Kali – Wprowadzenie

Wprowadzenie

Kali po raz pierwszy wprowadzono w 2012 r. z całkowicie nową architekturą. Ta oparta na Debianie dystrybucja została wydana z ponad 300 narzędziami wyspecjalizowanymi w testach penetracyjnych i kryminalistyce cyfrowej. Jest utrzymywana i finansowana przez Offensive Security Ltd, a głównymi programistami są Mati Aharoni, Devon Kearns i Raphael Hertzog. Kali 2.0 pojawiło się w 2016 r. z mnóstwem nowych aktualizacji i nowymi środowiskami graficznymi, takimi jak KDE, Mate, LXDE, e17 i kompilacje Xfce. Podczas gdy Kali jest już wstępnie wyposażone w setki niesamowitych narzędzi i programów użytkowych, które pomagają testerom penetracyjnym na całym świecie wydajnie wykonywać swoją pracę, w tym rozdziale omówimy przede wszystkim kilka niestandardowych poprawek, które można wykorzystać, aby zapewnić użytkownikom jeszcze lepsze wrażenia z testów penetracyjnych.

Konfigurowanie Kali Linux

Użyjemy oficjalnego Kali Linux ISO dostarczonego przez Offensive Security do zainstalowania i skonfigurowania różnych środowisk graficznych, takich jak Mate, e17, Xfce, LXDE i KDE.

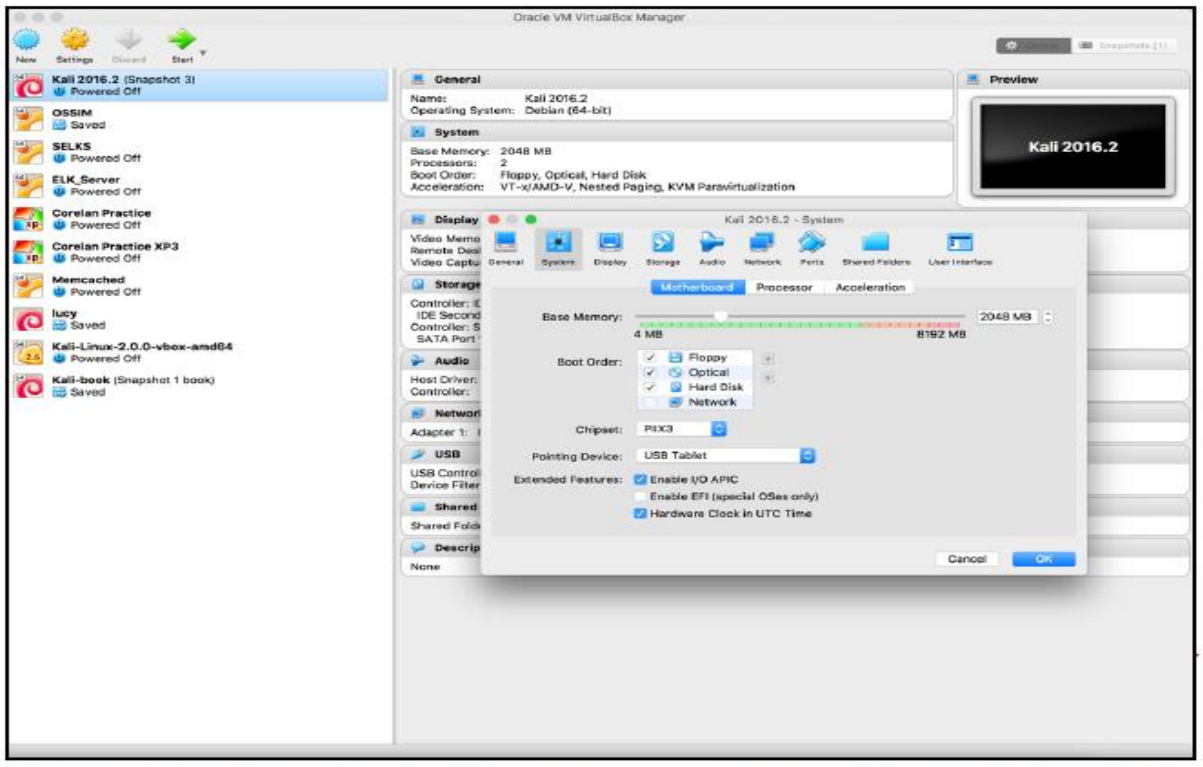
Przygotowania

Aby rozpocząć ten przepis, użyjemy 64-bitowego Kali Linux ISO wymienionego na stronie Offensive Security: https:/ / www. kali. org/ downloads/

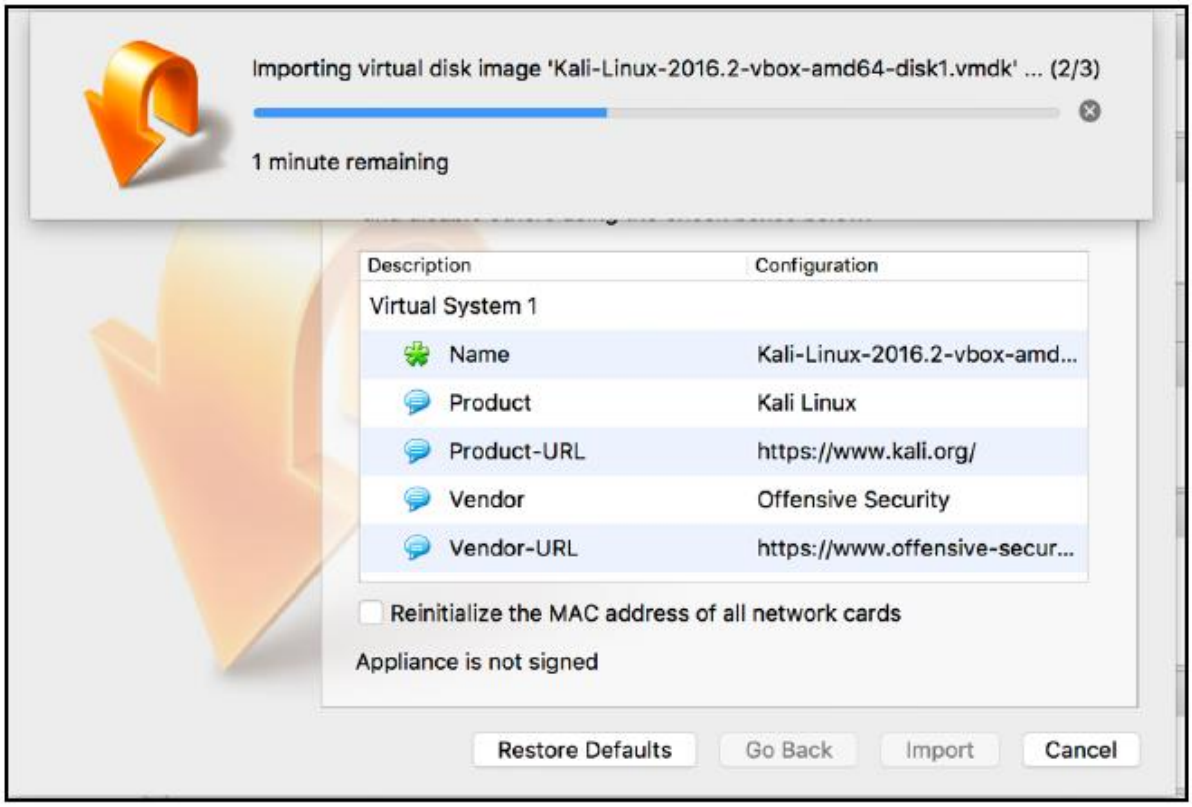
Jak to zrobić...

Możesz skonfigurować Kali za pomocą podanych kroków:

1. Kliknij dwukrotnie na obraz VirtualBox, powinien otworzyć się z VirtualBox:

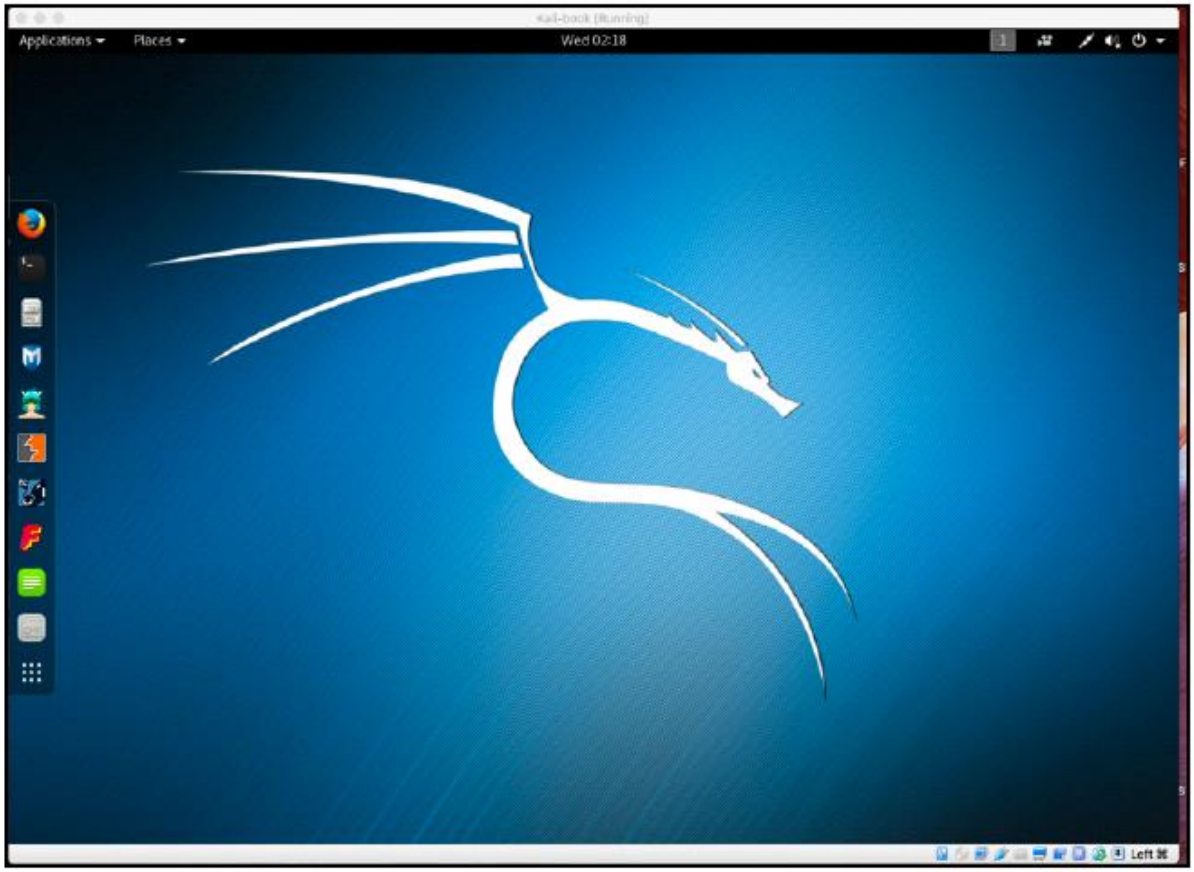


2. Kliknij Importuj:



3. Uruchom maszynę i wprowadź hasło jako toor:

4. Teraz Kali jest uruchomiony i domyślnie skonfigurowany ze środowiskiem graficznym GNOME:



Jak to działa...

Dzięki wstępnie zbudowanemu obrazowi nie musisz martwić się procesem instalacji. Możesz traktować to jako gotowe rozwiązanie. Wystarczy kliknąć Uruchom, a maszyna wirtualna uruchomi system Linux tak jak normalna maszyna.

Konfigurowanie środowiska Xfce

Xfce to darmowe, szybkie i lekkie środowisko graficzne dla platform Unix i podobnych do Unix. Zostało uruchomione przez Oliviera Fourdana w 1996 roku. Nazwa Xfce pierwotnie oznaczała XForms Common Environment, ale od tego czasu Xfce zostało przepisane dwa razy i nie używa już zestawu narzędzi XForms.

Jak to zrobić...

Aby skonfigurować środowisko Xfce, wykonaj następujące kroki:

1. Zaczynamy od użycia następującego polecenia, aby zainstalować Xfce wraz ze wszystkimi wtyczkami i dodatkami:

apt-get install kali-defaults kali-root desktop-base xfce4

xfce4-places-plugin xfce4-goodies

Poniższy zrzut ekranu pokazuje poprzednie polecenie:

2. Wpisz Y, gdy pojawi się prośba o potwierdzenie dodatkowych wymagań dotyczących przestrzeni.

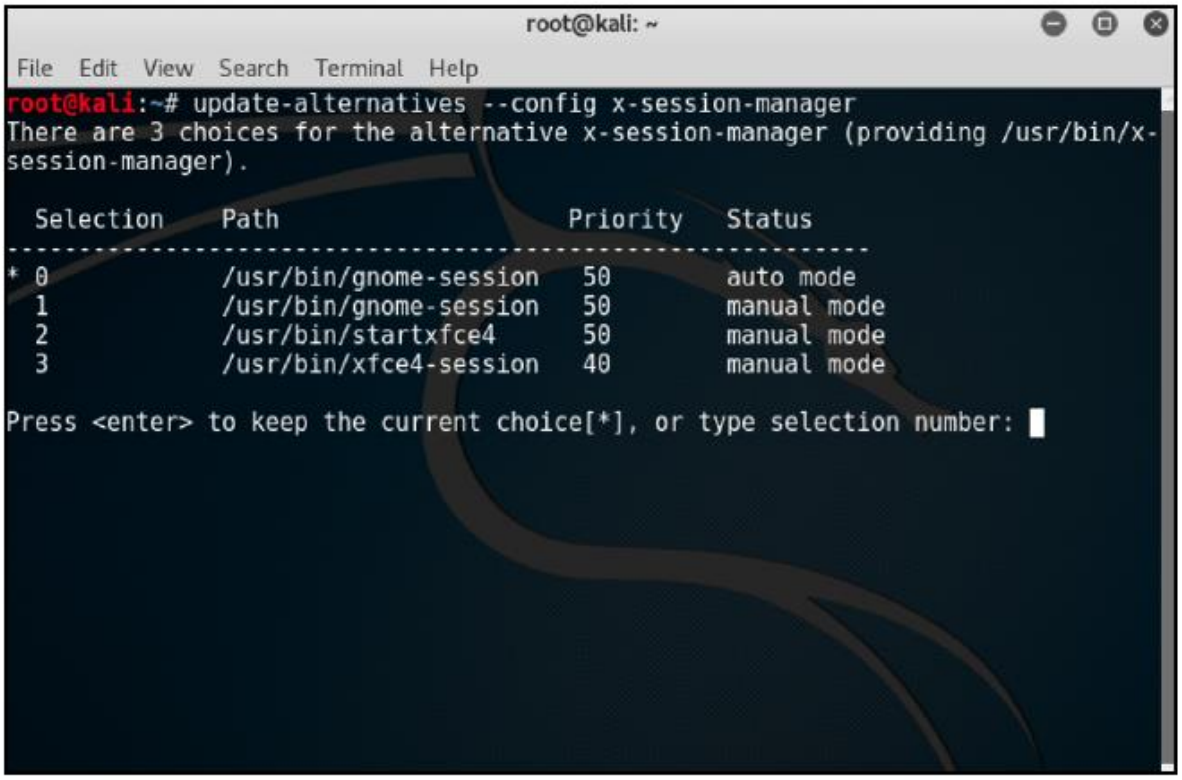
3. Wybierz OK w wyświetlonym oknie dialogowym.

4. Wybieramy lightdm jako domyślnego menedżera pulpitu i naciskamy klawisz Enter.

5. Po zakończeniu instalacji otwieramy okno terminala i wpisujemy następujące polecenie:

update-alternatives --config x-session-manager

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



6. Wybierz opcję xfce4-session (w naszym przypadku 3) i naciśnij klawisz Enter.

7. Wyloguj się i zaloguj ponownie lub uruchom ponownie maszynę, a my zobaczymy środowisko Xfce:

Konfigurowanie środowiska Mate

Środowisko graficzne Mate zostało zbudowane w kontynuacji GNOME 2. Zostało wydane po raz pierwszy w 2011 roku.

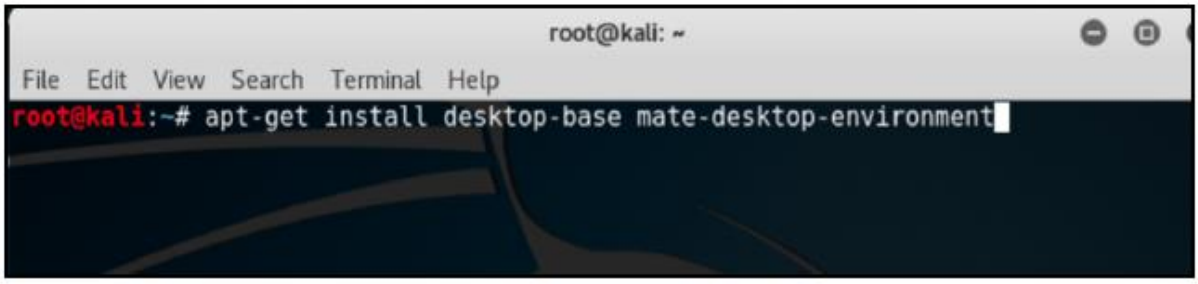
Jak to zrobić...

Aby skonfigurować środowisko Mate, wykonaj następujące kroki:

1. Zaczynamy od użycia następującego polecenia, aby zainstalować środowisko Mate:

apt-get install desktop-base mate-desktop-environment

Poniższy zrzut ekranu pokazuje poprzednie polecenie:

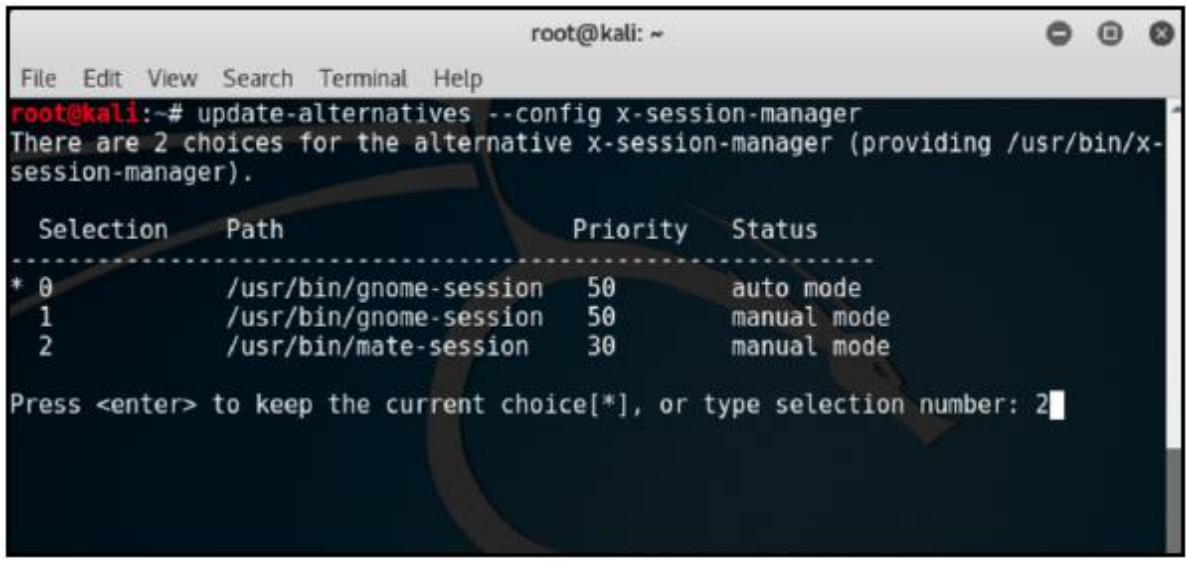


2. Wpisz Y, gdy poprosi o potwierdzenie dodatkowych wymagań dotyczących przestrzeni.

3. Po zakończeniu instalacji użyjemy następującego polecenia, aby ustawić Mate jako nasze domyślne środowisko:

update-alternatives --config x-session-manager

4. Wybierz opcję mate-session (w naszym przypadku 2) i naciśnij klawisz Enter:



5. Wyloguj się i zaloguj ponownie lub uruchom ponownie, a zobaczymy środowisko Mate:

Konfigurowanie środowiska LXDE

LXDE to darmowe środowisko open source napisane w C przy użyciu zestawu narzędzi GTK+ dla systemów Unix i innych platform POSIX. Lightweight X11 Desktop Environment (LXDE) to domyślne środowisko dla wielu systemów operacyjnych, takich jak Knoppix, Raspbian, Lubuntu itd.

Jak to zrobić...

Aby skonfigurować środowisko LXDE, wykonaj następujące kroki:

1. Zaczynamy od użycia następującego polecenia, aby zainstalować LXDE:

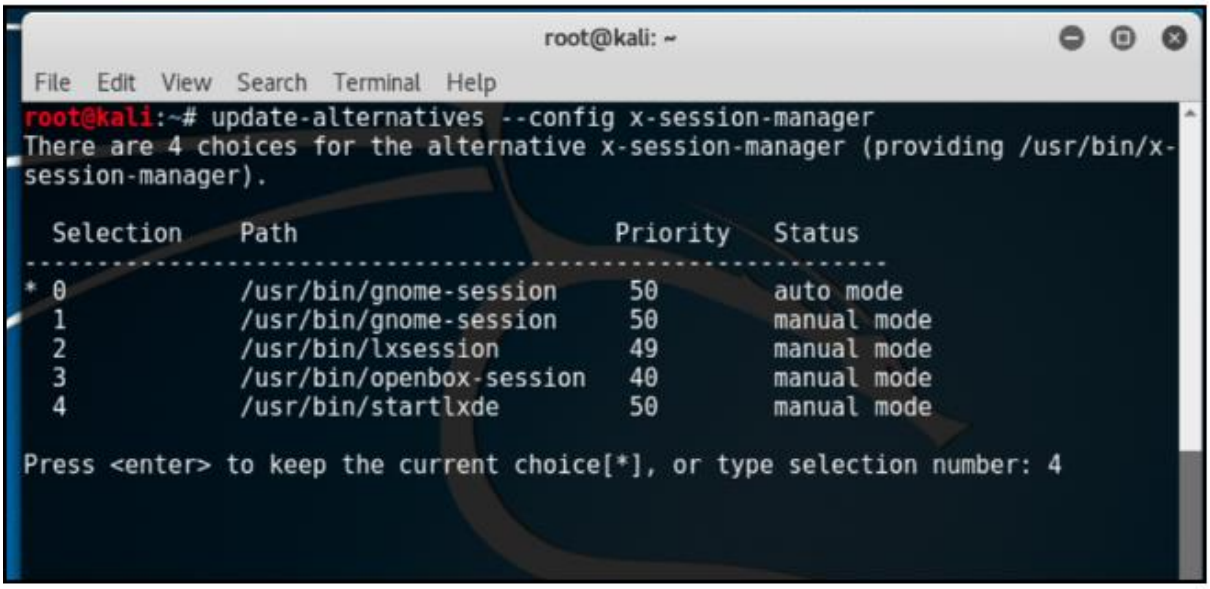
apt-get install lxde-core lxde

2. Wpisz Y, gdy poprosi o potwierdzenie dodatkowych wymagań dotyczących miejsca.

3. Po zakończeniu instalacji otwieramy okno terminala i wpisujemy następujące polecenie:

update-alternatives --config x-session-manager

Poniższy zrzut ekranu pokazuje dane wyjściowe poprzedniego polecenia:



4. Wybierz opcję lxsession (w naszym przypadku 4) i naciśnij Enter.

5. Wyloguj się i zaloguj ponownie, a zobaczymy środowisko LXDE:

Konfigurowanie środowiska e17

Enlightenment, znany również jako E, to menedżer okien dla systemu X Windows. Został wydany po raz pierwszy w 1997 roku. Posiada wiele funkcji, takich jak Engage, wirtualny pulpit, kafelkowanie itd.

Jak to zrobić...

Ze względu na problemy ze zgodnością i zależnościami lepiej jest skonfigurować środowisko Kali na innym komputerze. Ten obraz ISO (Kali 64-bit e17) jest już dostępny na oficjalnej stronie Kali Linux i można go pobrać z następującego adresu URL:

https:/ / www. kali. org/ downloads/ .

Konfigurowanie środowiska KDE

KDE to międzynarodowa społeczność wolnego oprogramowania. Pulpit Plasma jest jednym z najpopularniejszych projektów KDE; jest domyślnym środowiskiem pulpitu dla wielu dystrybucji Linuksa. Został założony w 1996 roku przez Mathiasa Ettricha.

Jak to zrobić...

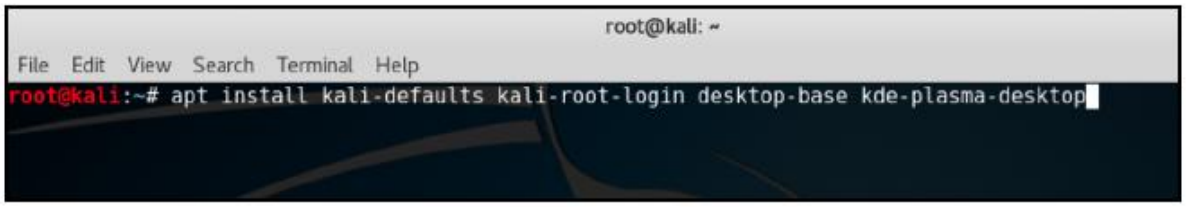
Aby skonfigurować środowisko KDE, wykonaj następujące kroki:

1. Używamy następującego polecenia, aby zainstalować KDE:

apt-get install kali-defaults kali-root-login desktop-base

kde-plasma-desktop

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



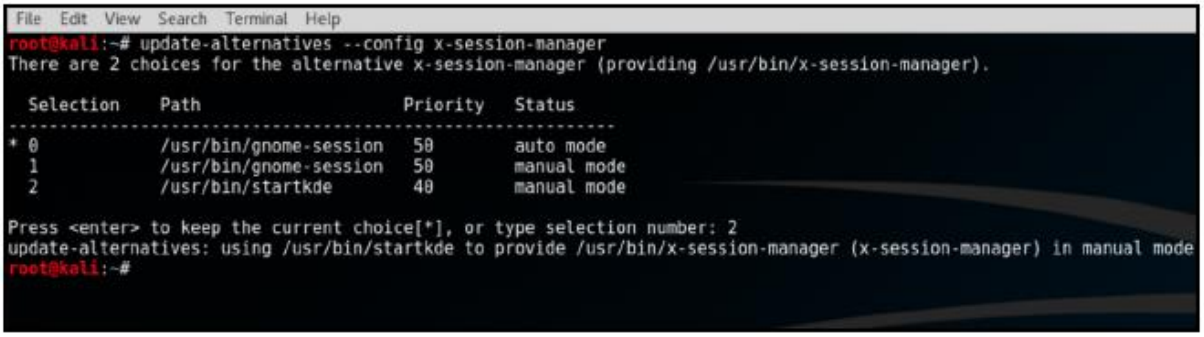
2. Wpisz Y, gdy pojawi się prośba o potwierdzenie dodatkowych wymagań dotyczących miejsca.

3. Kliknij OK w obu oknach, które się pojawią.

4. Po zakończeniu instalacji otwieramy okno terminala i wpisujemy następujące polecenie:

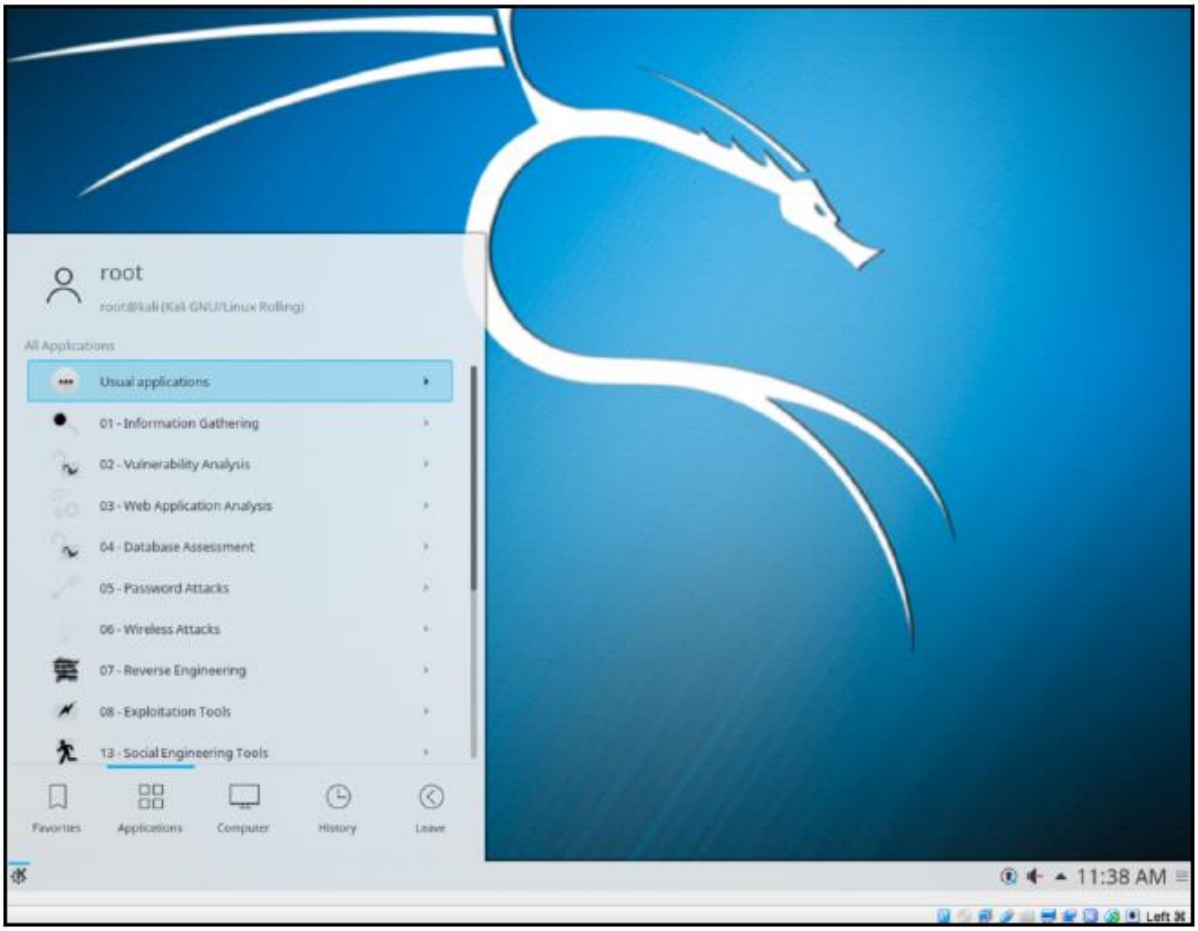
update-alternatives --config x-session-manager

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



5. Wybierz opcję KDE session (w naszym przypadku 2) i naciśnij Enter.

6. Wyloguj się i zaloguj ponownie, a zobaczymy środowisko KDE:



Przygotowanie za pomocą niestandardowych narzędzi

Te narzędzia, które zainstalujesz, są dostępne jako oprogramowanie open source na GitHub. Są znacznie szybsze i zawierają zbiory różnych poprawek, które ludzie dodawali przez pewien czas podczas własnych testów penetracyjnych.

Przygotowanie

Oto lista niektórych narzędzi, których będziesz potrzebować, zanim zagłębimy się w testy penetracyjne. Nie martw się, nauczysz się ich używania na przykładach z życia wziętych w kolejnych rozdziałach. Jeśli jednak nadal chcesz nauczyć się podstaw na wczesnym etapie, możesz to zrobić za pomocą prostych poleceń:

toolname -help

toolname -h

Jak to zrobić...

Niektóre narzędzia są wymienione w poniższych sekcjach.

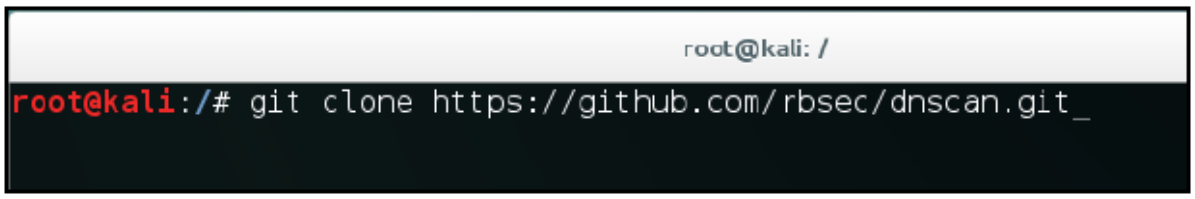
Dnscan

Dnscan to narzędzie Pythona, które używa listy słów do rozwiązywania prawidłowych subdomen. Aby dowiedzieć się więcej o Dnscan, wykonaj następujące kroki:

1. Użyjemy prostego polecenia, aby sklonować repozytorium git:

git clone https://github.com/rbsec/dnscan.git

Poniższy zrzut ekranu pokazuje poprzednie polecenie:



2. Możesz również pobrać i zapisać go z https:/ / github. com/ rbsec/ dnscan.

3. Następnie przeglądamy katalog, do którego pobraliśmy Dnscan.

4. Uruchom Dnscan, używając następującego polecenia:

./dnscan.py -h

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

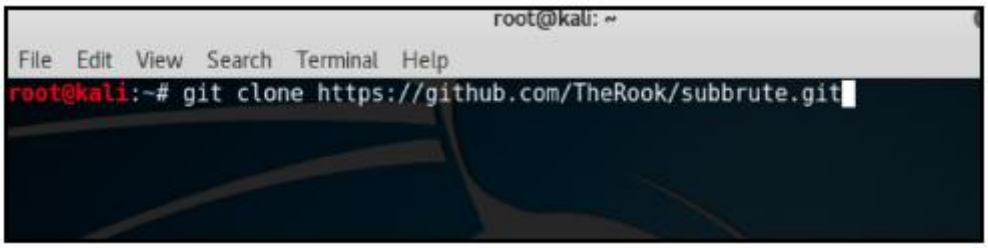
Subbrute

Następnie zainstalujemy subbrute. Jest on niesamowicie szybki i zapewnia dodatkową warstwę anonimowości, ponieważ używa publicznych resolverów do brutalnego ataku na subdomeny:

1. Polecenie tutaj jest znowu proste:

git clone https://github.com/TheRook/subbrute.git

Poniższy zrzut ekranu pokazuje poprzednie polecenie:



2. Możesz też pobrać i zapisać go z https:/ / github. com/TheRook/ subbrute.

3. Po zakończeniu instalacji będziemy potrzebować listy słów, aby ją uruchomić, dla której możemy pobrać listę dnspop. Ta lista może być również użyta w poprzednim przepisie: https:/ / github. com/ bitquark/ dnspop/tree/ master/ results.

4. Po skonfigurowaniu obu przeglądamy katalog subbrute i uruchamiamy go za pomocą następującego polecenia:

./subbrute.py

5. Aby uruchomić go w domenie z naszą listą słów, używamy następującego polecenia:

./subbrute.py -s /path/to/wordlist hostname.com

Dirsearch

Naszym kolejnym narzędziem w wierszu jest dirsearch. Jak sama nazwa wskazuje, jest to proste narzędzie wiersza poleceń, którego można użyć do przeprowadzenia ataku siłowego na katalogi. Jest znacznie szybszy niż tradycyjny DIRB:

1. Polecenie instalacji to:

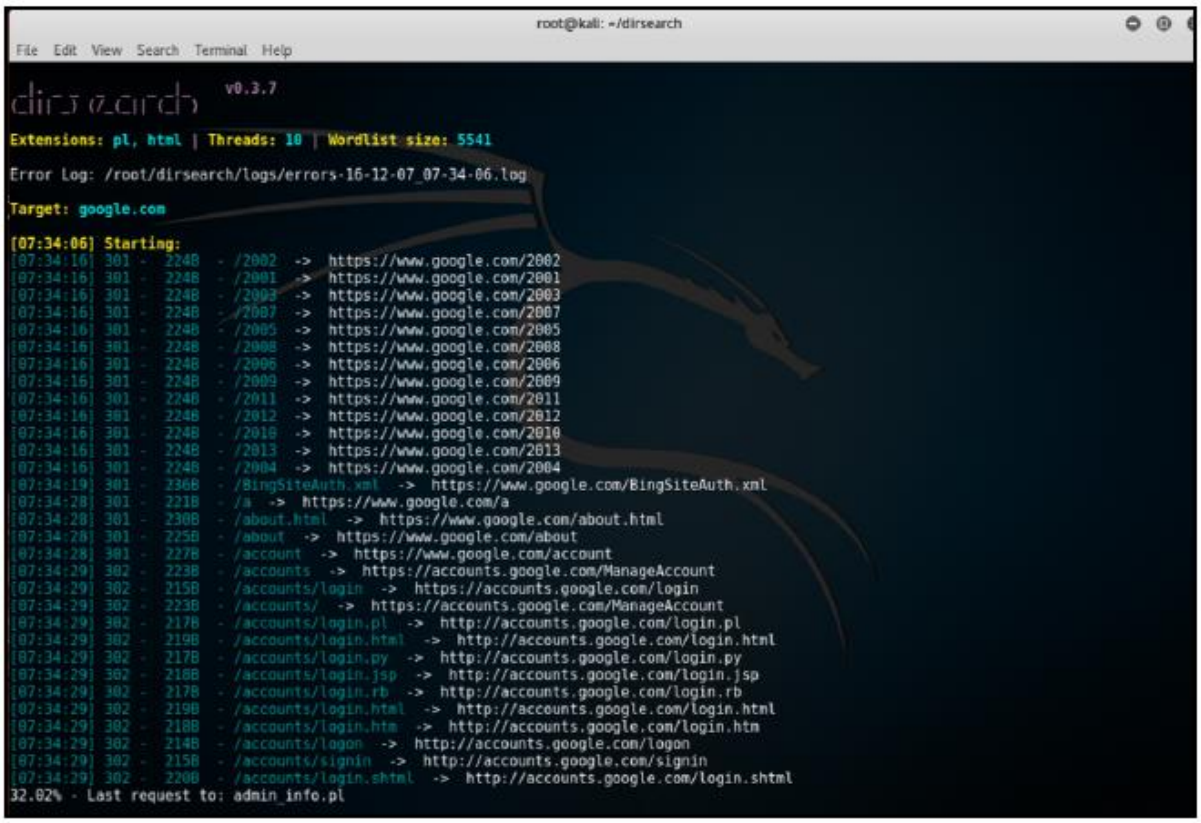
git clone https://github.com/maurosoria/dirsearch.git

2. Możesz też pobrać i zapisać go z https:/ / github. com/maurosoria/dirsearch. Poniższy zrzut ekranu pokazuje poprzednie polecenie:

3. Po zakończeniu klonowania przejdź do katalogu i uruchom narzędzie, używając następującego polecenia:

./dirsearch.py -u hostname.com -e aspx,php

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



Pentesting VPN ike-scan

Podczas pentestu często możemy napotkać punkty końcowe VPN. Jednak znajdowanie luk w tych punktach końcowych i wykorzystywanie ich nie jest dobrze znaną metodą. Punkty końcowe VPN używają protokołu Internet Key Exchange (IKE) do skonfigurowania skojarzenia zabezpieczeń między wieloma klientami w celu ustanowienia tunelu VPN. IKE ma dwie fazy, faza 1 odpowiada za skonfigurowanie i ustanowienie bezpiecznego uwierzytelnionego kanału komunikacyjnego, a faza 2 szyfruje i transportuje dane. Naszym celem tutaj będzie faza 1; wykorzystuje ona dwie metody wymiany kluczy:

Tryb główny

Tryb agresywny

Będziemy polować na punkty końcowe VPN z włączonym trybem agresywnym, używając uwierzytelniania PSK.

Przygotowania

W tym przepisie użyjemy narzędzi ike-scan i ikeprobe. Najpierw instalujemy ike-scan, klonując repozytorium git:

git clone https://github.com/royhills/ike-scan.git

Możesz też użyć następującego adresu URL, aby pobrać go z https:/ / github.com/ royhills/ike- scan.

Jak to zrobić...

Aby skonfigurować ike-scan, wykonaj następujące kroki:

1. Przejdź do katalogu, w którym zainstalowano ike-scan.

2. Zainstaluj autoconf, uruchamiając następujące polecenie:

apt-get install autoconf

3. Uruchom autoreconf --install, aby wygenerować plik .configure.

4. Uruchom ./configure.

5. Uruchom make, aby skompilować projekt.

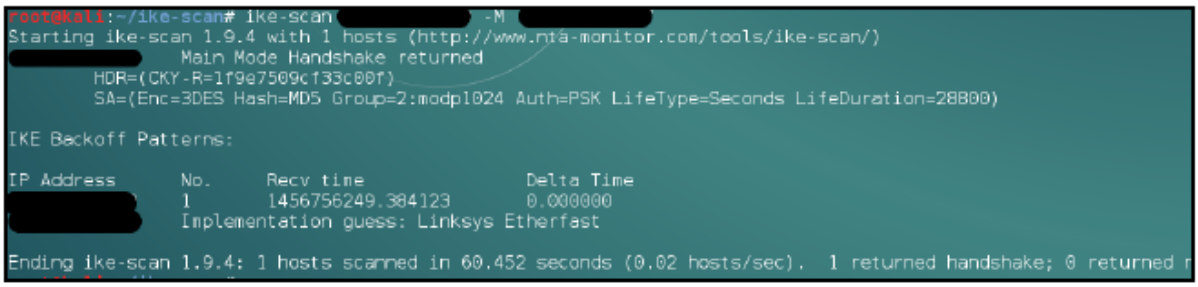
6. Uruchom make check, aby zweryfikować etap kompilacji.

7. Uruchom make install, aby zainstalować ike-scan.

8. Aby przeskanować hosta pod kątem agresywnego trybu uzgadniania, użyj następujących poleceń:

ike-scan x.x.x.x -M -A

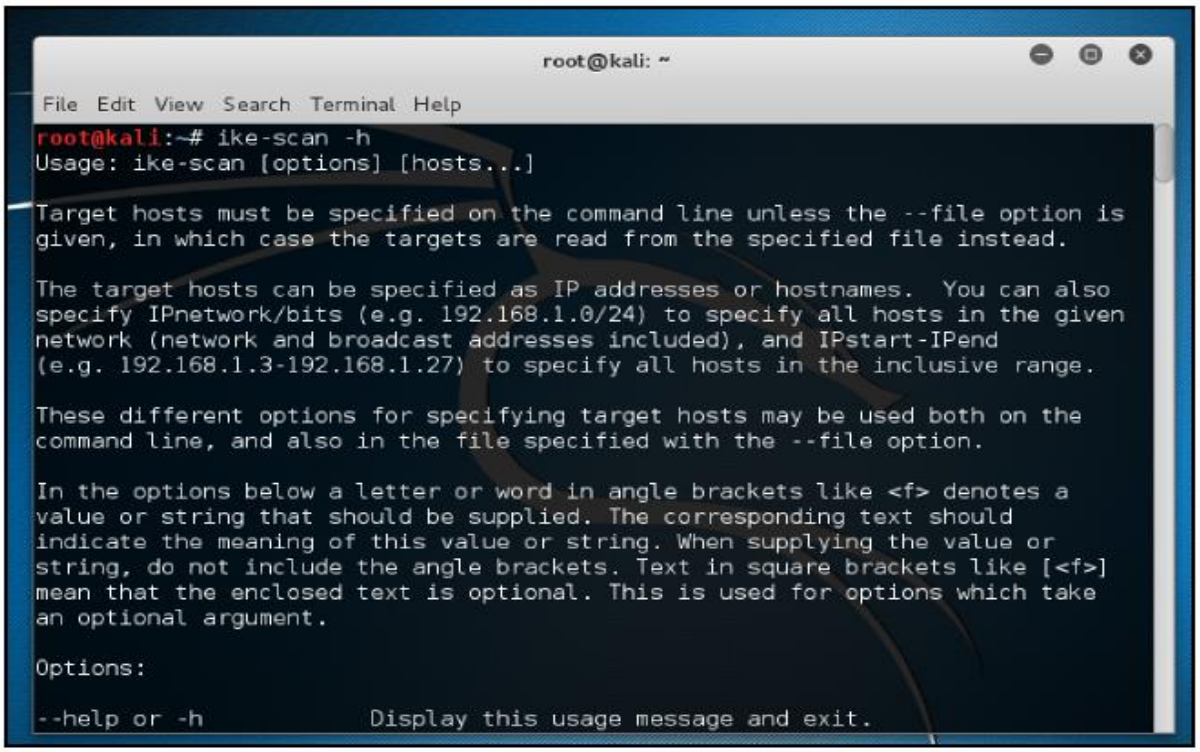
Poniższy zrzut ekranu pokazuje dane wyjściowe poprzedniego polecenia:



9. Czasami zobaczymy odpowiedź po podaniu prawidłowej nazwy grupy, takiej jak (vpn):

ike-scan x.x.x.x -M -A id=vpn

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:



Łamanie PSK

Aby dowiedzieć się, jak złamać PSK, wykonaj następujące kroki:

1. Dodaj flagę -P w poleceniu ike-scan, aby wyświetlić odpowiedź z przechwyconym hashem.

2. Aby zapisać hash, podajemy nazwę pliku wraz z flagą -P.

3. Następnie możemy użyć psk-crack z następującym poleceniem:

psk-crack -b 5 /path/to/pskkey

4. Gdzie -b to tryb siłowy, a długość to 5.

5. Aby użyć ataku opartego na słowniku, używamy następującego polecenia:

psk-crack -d /path/to/dictionary /path/to/pskkey

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
Starting psk-crack [ike-scan 1.9] (http://www.nta-monitor.com/tools/ike-scan/)
Running in dictionary cracking mode
key "123456" matches SHA1 hash d46e5c224092fedda5a1733aa71e515d0dfbb97e
Ending psk-crack: 1 iterations in 0.014 seconds (72.87 iterations/sec)
```

Jak to działa...

W trybie agresywnym hash uwierzytelniania jest przesyłany jako odpowiedź na pakiet klienta VPN, który próbuje nawiązać połączenie Tunnel (IPSEC). Ten hash nie jest szyfrowany, co pozwala nam na przechwycenie hasha i przeprowadzenie ataku siłowego na niego w celu odzyskania naszego PSK. Nie jest to możliwe w trybie głównym, ponieważ używa on zaszyfrowanego hasha wraz z sześcioetapowym uzgadnianiem, podczas gdy tryb agresywny używa tylko trzyetapowego.

Konfigurowanie proxychains

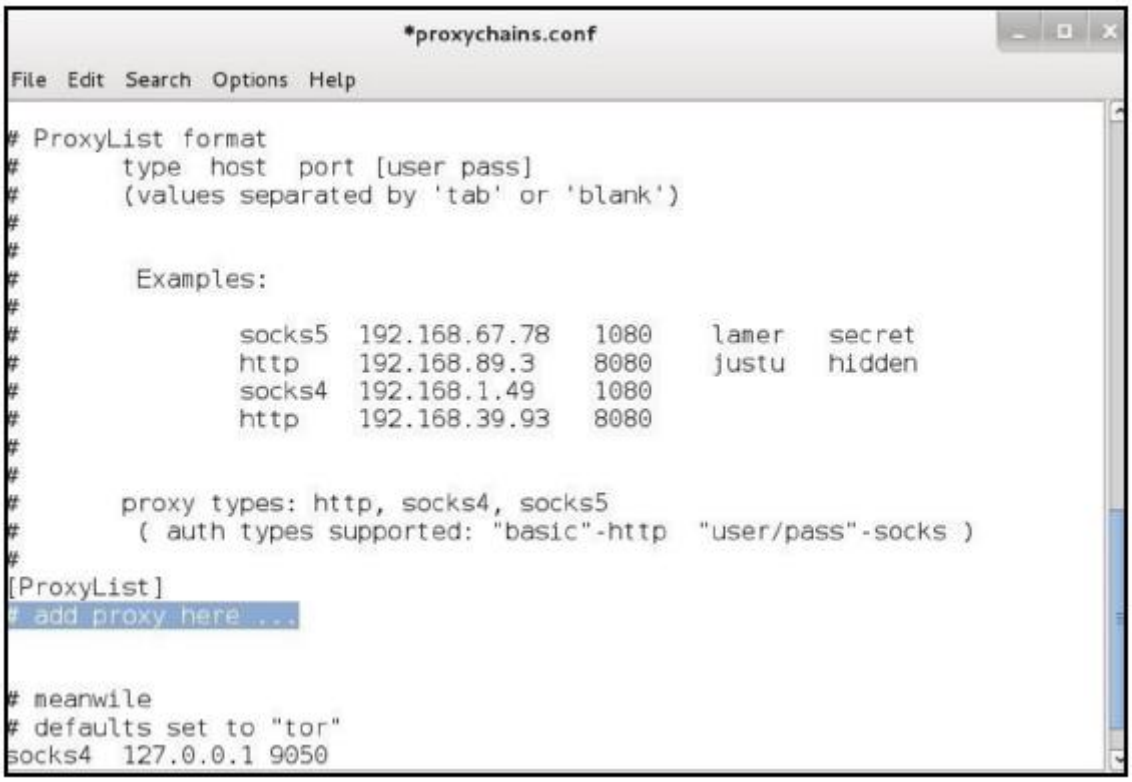
Czasami musimy pozostać niemożliwi do wyśledzenia podczas wykonywania czynności pentestu. Proxychains pomaga nam, umożliwiając korzystanie z systemu pośredniczącego, którego adres IP można pozostawić w logach systemu bez obawy, że zostanie on do nas wyśledzony. Proxychains to narzędzie, które pozwala dowolnej aplikacji śledzić połączenie za pośrednictwem serwera proxy, takiego jak SOCKS5, Tor itd.Jak to zrobić...

Proxychains jest już zainstalowany w Kali. Potrzebujemy jednak listy serwerów proxy w pliku konfiguracyjnym, których chcemy użyć:

1. Aby to zrobić, otwieramy plik konfiguracyjny proxychains w edytorze tekstu za pomocą tego polecenia:

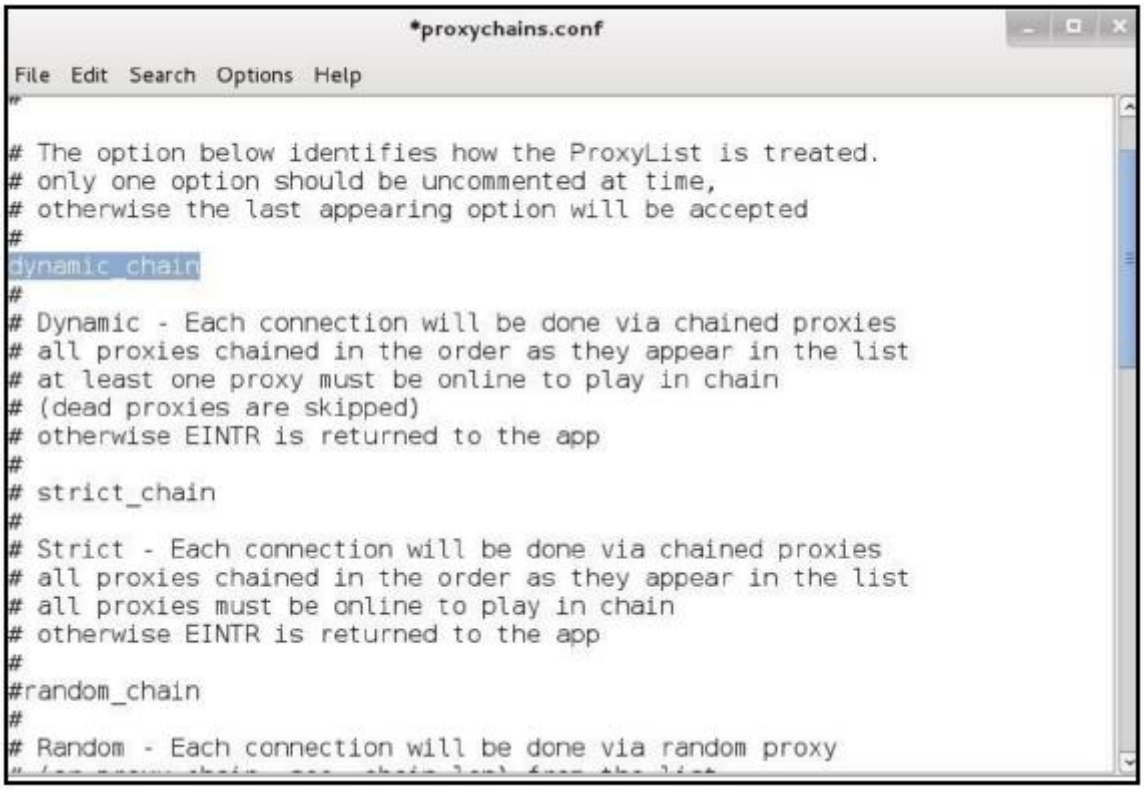
leafpad /etc/proxychains.conf

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



Możemy dodać wszystkie proxy, które chcemy w poprzednim wyróżnionym obszarze, a następnie zapisać. Proxychains pozwala nam również używać dynamicznego łańcucha lub losowego łańcucha podczas łączenia się z serwerami proxy.

2. W pliku konfiguracyjnym usuń komentarz z dynamic_chain lub random_chain:



Używanie proxychains z torem

Aby dowiedzieć się więcej o torze, wykonaj następujące kroki:

1. Aby użyć proxychains z torem, najpierw musimy zainstalować tor za pomocą następującego polecenia:

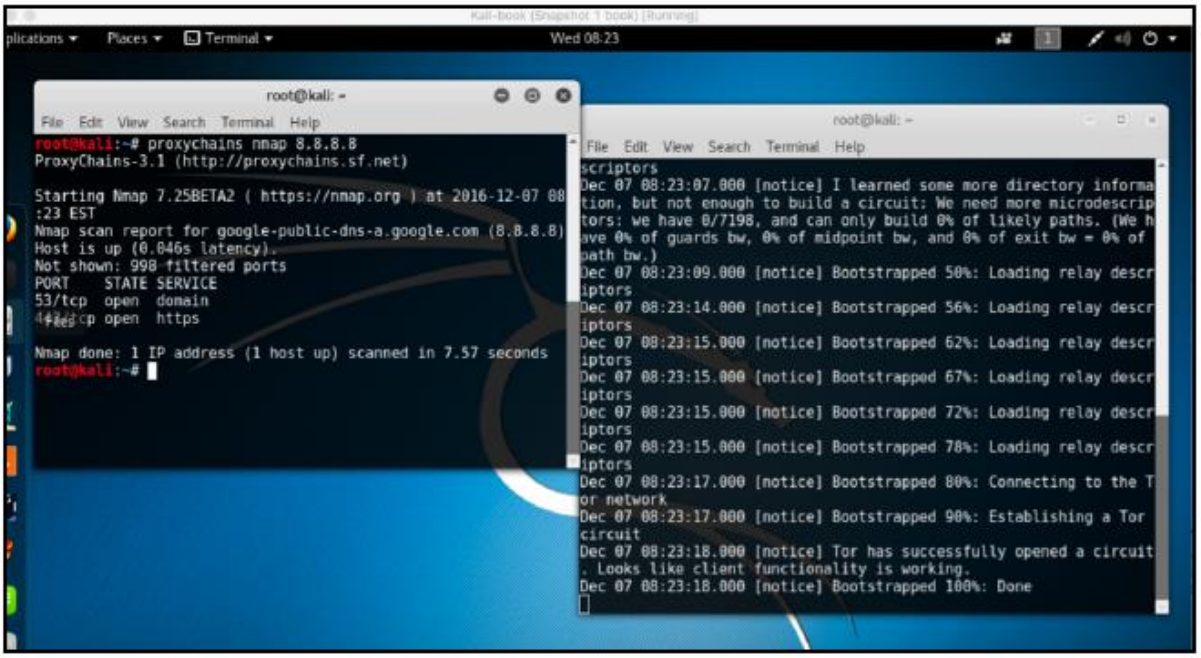
apt-get install tor

2. Po zainstalowaniu uruchamiamy tor, wpisując tor w terminalu.

3. Następnie otwieramy kolejny terminal i wpisujemy następujące polecenie, aby użyć aplikacji za pośrednictwem proxychains:

proxychains toolname -arguments

Poniższy zrzut ekranu pokazuje przykład poprzednich poleceń:



Wyrusz na polowanie z Routerhunter

Routerhunter to narzędzie służące do wyszukiwania podatnych routerów w sieci i przeprowadzania na nie różnych ataków w celu wykorzystania luki DNSChanger. Ta luka umożliwia atakującemu zmianę serwera DNS routera, kierując w ten sposób cały ruch do pożądanych witryn.

Przygotowania

W tym przepisie będziesz musiał ponownie sklonować repozytorium git. Użyjemy następującego polecenia:

git clone https://github.com/jh00nbr/RouterHunterBR.git

Jak to zrobić...

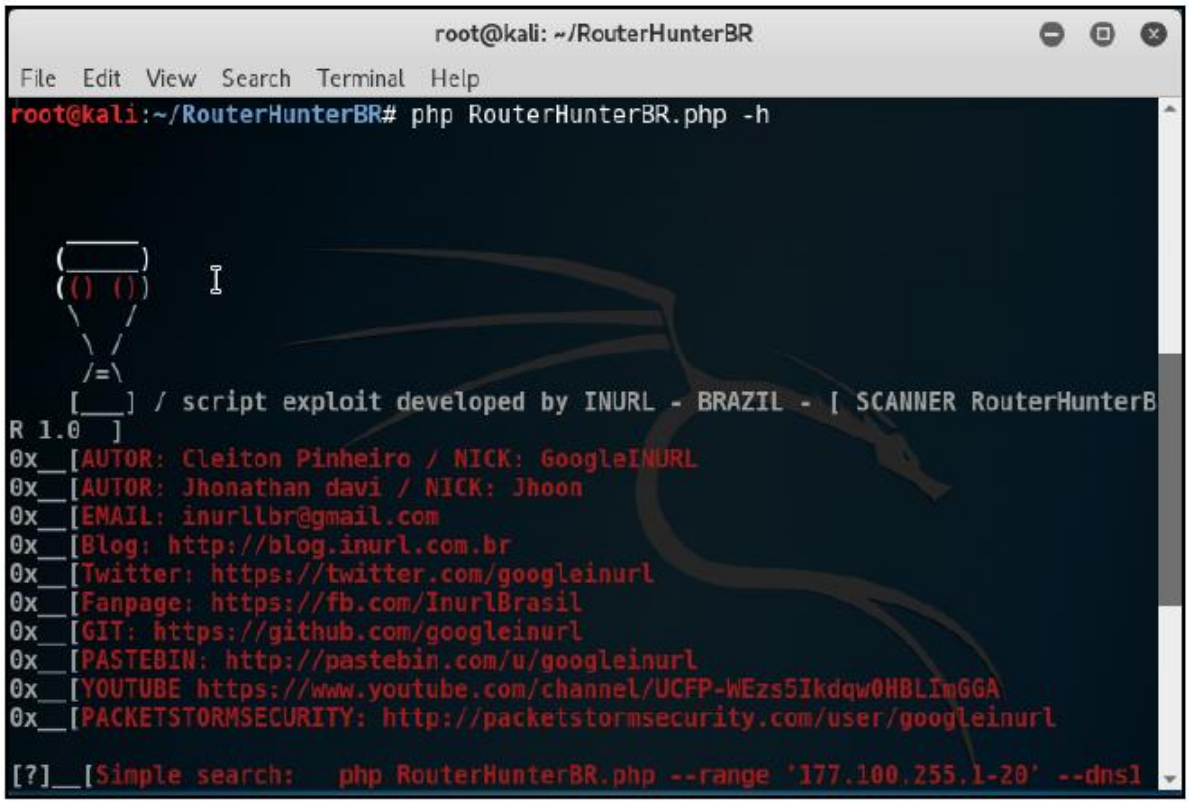
Aby uruchomić RouterHunterBR.php, wykonaj następujące kroki:

1. Po sklonowaniu pliku wejdź do katalogu.

2. Uruchom następujące polecenie:

php RouterHunterBR.php -h

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



3. Możemy dostarczyć Routerhunterowi zakres adresów IP, adresy IP serwerów DNS itd.