie *Manage/Virtual Machine Settings* (zarządzaj/ustawienia maszyny wirtualnej), przejdź na kartę *Options* (opcje), kliknij kategorię *Shared Folders* (foldery współdzielone) i zaznacz opcję *Always Enabled* (zawsze włączone). Wybierz katalog w systemie plików hosta, który ma być współdzielony, tak jak to zostało pokazane na rysunku poniżej:



6. Jeżeli używasz programu Oracle VirtualBox, zaznacz maszynę wirtualną, wybierz polecenie *Settings* (ustawienia), zaznacz opcję *Shared Folders* (foldery współdzielone) i wybierz katalog w systemie plików hosta, który ma być współdzielony, tak jak to zostało pokazane na rysunku poniżej:



W starszych wersjach programu VMware Player menu wygląda nieco inaczej.

7. Przejdź do systemu Kali Linux w maszynie wirtualnej i uruchom przeglądarkę plików. Wybrany współdzielony katalog powinien być widoczny w folderze *mnt* (lub w jego subfolderze *hgfs*).
8. Przeciągnij ikonę współdzielonego foldera na pulpit systemu Kali Linux, aby utworzyć na nim skrót do tego foldera.
9. Od tej chwili wszystkie pliki, jakie umieścisz we współdzielonym folderze, będą dostępne zarówno dla systemu Kali Linux, jak i z poziomu systemu operacyjnego hosta maszyny wirtualnej.

Pamiętaj, że jeżeli we współdzielonym folderze chcesz przechowywać wrażliwe dane pozyskane w trakcie przeprowadzania testu penetracyjnego, to zawartość takiego foldera powinna być zaszyfrowana. Dzięki temu wrażliwe dane klienta będą lepiej zabezpieczone i chronione przed przypadkowym wyciekiem, gdyby zawierający je dysk został zagubiony lub skradziony.

Dostosowywanie systemu Kali Linux do własnych potrzeb przy użyciu skryptów powłoki bash

W systemie Linux dostępnych jest wiele różnych rodzajów powłok, za pomocą których możemy korzystać z systemu z poziomu wiersza poleceń konsoli. Najczęściej możemy spotkać powłoki *sh*, *bash*, *csh*, *tcsh* oraz *ksh*.

W zależności od celu przeprowadzanego testu penetracyjnego do dostosowania systemu Kali Linux do własnych potrzeb możemy użyć jednego z następujących skryptów powłoki *bash*:

- *https://github.com/leebaird/discover/blob/master/update.sh*
- *https://code.google.com/archive/p/lazykali/downloads*

Budowanie środowiska testowego

Każdy pentester powinien utworzyć swoje własne środowisko testowe, w którym będzie można testować różne podatności i luki w zabezpieczeniach przed dokonaniem próby ich wykorzystania podczas rzeczywistego testu penetracyjnego w środowisku klienta.

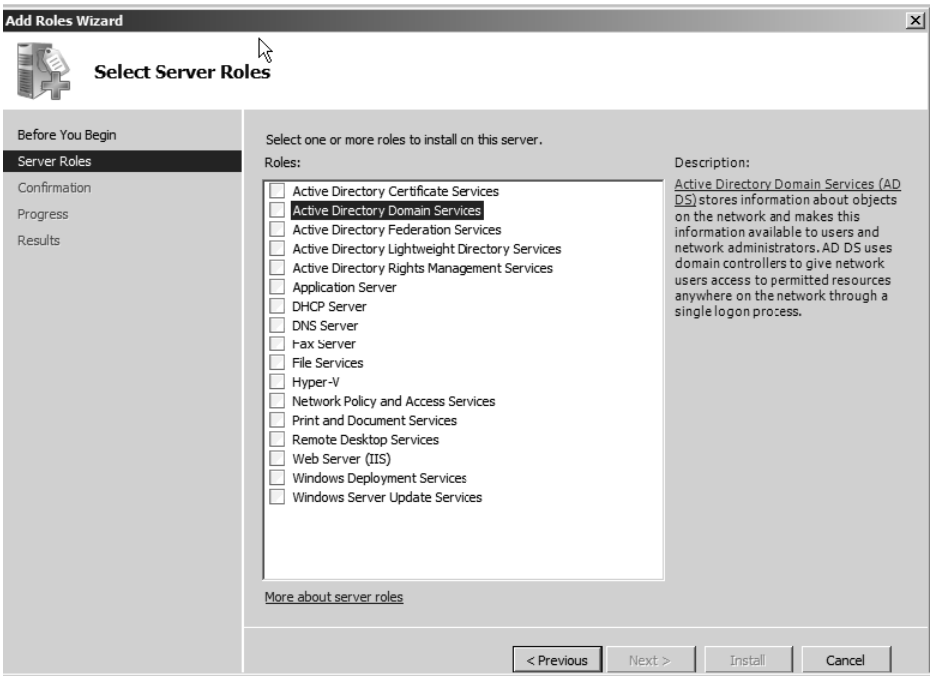
Konfigurowanie sieci wirtualnej z usługą Active Directory

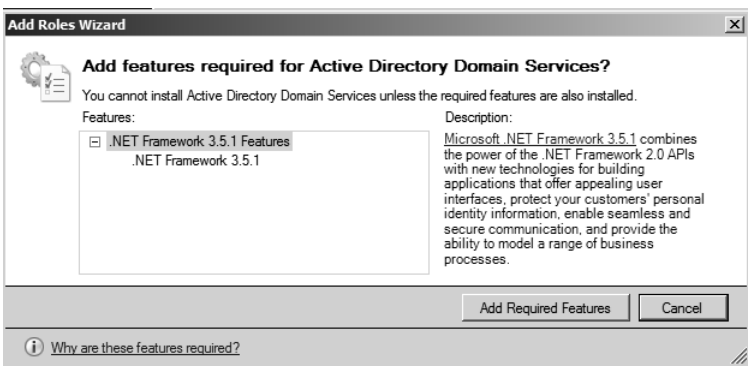
Zdecydowana większość dużych firm i organizacji do zarządzania kontami użytkowników, zasobami plikowymi, czy drukarkami sieciowymi wykorzystuje w swoich środowiskach usługę Microsoft Active Directory. Potencjalni napastnicy obecnie nie są już zainteresowani wyłącznie możliwością wykonywania poleceń na skompromitowanym serwerze, ponieważ znacznie bardziej atrakcyjnym dla nich celem może być przejęcie kontroli nad kontrolerem domeny, który spełnia rolę swego rodzaju podwójnej helisy DNA dla całej firmy. W dalszej części książki będziemy opisywać niektóre zaawansowane ataki na usługę Active Directory oraz serwery DNS danego środowiska. W tej sekcji pokażemy, jak zainstalować usługę Active Directory na serwerze Windows 2008 R2.

Najpierw musimy w naszym środowisku testowym zainstalować serwer Windows 2008 R2. Aby to zrobić, musimy wykonać takie same kroki, jakie wykonywaliśmy podczas instalowania systemu Kali Linux.

Następnie na ekranie pojawi się kreator, który krok po kroku przeprowadzi nas przez proces instalowania usług Active Directory Domain Services. Załóżmy zatem, że serwer Windows 2008 R2 mamy już zainstalowany i na ekranie pojawił się kreator instalowania usług Active Directory. Kliknij polecenie *Server Manager* (zarządzanie serwerem), przejdź do opcji *Roles* (role), a następnie wybierz polecenie *Add Roles* (dodaj role). Na ekranie pojawi się pierwszy krok kreatora, *Before you begin* (zanim rozpoczniesz). Naciśnij przycisk *Next* (dalej), a na ekranie zobaczysz okno przedstawione na pierwszym rysunku na następnej stronie.

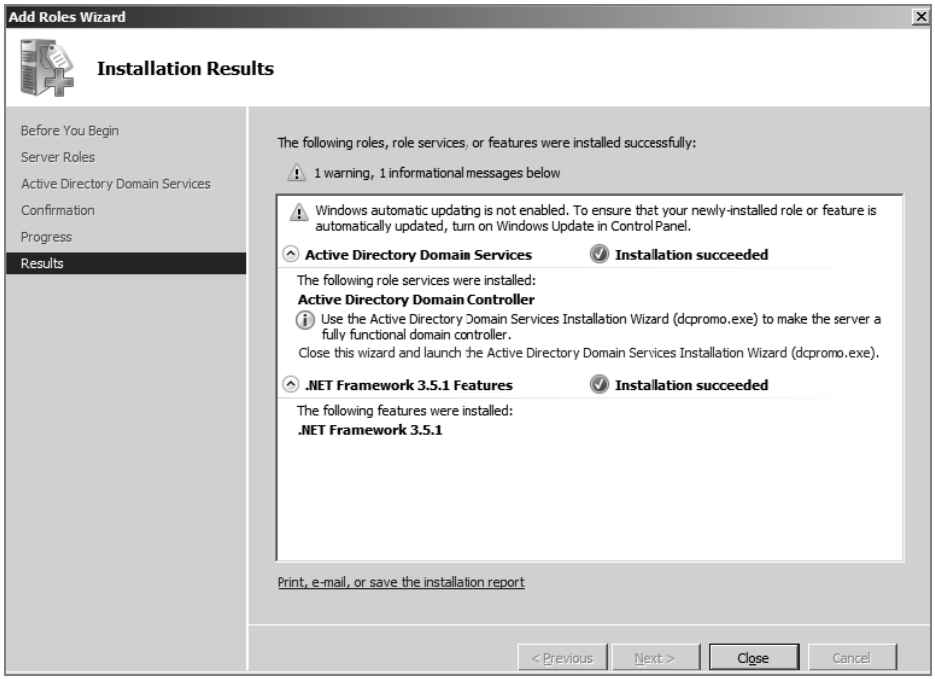
Zaznacz opcję *Active Directory Domain Services* (domenowe usługi Active Directory). Istnieje duże prawdopodobieństwo, że po wybraniu tej opcji na ekranie pojawi się komunikat z prośbą o zainstalowanie pakietu Microsoft .NET Framework 3.5.1, który jest niezbędny do poprawnego działania usług Active Directory. Naciśnij przycisk *Add Required Features* (dodaj wymagane komponenty), tak jak to zostało pokazane na drugim rysunku na następnej stronie.





Aby rozpocząć instalowanie, naciśnij przycisk *Install* (instaluj). Wybrane komponenty zostaną zainstalowane i na ekranie pojawi się okno z informacją o pomyślnym zakończeniu procesu instalacji usług Active Directory, tak jak to zostało pokazane na pierwszym rysunku na następnej stronie.

Po zakończeniu instalacji usług Active Directory musimy się upewnić, że wszystko działa poprawnie. Aby to zrobić, musimy kliknąć przycisk uruchamiający kreatora usług *Active Directory Domain Services* i utworzyć nowy las AD (ang. *Active Directory Forest*). W naszym przypadku będziemy tworzyć nowy las, którego pełna nazwa domenowa FQDN (ang. *Fully Qualified Domain Name*) to *Secure.kali.com*. Nazwę domeny NetBIOS ustawiamy na *Secure*, następnie



ustawiamy poziom funkcjonalności lasu (ang. *forest functional level*) na `Windows 2003` lub `Windows 2008 R2`, co spowoduje uruchomienie konfiguracji serwera DNS (ang. *Domain Name Server*). Ponieważ w naszym przypadku mamy zupełnie nową instancję domeny, musimy dopiero zainstalować serwer DNS i następnie przy użyciu kreatora ustawić nową domenę na *secure.kali.com*, tak jak to zostało pokazane na rysunku poniżej:

Instalowanie zdefiniowanych celów

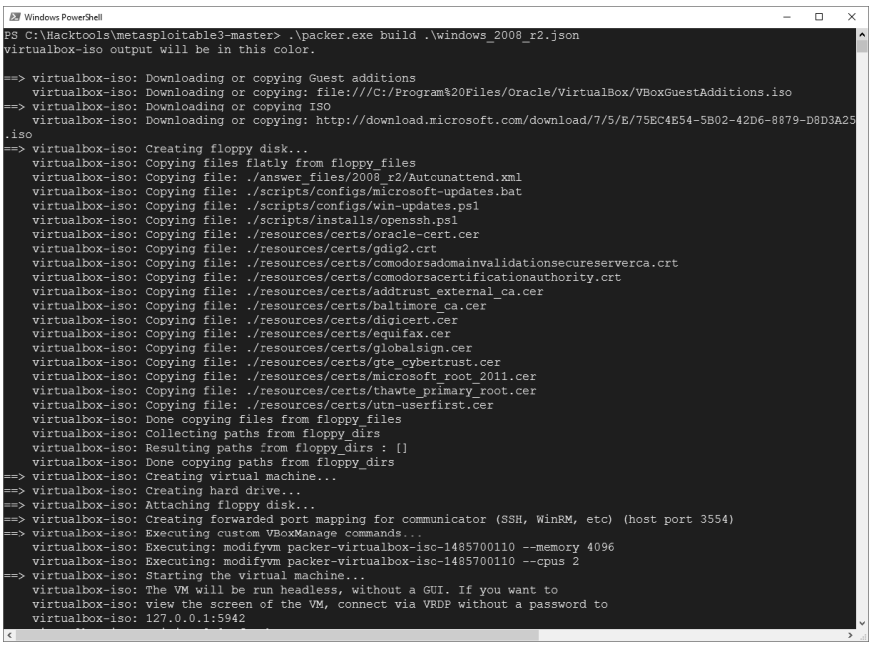
To praktyka sprawia, że człowiek staje się doskonały. Aby zatem wprawiać się w sztuce przełamywania zabezpieczeń, powinieneś użyć oprogramowania, które posiada szereg dobrze znanych i opisanych podatności i luk w zabezpieczeniach. W tej sekcji pokażemy, jak możesz zainstalować pakiet metasploitable3 (platforma Windows) oraz Mutillidae (aplikacja sieciowa PHP).

Metasploitable3

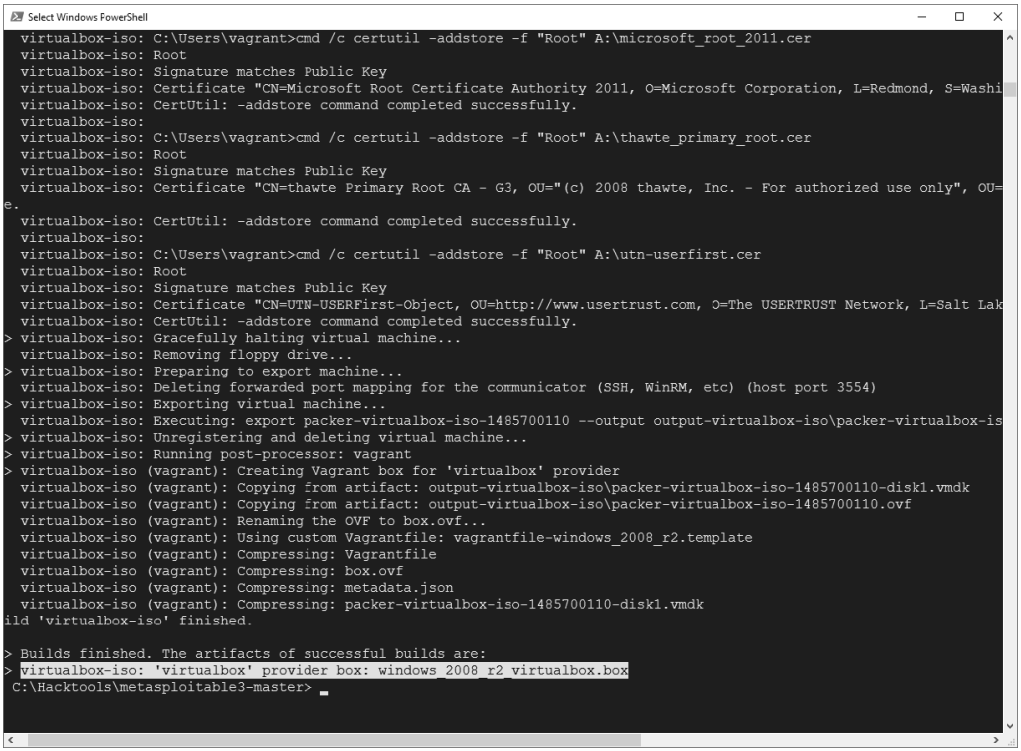
Metasploitable3 to maszyna wirtualna działająca pod kontrolą systemu Windows i celowo wyposażona w szereg podatności i luk w zabezpieczeniach, przeznaczona do wspomagania ćwiczeń w wykrywaniu i wykorzystywaniu luk w zabezpieczeniach przy użyciu pakietu Metasploit. Pakiet jest udostępniany na licencji opartej na licencji BSD. Maszynę wirtualną Metasploitable3 można pobrać ze strony *https://github.com/rapid7/metasploitable3*. W zależności od potrzeb możesz pobrać archiwum ZIP i rozpakować je do wybranego foldera w swoim systemie Windows (w naszym przypadku zazwyczaj umieszczamy pliki w folderze *C:\HackTools*) lub z poziomu konsoli użyć polecenia `git clone`.

Powinieneś również zainstalować wszystkie dostępne pomocnicze pakiety oprogramowania, takie jak Packer, Vagrant, VirtualBox czy wtyczka Vagrant.

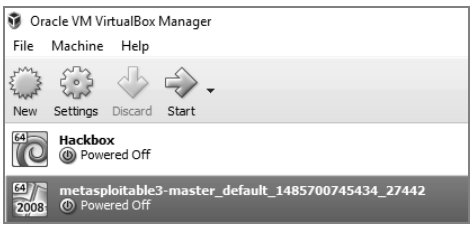
Na rysunku zamieszczonym poniżej przedstawiamy proces ręcznej instalacji pakietu Metasploitable3 na platformie Windows 10.



Po zakończeniu pobierania pliku ISO zawierającego obraz maszyny wirtualnej w oknie konsoli zostanie wyświetlony komunikat przedstawiony na rysunku poniżej:



Po zakończeniu pobierania pliku maszyny wirtualnej musisz jeszcze tylko z poziomu tej samej konsoli PowerShell uruchomić polecenie `vagrant up`, które powinno dodać nową maszynę wirtualną do konsoli VirtualBox, tak jak to zostało pokazane na rysunku poniżej:

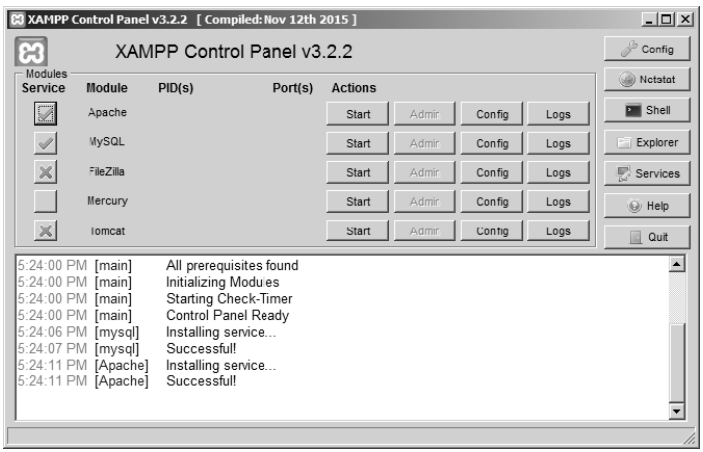


Mutillidae

Mutillidae to wyposażona w szereg podatności i luk w zabezpieczeniach aplikacja sieciowa typu open source, która jest przeznaczona do wspomagania ćwiczeń w wykrywaniu i wykorzystywaniu luk w zabezpieczeniach aplikacji sieciowych.

XAMPP to inna bezpłatna aplikacja typu open source, opracowana przez zespół programistów Apache Friends, którą możesz pobrać ze strony *https://www.apachefriends.org/download.html*.

Teraz zainstalujemy aplikację Mutillidae na naszym nowo zainstalowanym serwerze Microsoft Windows 2008 R2. Po zakończeniu pobierania pakietu XAMPP uruchamiamy program instalacyjny i postępujemy zgodnie z poleceniami kreatora. Po zakończeniu instalacji uruchamiamy XAMPP; na ekranie powinno się pojawić okno przedstawione na rysunku poniżej:



Pakiet Mutillidae można pobrać ze strony *https://sourceforge.net/projects/mutillidae/files/latest/download*.

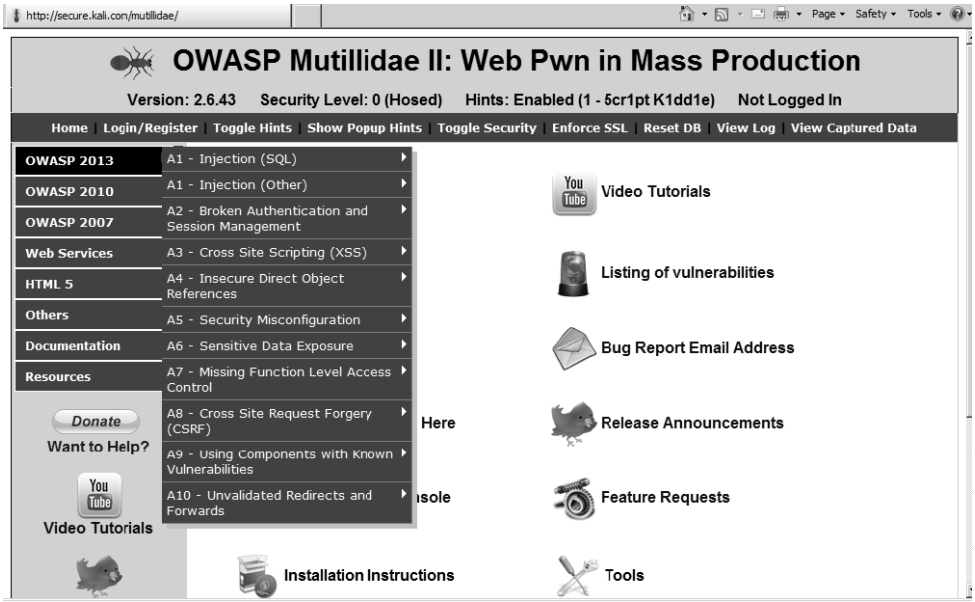
Po zakończeniu pobierania rozpakuj archiwum ZIP i skopiuj pliki do katalogu *c:**Lokalizacja XAMPP**\htdocs\<mutillidae>*.

Aby sprawdzić, czy aplikacja została zainstalowana pomyślnie, powinieneś uruchomić przeglądarkę sieciową i wpisać w niej adres przedstawiony na pierwszym rysunku na następnej stronie:

http://localhost/mutillidae/

Zarządzanie testami penetracyjnymi przy użyciu pakietu Faraday

Do najtrudniejszych aspektów przeprowadzania rozbudowanych testów penetracyjnych należą: konieczność przetestowania wszystkich istotnych elementów sieci i systemów środowiska celu, umiejętność zapamiętywania, które elementy systemu zostały już sprawdzone, oraz umiejętność określenia po zakończeniu testu, jakie operacje zostały przeprowadzone w trakcie jego trwania. W niektórych przypadkach klient może zażądać przeprowadzenia rozbudowanych

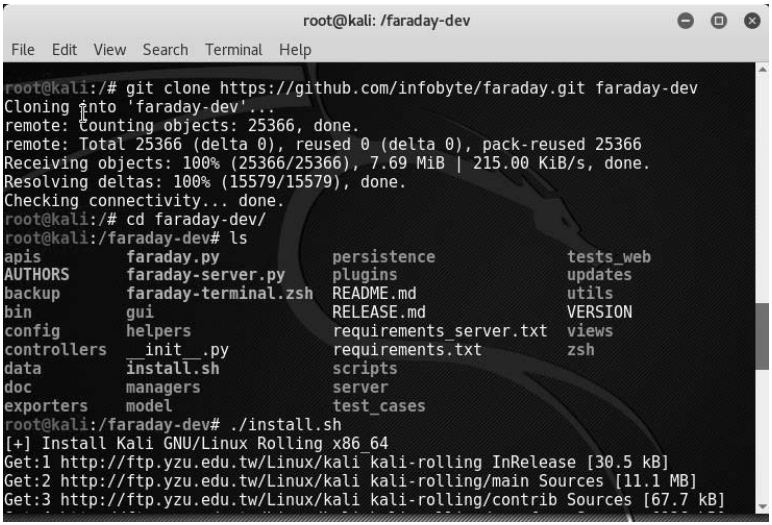


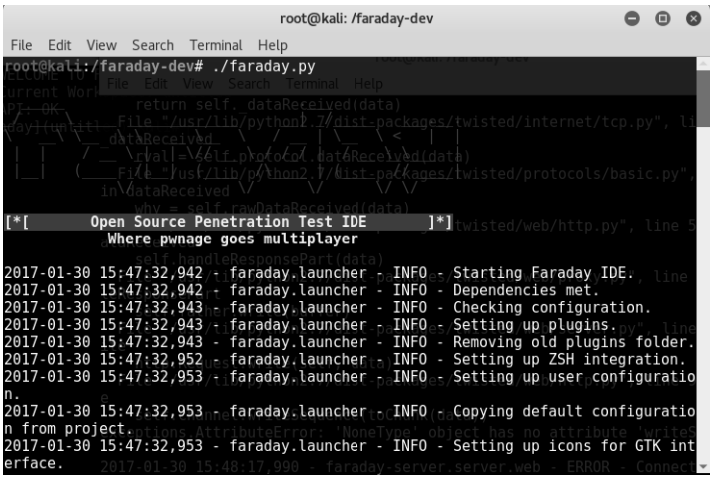
testów penetracyjnych, wymagających zatrudnienia wielu pentesterów operujących z różnych lokalizacji, a kierownictwo chce mieć możliwość zbiorczego monitorowania i koordynowania ich działań z jednego miejsca. Pakiet Faraday zapewnia pentesterom możliwość ujednolicenego widoku na testowane środowisko, przy założeniu, że mogą się oni ze sobą komunikować w danej sieci lokalnej lub sieci internet (w przypadku pentestów zewnętrznych).

Faraday to wieloużytkownikowe, zintegrowane środowisko IDE (ang. *Integrated Development Environment*) wspomagające przeprowadzanie testów penetracyjnych, które pozwala pentesterom na współużytkowanie, dystrybucję, indeksowanie i analizowanie wszelkich danych wygenerowanych lub pozyskanych podczas przeprowadzania testów penetracyjnych oraz przeprowadzanie audytów bezpieczeństwa i tworzenie raportów.

Środowisko Faraday IDE zostało zaprojektowane i napisane w języku Python przez programistów firmy Infobyte. Aplikację można pobrać ze strony *https://github.com/infobyte/faraday/wiki* lub bezpośrednio za pomocą polecenia `git clone`, tak jak to zostało pokazane na pierwszym rysunku na następnej stronie.

Po zakończeniu klonowania powinieneś wykonać polecenie `./install.sh`, które spowoduje również zainstalowanie wszystkich niezbędnych zależności. Nie zapomnij również uruchomić usługi CouchDB, ponieważ platforma Faraday wykorzystuje bazę danych CouchDB do przechowywania swoich danych. Na koniec powinieneś wykonać polecenie `faraday-server.py`, które spowoduje uruchomienie serwera Faraday. Aby uruchomić klienta środowiska, powinieneś z poziomu konsoli wykonać polecenie `faraday.py`, tak jak to zostało pokazane na drugim rysunku na następnej stronie.

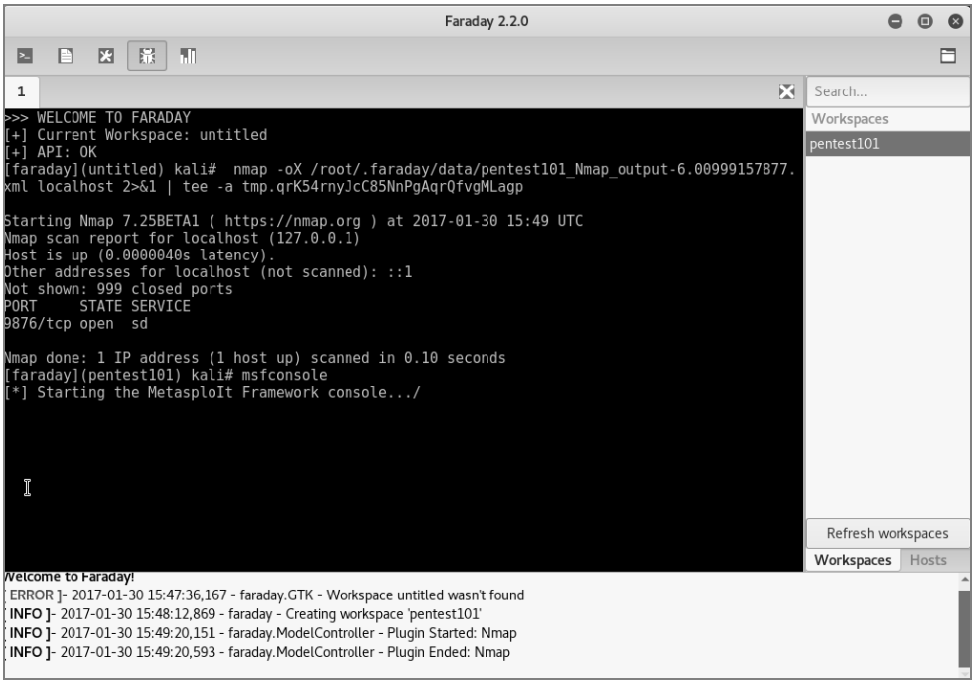


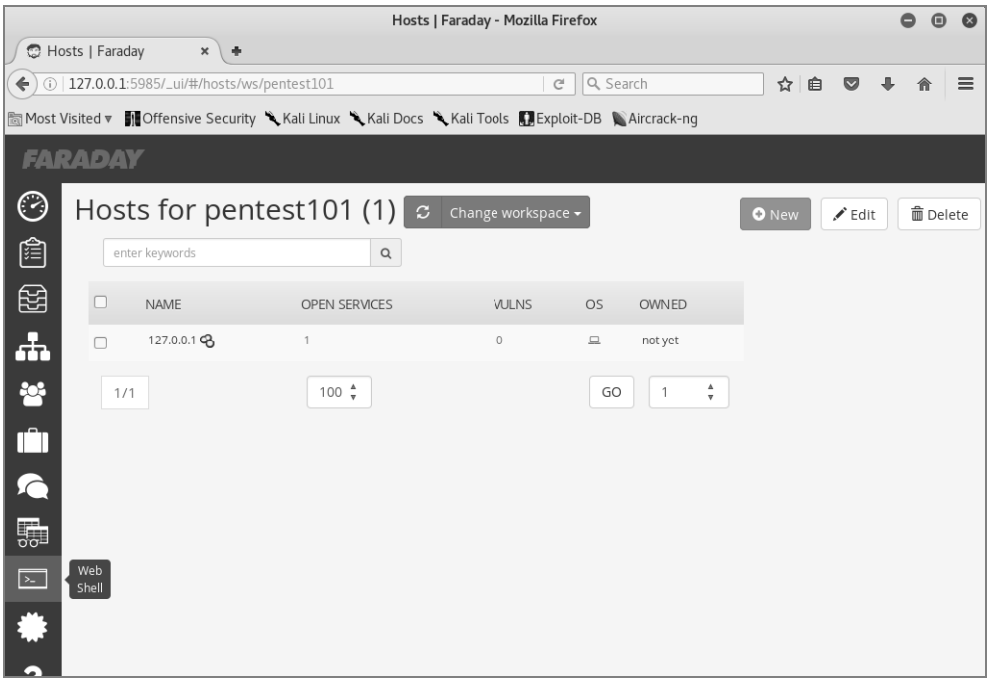


Uruchomienie klienta powinno spowodować otwarcie konsoli środowiska Faraday, tak jak to zostało pokazane na pierwszym rysunku na następnej stronie.

Jedną z wielkich zalet środowiska Faraday jest to, że po kliknięciu odpowiedniej opcji możemy od razu zobaczyć wizualizację wszystkich skanów i innych operacji wykonywanych przez Ciebie lub innych pentesterów pracujących nad tym projektem, tak jak to zostało pokazane na drugim rysunku na następnej stronie.

Choć pełna wersja pakietu Faraday jest produktem komercyjnym, to jednak nadal dostępna jest również bezpłatna wersja tego środowiska, która ma nieco ograniczone możliwości, ale nadal pozwala na wyświetlanie w jednym miejscu wszystkich informacji o wynikach przeprowadzanego testu penetracyjnego.





Podsumowanie

W tym rozdziale omawialiśmy różne metodologie testów penetracyjnych ukierunkowanych na osiągnięcie celu, które pozwalają firmom i organizacjom na sprawdzanie i szacowanie odporności ich środowiska na pełnowymiarowe ataki cybernetyczne. Pokazywaliśmy, jak pentesterzy mogą używać systemu Kali Linux do przeprowadzania testów bezpieczeństwa sieci i systemów w środowisku celu. Szczegółowo omówiliśmy proces instalowania systemu Kali Linux na różnych platformach wirtualizacyjnych i pokazywaliśmy, jak przy użyciu aplikacji Docker można szybko uruchomić system Linux na platformie Windows.

Zbudowaliśmy również nasze własne środowisko testowe, zainstalowaliśmy usługi Active Directory Domain Services oraz tak skonfigurowaliśmy dwie różne maszyny wirtualne, aby działały w tej samej sieci. Dowiedziałeś się również, jak można dostosować system Kali Linux do własnych, indywidualnych wymagań oraz jak zwiększyć bezpieczeństwo używanych narzędzi i pozyskiwanych przez nie danych. Pracowaliśmy nad osiągnięciem celu, jakim jest przygotowanie narzędzi wspierających nasz proces, a nie odwrotnie!

W kolejnym rozdziale dowiesz się, jak efektywnie używać narzędzi *Open Source Intelligence* (OSINT) do identyfikacji podatnej na atak powierzchni środowiska oraz jak tworzyć niestandardowe listy nazw użytkowników i haseł ułatwiających przeprowadzenie bardziej skoncentrowanych ataków oraz wykorzystywanie znalezionych podatności i luk w zabezpieczeniach.

Skorowidz

B

C

Ć

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

U

V

W

X

Z

Kali Linux — subtelne narzędzie pentestera!

Kali Linux jest dystrybucją BackTrack systemu Linux służącą do zaawansowanego badania zabezpieczeń systemów teleinformatycznych, również poprzez testy penetracyjne. Naturalnie, praca pentestera wiąże się również z przeprowadzaniem rozpoznania, skanowaniem w poszukiwaniu słabych stron zabezpieczeń, wykorzystywaniem exploitów, omijaniem zabezpieczeń i późniejszą eksploracją skompromitowanych systemów. W ten sposób diagnozuje się słabe strony systemu, co z kolei umożliwia usunięcie usterek i osiągnięcie wysokiego stopnia bezpieczeństwa. Realizacja tak ambitnego celu wymaga jednak znakomitego przygotowania i szerokiej wiedzy pentestera.

Dzięki tej książce poznasz sprawdzone techniki pokonywania mechanizmów obronnych różnych systemów za pomocą narzędzi dostępnych w Kali Linux. Dowiesz się, jak wybrać najbardziej efektywne rozwiązania, nauczysz się szybkiego skanowania sieci w poszukiwaniu luk w systemie zabezpieczeń, aż w końcu będziesz mógł przeprowadzić atak i powłamaniową eksplorację środowiska, przy czym będziesz wiedzieć, jakie techniki zminimalizują ryzyko wykrycia. Zapoznasz się ze specyfiką ataków na sieci bezprzewodowe, aplikacje internetowe i systemy wykorzystujące zdalny dostęp. W książce przedstawiono również zagadnienia związane z bezpieczeństwem fizycznym infrastruktury i z metodami socjotechnicznymi stosowanymi przez hakerów.

Najważniejsze zagadnienia:

- zarys metodologii testów penetracyjnych
- aktywne i pasywne rozpoznanie celu przed atakiem
- rozpoznawanie i przełamywanie zabezpieczeń
- powłamaniowa eksploracja celu i pozioma eskalacja ataku
- przejmowanie kontroli nad skompromitowanym systemem

Vijay Kumar Velu jest zapalonym praktykiem bezpieczeństwa teleinformatycznego. Ma ponad 11-letnie doświadczenie w branży IT. Zdobył wiele certyfikatów bezpieczeństwa, w tym Certified Ethical Hacker, EC-Council Certified Security Analyst i Computer Hacking Forensics Investigator. Jest członkiem zarządu Cloud Security Alliance (CSA) w Kuala Lumpur oraz członkiem National Cyber Defense and Research Center (NCDRC) w Indiach. Fanatyk technologii, kocha muzykę i chętnie angażuje się w działalność charytatywną.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
Sprawdź nasze szkolenia!
SZKOLENIA
AKADEMIA IT & BUSINESS
WWW.SZKOLENIA.HELION.PL
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-4037-4
9 788328 340374
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 69,00 zł
Packt