

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.

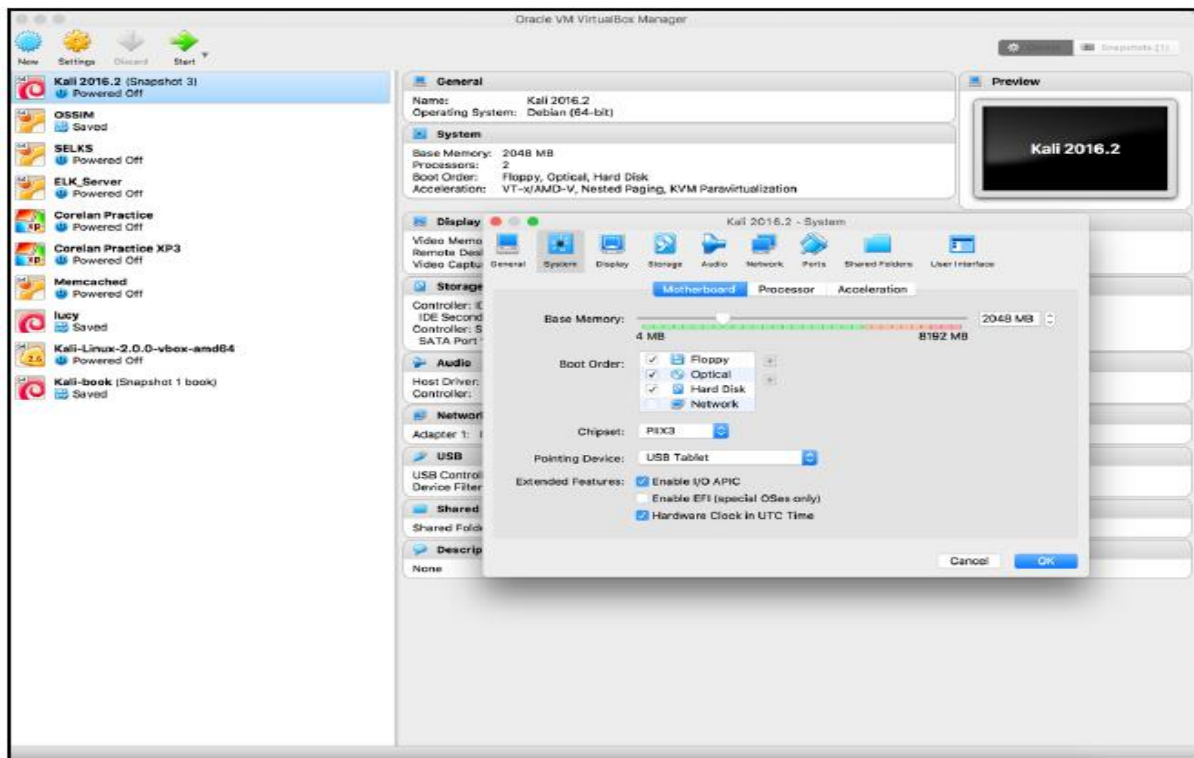
Przygotowania

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

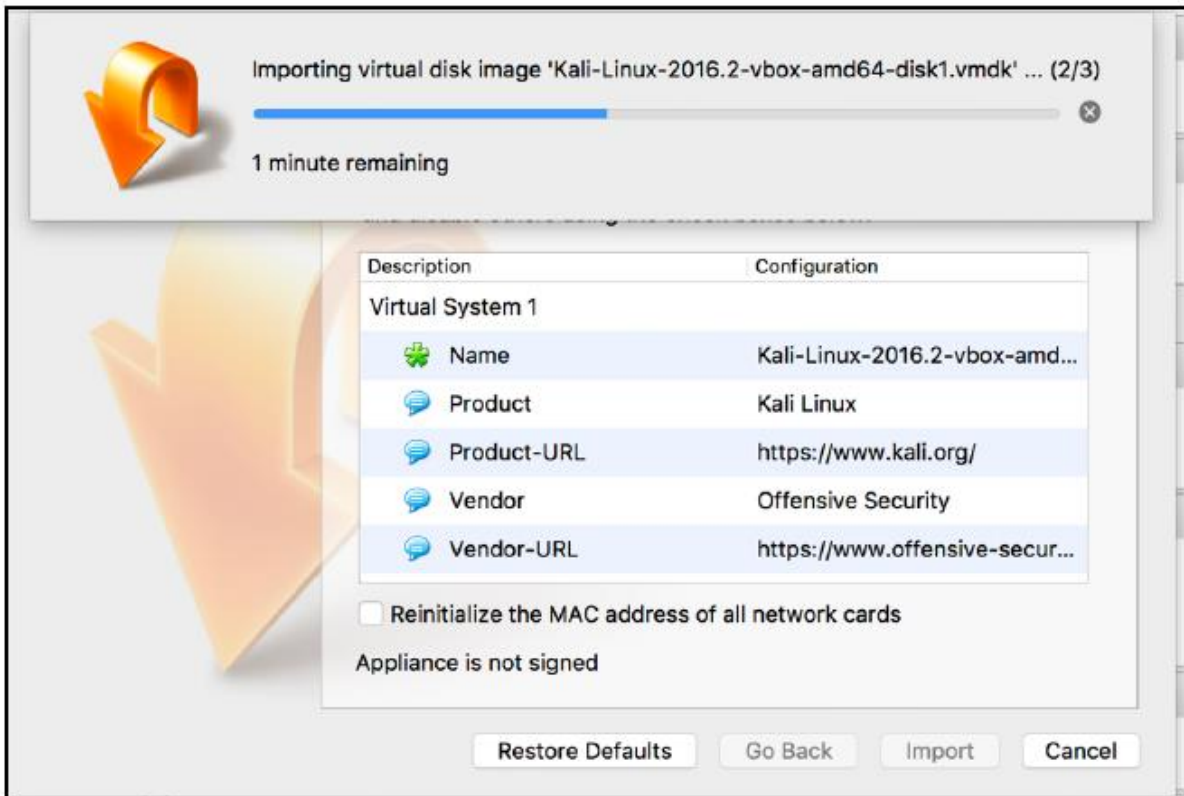
Jak to zrobić...

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...

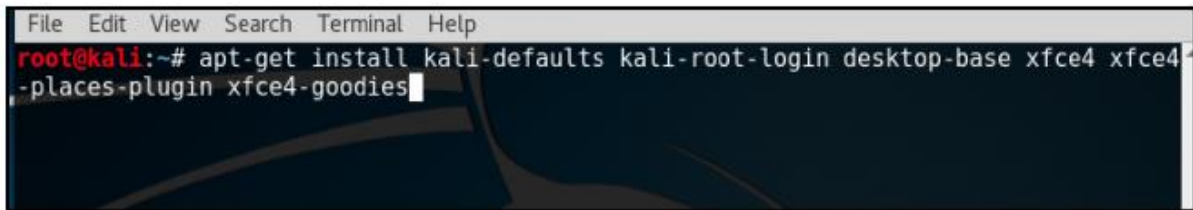
Aby skonfigurować środowisko Xfce, wykonaj następujące kroki:

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:



```
File Edit View Search Terminal Help
root@kali:~# apt-get install kali-defaults kali-root-login desktop-base xfce4 xfce4-places-plugin xfce4-goodies
```

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:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# update-alternatives --config x-session-manager  
There are 3 choices for the alternative x-session-manager (providing /usr/bin/x-  
session-manager).  


| Selection | Path                   | Priority | Status      |
|-----------|------------------------|----------|-------------|
| * 0       | /usr/bin/gnome-session | 50       | auto mode   |
| 1         | /usr/bin/gnome-session | 50       | manual mode |
| 2         | /usr/bin/startxfce4    | 50       | manual mode |
| 3         | /usr/bin/xfce4-session | 40       | manual mode |

  
Press <enter> to keep the current choice[*], or type selection number: █
```

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.

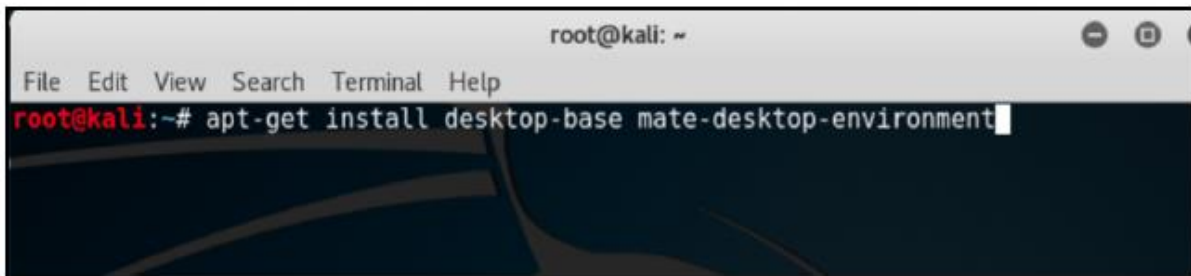
Jak to zrobić...

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:



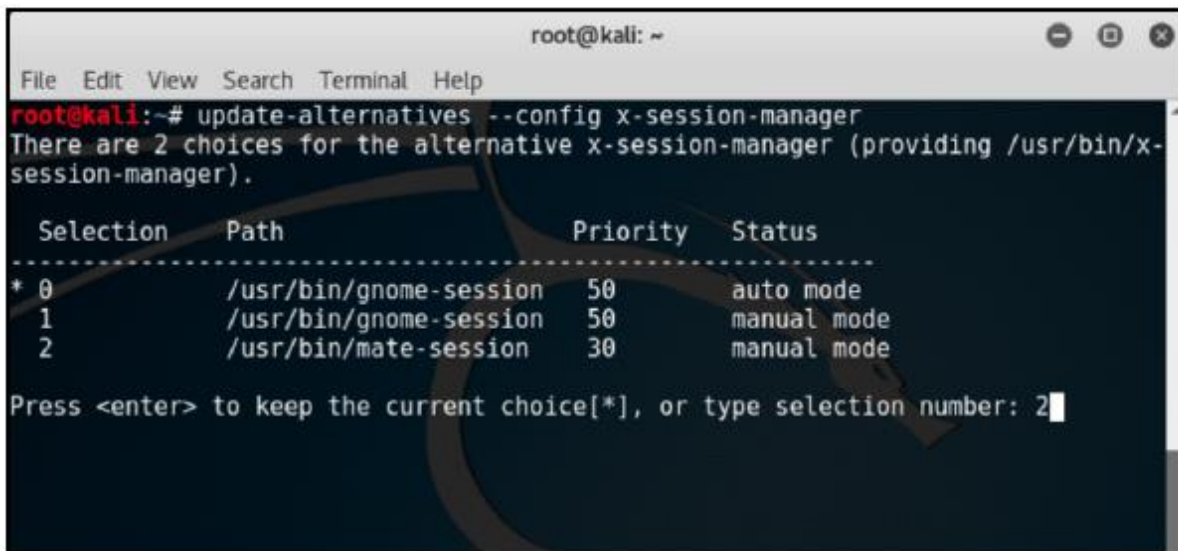
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# apt-get install desktop-base mate-desktop-environment
```

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:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# update-alternatives --config x-session-manager  
There are 2 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).  


| Selection | Path                   | Priority | Status      |
|-----------|------------------------|----------|-------------|
| * 0       | /usr/bin/gnome-session | 50       | auto mode   |
| 1         | /usr/bin/gnome-session | 50       | manual mode |
| 2         | /usr/bin/mate-session  | 30       | manual mode |

  
Press <enter> to keep the current choice[*], or type selection number: 2
```

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, lub Ubuntu 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:

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# update-alternatives --config x-session-manager  
There are 4 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).  


| Selection | Path                     | Priority | Status      |
|-----------|--------------------------|----------|-------------|
| * 0       | /usr/bin/gnome-session   | 50       | auto mode   |
| 1         | /usr/bin/gnome-session   | 50       | manual mode |
| 2         | /usr/bin/lxsession       | 49       | manual mode |
| 3         | /usr/bin/openbox-session | 40       | manual mode |
| 4         | /usr/bin/startlxde       | 50       | manual mode |

  
Press <enter> to keep the current choice[*], or type selection number: 4
```

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...

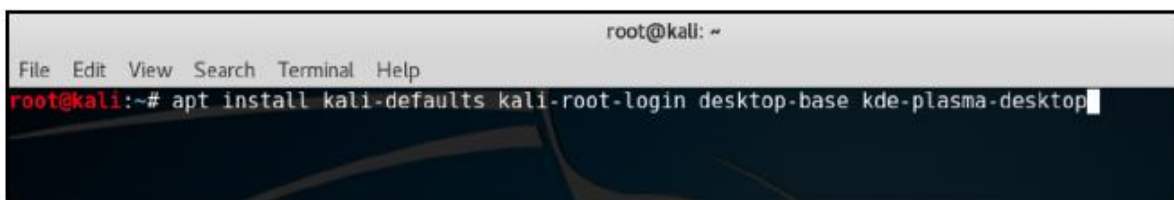
Aby skonfigurować środowisko KDE, wykonaj następujące kroki:

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:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# apt install kali-defaults kali-root-login desktop-base kde-plasma-desktop
```

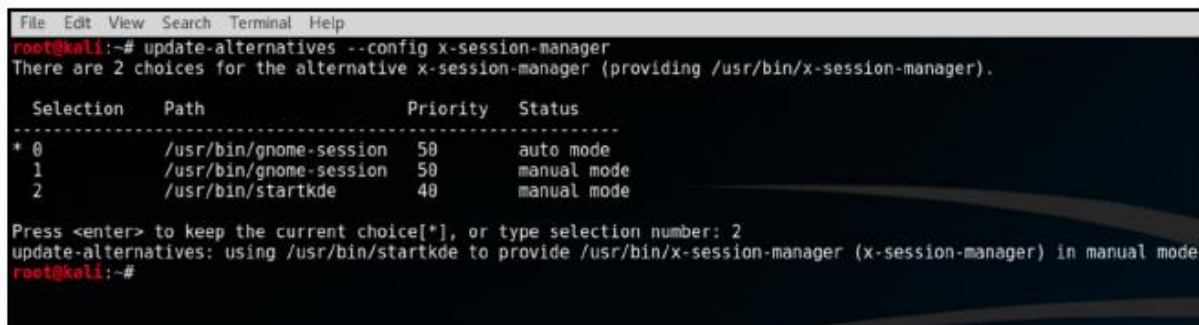
2. Wpisz Y, gdy pojawi się prośba o potwierdzenie dodatkowych wymagań dotyczących miejsca.

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:



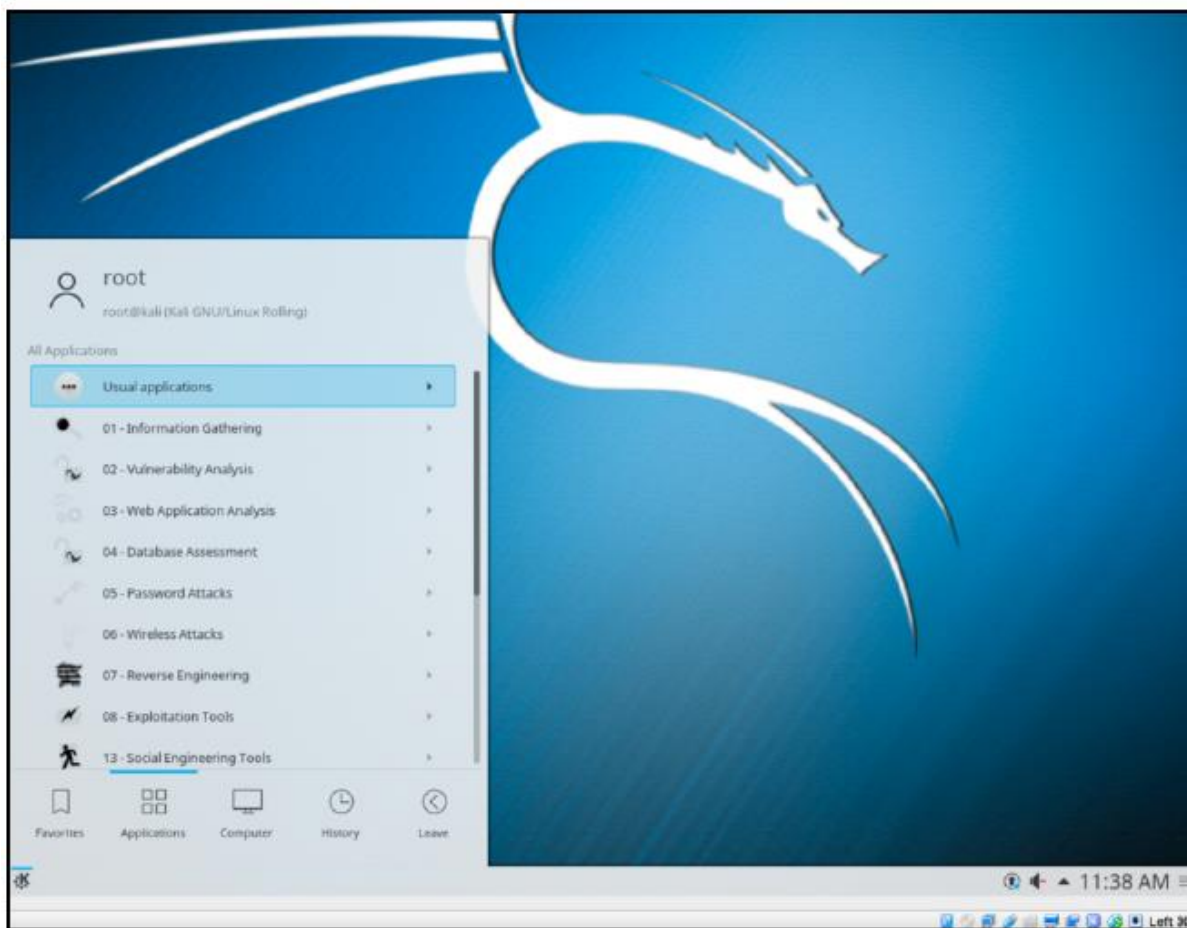
```
File Edit View Search Terminal Help  
root@kali:~# update-alternatives --config x-session-manager  
There are 2 choices for the alternative x-session-manager (providing /usr/bin/x-session-manager).  


| Selection | Path                   | Priority | Status      |
|-----------|------------------------|----------|-------------|
| * 0       | /usr/bin/gnome-session | 50       | auto mode   |
| 1         | /usr/bin/gnome-session | 50       | manual mode |
| 2         | /usr/bin/startkde      | 40       | manual mode |

  
Press <enter> to keep the current choice[*], or type selection number: 2  
update-alternatives: using /usr/bin/startkde to provide /usr/bin/x-session-manager (x-session-manager) in manual mode  
root@kali:~#
```

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:

```
root@kali: /
root@kali:/# git clone https://github.com/rbsec/dnscan.git_
```

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:

```
root@kali:/# cd dnscan/
root@kali:/dnscan# ./dnscan.py -h
usage: dnscan.py [-h] -d DOMAIN [-w WORDLIST] [-t THREADS] [-6] [-z] [-r] [-T]
                [-o OUTPUT_FILENAME] [-D] [-v]

optional arguments:
  -h, --help                show this help message and exit
  -d DOMAIN, --domain DOMAIN Target domain
  -w WORDLIST, --wordlist WORDLIST Wordlist
  -t THREADS, --threads THREADS Number of threads
  -6, --ipv6                Scan for AAAA records
  -z, --zonetransfer        Only perform zone transfers
  -r, --recursive          Recursively scan subdomains
  -T, --tld                 Scan for TLDs
  -o OUTPUT_FILENAME, --output OUTPUT_FILENAME Write output to a file
  -D, --domain-first        Output domain first, rather than IP address
  -v, --verbose            Verbose mode
root@kali:/dnscan# _
```

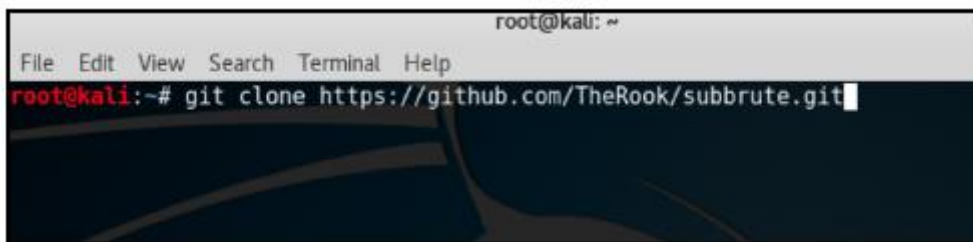
Subbrute

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:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# git clone https://github.com/TheRook/subbrute.git
```

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
```

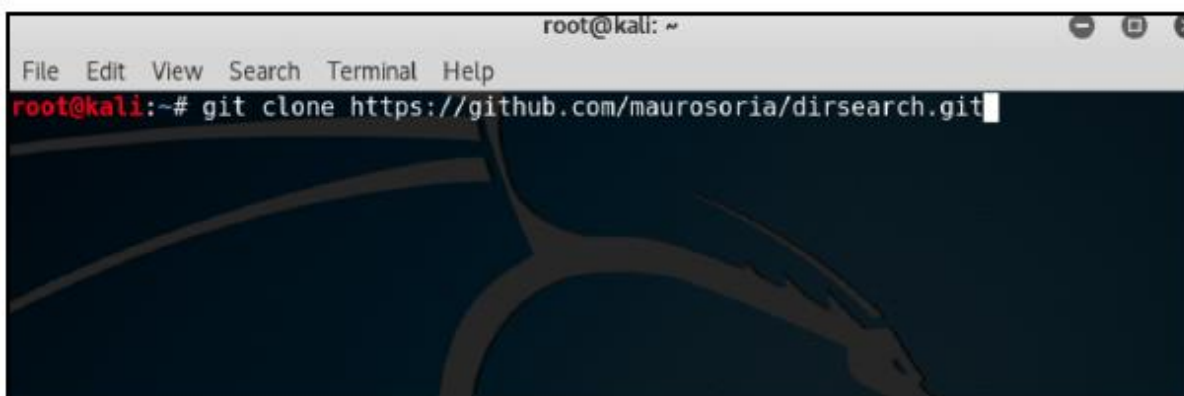
Dirsearch

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:



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# git clone https://github.com/maurosoria/dirsearch.git
```

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:

```
root@kali: ~/dirsearch
File Edit View Search Terminal Help
dirsearch v0.3.7
Extensions: pl, html | Threads: 10 | Wordlist size: 5541
Error Log: /root/dirsearch/logs/errors-16-12-07_07-34-06.log
Target: google.com

[07:34:06] Starting:
[07:34:16] 301 - 2248 - /2002 -> https://www.google.com/2002
[07:34:16] 301 - 2248 - /2001 -> https://www.google.com/2001
[07:34:16] 301 - 2248 - /2003 -> https://www.google.com/2003
[07:34:16] 301 - 2248 - /2007 -> https://www.google.com/2007
[07:34:16] 301 - 2248 - /2005 -> https://www.google.com/2005
[07:34:16] 301 - 2248 - /2008 -> https://www.google.com/2008
[07:34:16] 301 - 2248 - /2006 -> https://www.google.com/2006
[07:34:16] 301 - 2248 - /2009 -> https://www.google.com/2009
[07:34:16] 301 - 2248 - /2011 -> https://www.google.com/2011
[07:34:16] 301 - 2248 - /2012 -> https://www.google.com/2012
[07:34:16] 301 - 2248 - /2010 -> https://www.google.com/2010
[07:34:16] 301 - 2248 - /2013 -> https://www.google.com/2013
[07:34:16] 301 - 2248 - /2004 -> https://www.google.com/2004
[07:34:19] 301 - 2368 - /BingSiteAuth.xml -> https://www.google.com/BingSiteAuth.xml
[07:34:28] 301 - 2218 - /a -> https://www.google.com/a
[07:34:28] 301 - 2308 - /about.html -> https://www.google.com/about.html
[07:34:28] 301 - 2258 - /about -> https://www.google.com/about
[07:34:28] 301 - 2278 - /account -> https://www.google.com/account
[07:34:29] 302 - 2238 - /accounts -> https://accounts.google.com/ManageAccount
[07:34:29] 302 - 2158 - /accounts/login -> https://accounts.google.com/login
[07:34:29] 302 - 2238 - /accounts/ -> https://accounts.google.com/ManageAccount
[07:34:29] 302 - 2178 - /accounts/login.pl -> http://accounts.google.com/login.pl
[07:34:29] 302 - 2198 - /accounts/login.html -> http://accounts.google.com/login.html
[07:34:29] 302 - 2178 - /accounts/login.py -> http://accounts.google.com/login.py
[07:34:29] 302 - 2188 - /accounts/login.jsp -> http://accounts.google.com/login.jsp
[07:34:29] 302 - 2178 - /accounts/login.rb -> http://accounts.google.com/login.rb
[07:34:29] 302 - 2198 - /accounts/login.html -> http://accounts.google.com/login.html
[07:34:29] 302 - 2188 - /accounts/login.htm -> http://accounts.google.com/login.htm
[07:34:29] 302 - 2148 - /accounts/lagon -> http://accounts.google.com/lagon
[07:34:29] 302 - 2158 - /accounts/signin -> http://accounts.google.com/signin
[07:34:29] 302 - 2208 - /accounts/login.shtml -> http://accounts.google.com/login.shtml
32.02% - Last request to: admin info.pl
```

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:

```
root@kali:~/ike-scan# ike-scan [redacted] -M [redacted]
Starting ike-scan 1.9.4 with 1 hosts (http://www.ntia-monitor.com/tools/ike-scan/)
[redacted] Main Mode Handshake returned
HDR=(CKY-R=1f9e7509c133c00f)
SA=(Enc=3DES Hash=MD5 Group=2:modp1024 Auth=PSK LifeType=Seconds LifeDuration=28800)

IKE Backoff Patterns:
IP Address      No.      Recv time      Delta Time
[redacted]      1        1456756249.384123  0.000000
[redacted]      Implementation guess: Linksys Etherfast

Ending ike-scan 1.9.4: 1 hosts scanned in 60.452 seconds (0.02 hosts/sec). 1 returned handshake; 0 returned f
```

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:

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ike-scan -h
Usage: ike-scan [options] [hosts...]

Target hosts must be specified on the command line unless the --file option is
given, in which case the targets are read from the specified file instead.

The target hosts can be specified as IP addresses or hostnames. You can also
specify IPnetwork/bits (e.g. 192.168.1.0/24) to specify all hosts in the given
network (network and broadcast addresses included), and IPstart-IPend
(e.g. 192.168.1.3-192.168.1.27) to specify all hosts in the inclusive range.

These different options for specifying target hosts may be used both on the
command line, and also in the file specified with the --file option.

In the options below a letter or word in angle brackets like <f> denotes a
value or string that should be supplied. The corresponding text should
indicate the meaning of this value or string. When supplying the value or
string, do not include the angle brackets. Text in square brackets like [<f>]
mean that the enclosed text is optional. This is used for options which take
an optional argument.

Options:
--help or -h          Display this usage message and exit.
```

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 sześćoetapowym 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:

```
*proxychains.conf
File Edit Search Options Help
# ProxyList format
#   type host port [user pass]
#   (values separated by 'tab' or 'blank')
#
#   Examples:
#
#       socks5 192.168.67.78 1080 lamer secret
#       http   192.168.89.3   8080 justu hidden
#       socks4 192.168.1.49  1080
#       http   192.168.39.93  8080
#
#   proxy types: http, socks4, socks5
#   ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...

# meanwhile
# defaults set to "tor"
socks4 127.0.0.1 9050
```

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`:

```
*proxychains.conf
File Edit Search Options Help
"
# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
# strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (as many chains as chain list from the list
```

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:

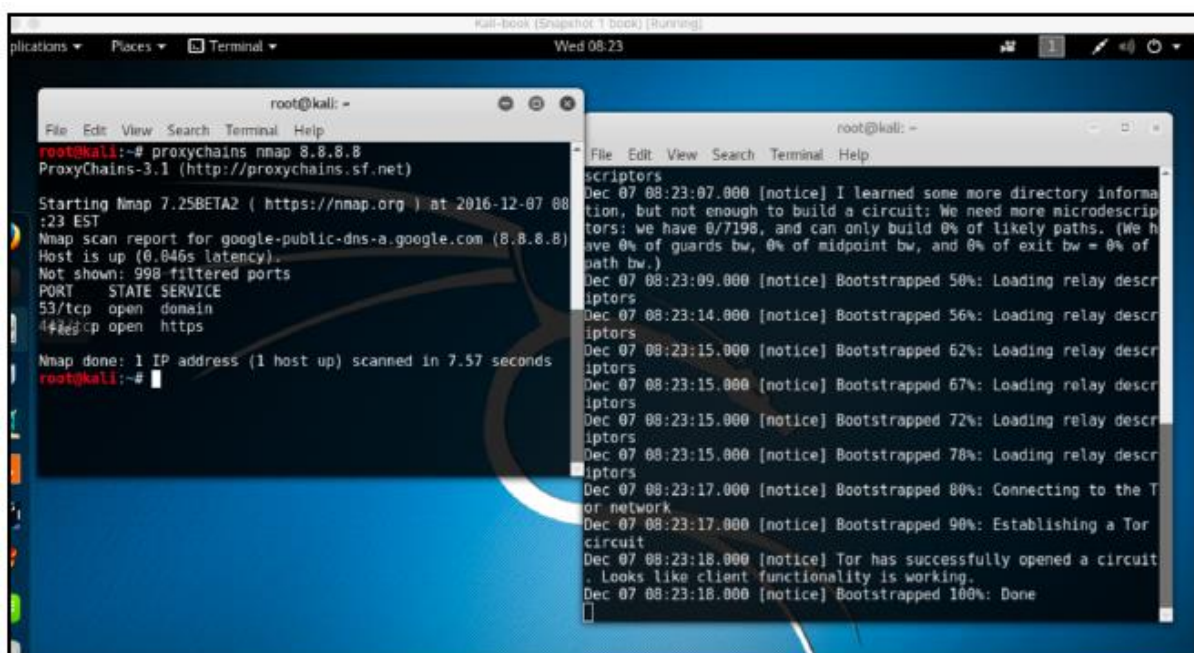
```
apt-get install tor
```

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:



```
root@kali: ~# proxychains nmap 8.8.8.8
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-07 08:23:23 EST
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.046s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 7.57 seconds
root@kali: ~#
```

```
Dec 07 08:23:07.000 [notice] I learned some more directory information, but not enough to build a circuit: We need more microdescriptors: we have 0/7198, and can only build 0% of likely paths. (We have 0% of guards bw, 0% of midpoint bw, and 0% of exit bw = 0% of path bw.)
Dec 07 08:23:09.000 [notice] Bootstrapped 50%: Loading relay descriptors
Dec 07 08:23:14.000 [notice] Bootstrapped 56%: Loading relay descriptors
Dec 07 08:23:15.000 [notice] Bootstrapped 62%: Loading relay descriptors
Dec 07 08:23:15.000 [notice] Bootstrapped 67%: Loading relay descriptors
Dec 07 08:23:15.000 [notice] Bootstrapped 72%: Loading relay descriptors
Dec 07 08:23:15.000 [notice] Bootstrapped 78%: Loading relay descriptors
Dec 07 08:23:17.000 [notice] Bootstrapped 80%: Connecting to the Tor network
Dec 07 08:23:17.000 [notice] Bootstrapped 90%: Establishing a Tor circuit
Dec 07 08:23:18.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
Dec 07 08:23:18.000 [notice] Bootstrapped 100%: Done
```

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 pożądaných 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...

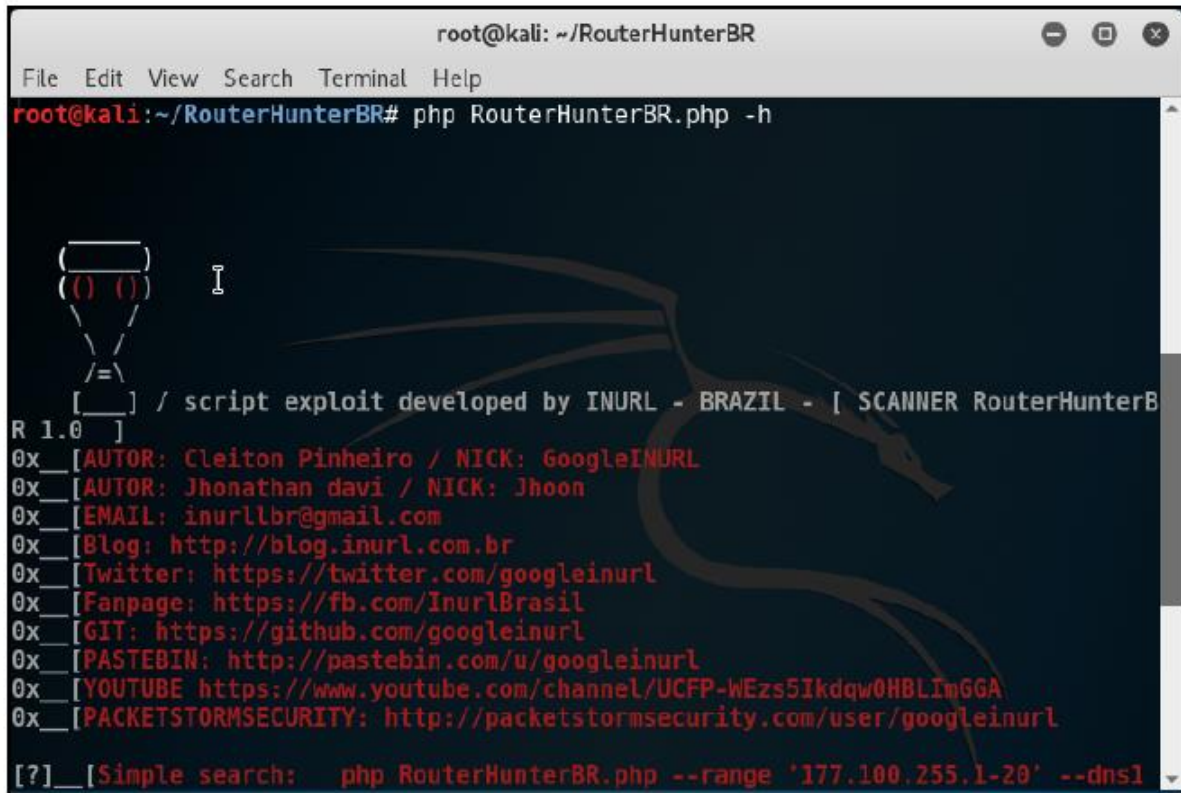
Aby uruchomić RouterHunterBR.php, wykonaj następujące kroki:

1. Po sklonowaniu pliku wejdź do katalogu.

2. Uruchom następujące polecenie:

```
php RouterHunterBR.php -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



```
root@kali: ~/RouterHunterBR
File Edit View Search Terminal Help
root@kali:~/RouterHunterBR# php RouterHunterBR.php -h

  {
  () ()
  /=\
  [ ] / script exploit developed by INURL - BRAZIL - [ SCANNER RouterHunterB
R 1.0 ]
0x_ [AUTOR: Cleiton Pinheiro / NICK: GoogleINURL
0x_ [AUTOR: Jhonathan davi / NICK: Jhoon
0x_ [EMAIL: inurlbr@gmail.com
0x_ [Blog: http://blog.inurl.com.br
0x_ [Twitter: https://twitter.com/googleinurl
0x_ [Fanpage: https://fb.com/InurlBrasil
0x_ [GIT: https://github.com/googleinurl
0x_ [PASTEBIN: http://pastebin.com/u/googleinurl
0x_ [YOUTUBE https://www.youtube.com/channel/UCFP-wEzs5Ikdqw0HBLImGGA
0x_ [PACKETSTORMSECURITY: http://packetstormsecurity.com/user/googleinurl

[?_] [Simple search: php RouterHunterBR.php --range '177.100.255.1-20' --dns1
```

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