

Zbieranie informacji wywiadowczych i planowanie strategii ataku

Wprowadzenie

Poznaliśmy podstawy polowania na subdomeny. Tu zagłębimy się nieco bardziej i przyjrzymy się innym dostępnym narzędziom do zbierania informacji wywiadowczych na temat naszego celu. Zaczynamy od użycia niesławnych narzędzi Kali Linux. Zbieranie informacji jest bardzo ważnym etapem przeprowadzania testu penetracyjnego, ponieważ każdy kolejny krok, który podejmiemy po tym, będzie całkowicie wynikiem wszystkich informacji, które zbierzemy na tym etapie. Dlatego bardzo ważne jest, abyśmy zebrali jak najwięcej informacji, zanim przejdziemy do etapu eksploatacji.

Uzyskiwanie listy subdomen

Nie zawsze mamy sytuację, w której klient zdefiniował pełny szczegółowy zakres tego, co należy poddać testowi penetracyjnemu. Dlatego wykorzystamy poniższe wymienione przepisy, aby zebrać jak najwięcej informacji, aby przeprowadzić test penetracyjny.

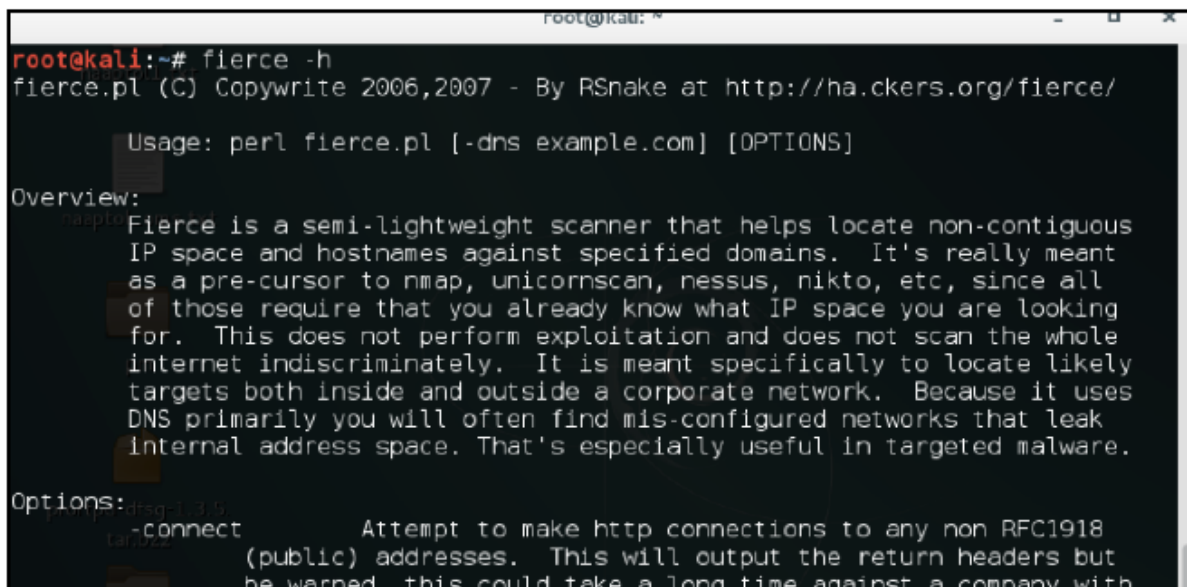
Fierce

Zaczynamy od przejścia do terminala Kali i użycia pierwszego i najszerzej używanego narzędzia Fierce.

Jak to zrobić...

Poniższe kroki pokazują użycie programu fierce:

1. Aby uruchomić program fierce, wpisujemy polecenie `fierce -h`, aby wyświetlić menu pomocy:



```
root@kali:~# fierce -h
fierce.pl (C) Copywrite 2006,2007 - By RSnake at http://ha.ckers.org/fierce/

Usage: perl fierce.pl [-dns example.com] [OPTIONS]

Overview:
Fierce is a semi-lightweight scanner that helps locate non-contiguous
IP space and hostnames against specified domains. It's really meant
as a pre-cursor to nmap, unicornscan, nessus, nikto, etc, since all
of those require that you already know what IP space you are looking
for. This does not perform exploitation and does not scan the whole
internet indiscriminately. It is meant specifically to locate likely
targets both inside and outside a corporate network. Because it uses
DNS primarily you will often find mis-configured networks that leak
internal address space. That's especially useful in targeted malware.

Options:
-dns example.com    Attempt to scan for subdomains against the specified domain
-connect            Attempt to make http connections to any non RFC1918
                    (public) addresses. This will output the return headers but
                    be warned, this could take a long time against a company with
```

2. Aby wykonać skanowanie subdomeny, używamy następującego polecenia:

```
fierce -dns host.com -threads 10
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# fierce -dns google.com -threads 10
DNS Servers for google.com:
  ns1.google.com
  ns3.google.com
  ns4.google.com
  ns2.google.com

Trying zone transfer first...
Testing ns1.google.com
  Request timed out or transfer not allowed.
Testing ns3.google.com
  Request timed out or transfer not allowed.
Testing ns4.google.com
  Request timed out or transfer not allowed.
Testing ns2.google.com
  Request timed out or transfer not allowed.

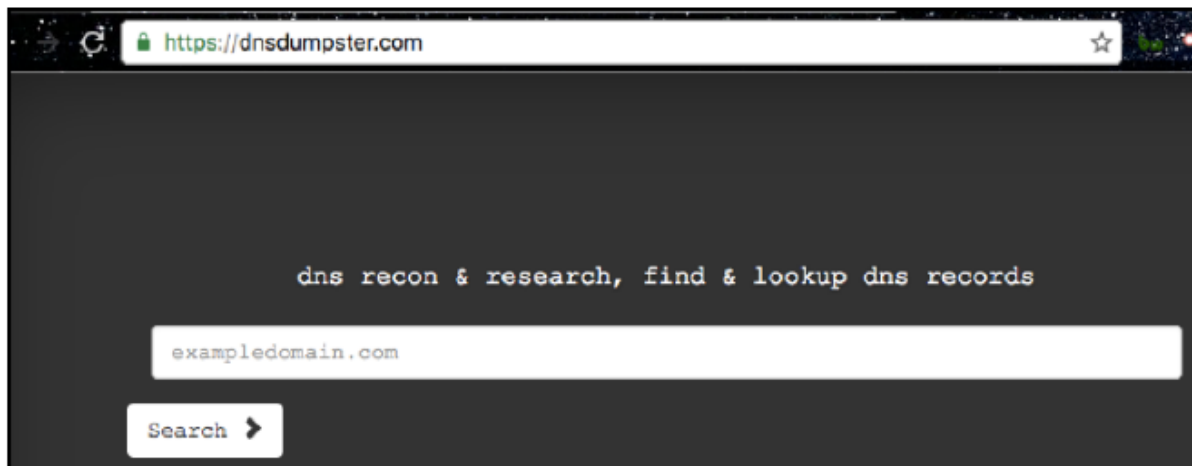
Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force
```

DNSdumpster

To darmowy projekt Hacker Target służący do wyszukiwania subdomen. Opiera się na <https://scans.io/> w celu uzyskania wyników. Może być również używany do pobierania subdomen witryny. Zawsze powinniśmy preferować używanie więcej niż jednego narzędzia do wyliczania subdomen, ponieważ możemy uzyskać coś z innych narzędzi, czego pierwsze nie wykryło.

Jak to zrobić...

Jest dość prosty w użyciu. Wpisujemy nazwę domeny, dla której chcemy uzyskać subdomeny, a on pokaże nam wyniki:



Korzystanie z Shodan dla zabawy i zysku

Shodan to pierwsza na świecie wyszukiwarka, która wyszukuje urządzenia podłączone do Internetu. Została uruchomiona w 2009 roku przez Johna Matherly'ego. Shodan może być używany do wyszukiwania kamer internetowych, baz danych, systemów przemysłowych, gier wideo itd. Shodan zbiera głównie dane dotyczące najpopularniejszych usług sieciowych, takich jak HTTP, HTTPS, MongoDB, FTP i wiele innych.

Przygotowanie

Aby korzystać z Shodan, musimy założyć konto w Shodan.

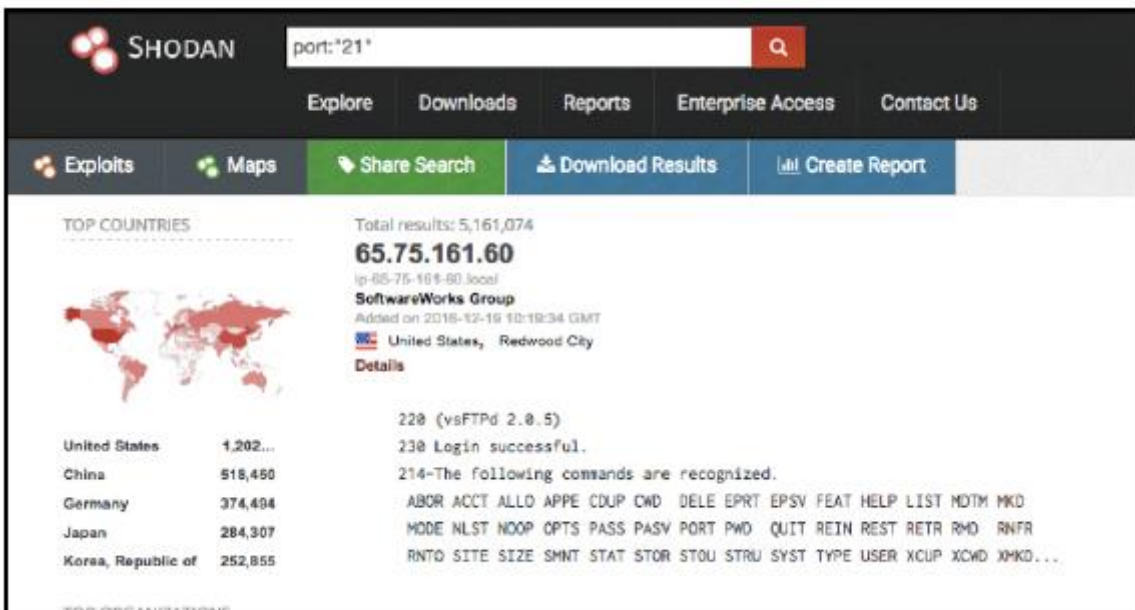
Jak to zrobić...

Aby dowiedzieć się więcej o Shodan, wykonaj poniższe kroki:

1. Otwórz przeglądarkę i odwiedź <https://www.shodan.io>:



2. Zaczynamy od wykonania prostego wyszukiwania działających usług FTP. Aby to zrobić, możemy użyć następujących dorks Shodan: `port:"21"`. Poniższy zrzut ekranu pokazuje wyniki wyszukiwania:



3. To wyszukiwanie można uczynić bardziej szczegółowym, określając konkretny kraj/organizację: port:"21" country:"IN". Poniższy zrzut ekranu pokazuje wyniki wyszukiwania:

The screenshot shows the Shodan search interface with the query 'port:21 country:IN'. The search bar is at the top, and the results are displayed below. The interface includes navigation tabs like 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area shows a list of results with columns for 'TOP COUNTRIES', 'TOP CITIES', and 'TOP ORGANIZATIONS'. The first result is for IP 103.43.7.23, belonging to Elbore Data Services Pvt. Ltd. in India. The second result is for IP 203.109.119.44, belonging to YOU Broadband & Cable India Ltd. in India. The results also show FTP service banners for each IP.

IP Address	Organization	City	Country	Service
103.43.7.23	Elbore Data Services Pvt. Ltd.		India	220 ravi skrona FTP server (Mikrotik 6.32.2) ready
203.109.119.44	YOU Broadband & Cable India Ltd.		India	220 Microsoft FTP Service

4. Teraz możemy zobaczyć wszystkie serwery FTP działające w Indiach; możemy również zobaczyć serwery, które umożliwiają anonimowe logowanie i wersję serwera FTP, na którym działają.

5. Następnie wypróbujmy filtr organizacji. Można to zrobić, wpisując port:"21" country:"IN" org:"BSNL", jak pokazano na poniższym zrzucie ekranu:

The screenshot shows the Shodan search interface with the query 'port:21 country:IN org:BSNL'. The search bar is at the top, and the results are displayed below. The interface includes navigation tabs like 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area shows a list of results with columns for 'TOP COUNTRIES', 'TOP CITIES', and 'TOP ORGANIZATIONS'. The first result is for IP 117.223.178.201, belonging to BSNL in India. The second result is for IP 117.218.140.46, belonging to BSNL in India, Bangalore. The results also show FTP service banners for each IP.

IP Address	Organization	City	Country	Service
117.223.178.201	BSNL		India, Trivandrum	220 Welcome to TBS FTP Server.
117.218.140.46	BSNL	Bangalore	India	220 ucftpd FTP server ready.

Shodan ma również inne tagi, których można używać do przeprowadzania zaawansowanych wyszukiwań, takie jak:

net: skanowanie zakresów adresów IP

city: filtrowanie według miasta

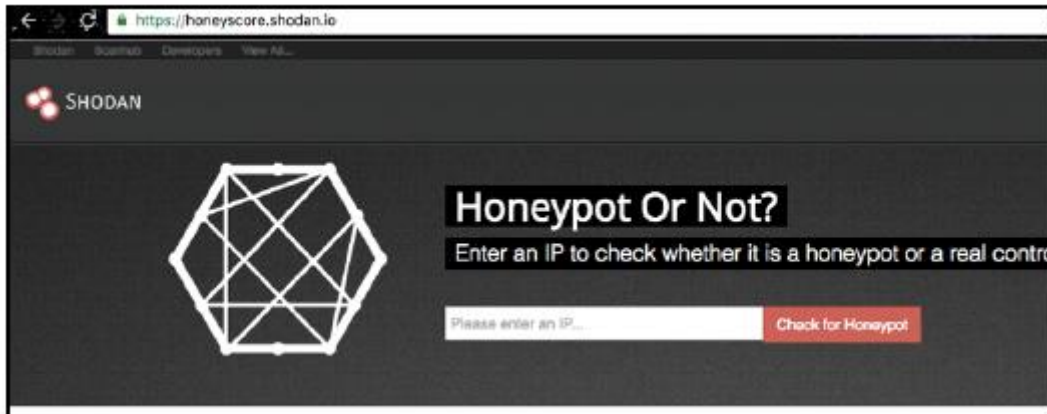
Shodan Honeyscore

Shodan Honeyscore to kolejny świetny projekt zbudowany w Pythonie. Pomaga nam ustalić, czy adres IP, który mamy, jest honeypotem, czy prawdziwym systemem.

Jak to zrobić...

Poniższe kroki demonstrują użycie Shodan Honeyscore:

1. Aby użyć Shodan Honeyscore, odwiedzamy <https://honeyscore.shodan.io/> :



2. Wpisz adres IP, który chcesz sprawdzić i gotowe!

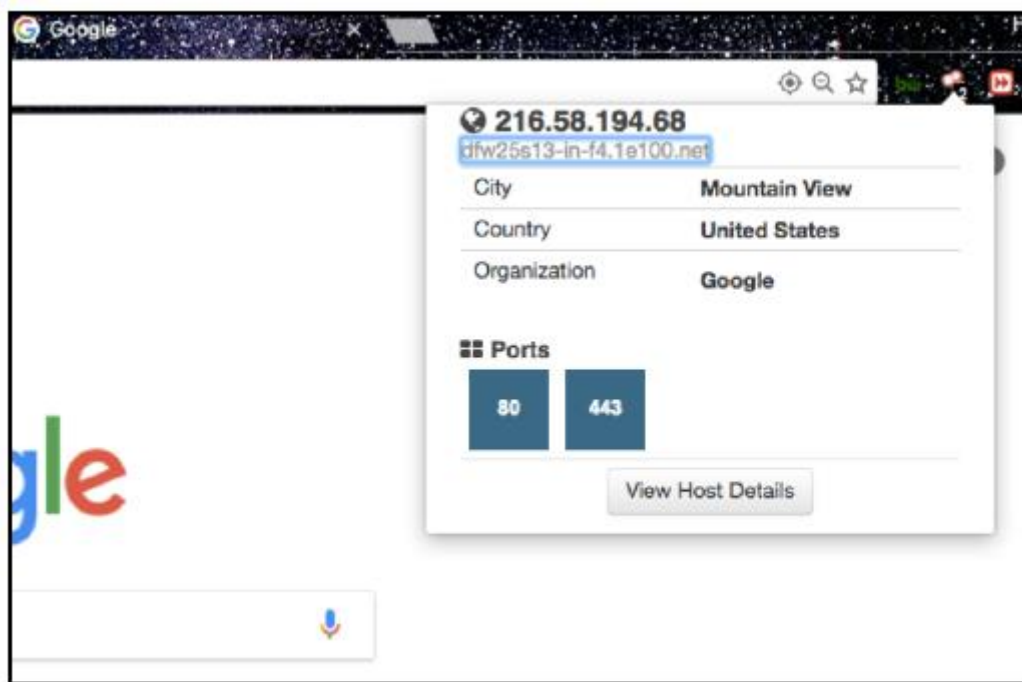


Wtyczki Shodan

Aby jeszcze bardziej ułatwić nam życie, Shodan ma wtyczki do przeglądarek Chrome i Firefox, których można używać do sprawdzania otwartych portów dla stron internetowych, które odwiedzamy w podróży!

Jak to zrobić...

Pobieramy i instalujemy wtyczkę z <https://www.shodan.io/> . Przeglądaj dowolną stronę internetową, a zobaczymy, że klikając na wtyczkę możemy zobaczyć otwarte porty:



Używanie Nmap do znajdowania otwartych portów

Network Mapper (Nmap) to skaner bezpieczeństwa napisany przez Gordona Lyona. Służy do znajdowania hostów i usług w sieci. Po raz pierwszy pojawił się we wrześniu 1997 r. Nmap ma różne funkcje, a także skrypty do wykonywania różnych testów, takich jak znajdowanie systemu operacyjnego, wersji usługi, siłowe wymuszanie domyślnych logowań itd.

Niektóre z najczęstszych typów skanowania to:

Skanowanie TCP connect()

Skanowanie SYN stealth

Skanowanie UDP

Skanowanie ping

Skanowanie w trybie bezczynności

Jak to zrobić...

Oto przepis na korzystanie z Nmap:

1. Nmap jest już zainstalowany w systemie Kali Linux. Możemy wpisać następujące polecenie, aby go uruchomić i zobaczyć wszystkie dostępne opcje:

```
nmap -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# nmap -h
Nmap 7.01 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
```

2. Aby wykonać podstawowe skanowanie, używamy następującego polecenia:

```
nmap -sV -Pn x.x.x.x
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# nmap -sV -Pn 192.168.1.1
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-19 14:52 MSK
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 14:53 (0:00:06 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 14:54 (0:00:12 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0091s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp
23/tcp    open  tcpwrapped
53/tcp    open  domain
80/tcp    open  http         Realtron WebServer 1.1
5431/tcp  open  upnp         MiniUPnP
```

3. -Pn oznacza, że nie sprawdzamy, czy host jest włączony, czy nie, wykonując najpierw żądanie ping. Parametr -sV służy do wyświetlania listy wszystkich uruchomionych usług na znalezionych otwartych portach.

4. Inną flagą, której możemy użyć, jest -A, która automatycznie wykonuje wykrywanie systemu operacyjnego, wykrywanie wersji, skanowanie skryptów i traceroute. Polecenie to:

```
nmap -A -Pn x.x.x.x
```

5. Aby przeskanować zakres adresów IP lub wiele adresów IP, możemy użyć tego polecenia:

```
nmap -A -Pn x.x.x.0/24
```

Korzystanie ze skryptów

Nmap Scripting Engine (NSE) umożliwia użytkownikom tworzenie własnych skryptów w celu automatycznego wykonywania różnych zadań. Skrypty te są wykonywane obok siebie podczas

skanowania. Można ich używać do skuteczniejszego wykrywania wersji, wykorzystywania luk w zabezpieczeniach itd. Polecenie do korzystania ze skryptu to:

```
nmap -Pn -sV host.com --script dns-brute
```

```
root@kali:~# nmap -sV google.com --script dns-brute
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-19 14:56 MSK
_
```

Wynik poprzedniego polecenia jest następujący:

```
Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|   id.google.com - 216.58.220.195
|   images.google.com - 216.58.197.78
|   admin.google.com - 216.58.220.206
|   admin.google.com - 2404:6800:4002:804:0:0:0:200e
|   ads.google.com - 216.58.220.206
|   ads.google.com - 2404:6800:4002:804:0:0:0:200e
|   alerts.google.com - 216.58.220.206
|   news.google.com - 216.58.220.206
|   alerts.google.com - 2404:6800:4002:804:0:0:0:200e
|   news.google.com - 2404:6800:4002:804:0:0:0:200e
|   upload.google.com - 216.58.220.207
|   dns.google.com - 216.58.220.206
```

W tym przypadku skrypt dns-brute próbuje pobrać dostępne subdomeny metodą siłową na podstawie zestawu powszechnych nazw subdomen.

Omijanie zapór sieciowych za pomocą Nmap

W większości przypadków podczas testów penetracyjnych natrafimy na systemy chronione przez zapory sieciowe lub systemy wykrywania włamań (IDS). Nmap udostępnia różne sposoby omijania tych systemów IDS/zapór sieciowych w celu skanowania portów w sieci. W tym przepisie poznamy kilka sposobów omijania zapór sieciowych.

Skanowanie TCP ACK

Skanowanie ACK (-sA) wysyła pakiety potwierdzenia zamiast pakietów SYN, a zapora sieciowa nie tworzy dzienników pakietów ACK, ponieważ traktuje pakiety ACK jako odpowiedzi na pakiety SYN. Jest ono najczęściej używane do mapowania typu używanej zapory sieciowej.

Jak to zrobić...

Skanowanie ACK zostało stworzone, aby pokazywać niefiltrowane i filtrowane porty zamiast otwartych. Polecenie dla skanowania ACK to:

```
nmap -sA x.x.x.x
```

Przyjrzyjmy się porównaniu różnic między zwykłym skanowaniem a skanowaniem ACK:


```
root@kali:~# nmap -Pn 1 [redacted]
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:18 MSK
Nmap scan report for 180.[redacted]
Host is up.
All 1000 scanned ports on 180.[redacted] are filtered
```

Tutaj widzimy różnicę pomiędzy normalnym skanowaniem a skanowaniem ACK:

```
root@kali:~# nmap -sA 1 [redacted]
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:32 MSK
Nmap scan report for 1 [redacted]
Host is up (0.00034s latency).
All 1000 scanned ports on 1 [redacted] are unfiltered
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
root@kali:~#
```

Jak to działa...

Wyniki skanowania portów filtrowanych i niefiltrowanych zależą od tego, czy używana zaporą jest stanowa czy bezstanowa. Zaporą stanowa sprawdza, czy przychodzący pakiet ACK jest częścią istniejącego połączenia, czy nie. Blokuje go, jeśli pakiety nie są częścią żadnego żądanego połączenia. Dlatego port będzie wyświetlany jako filtrowany podczas skanowania. Podczas gdy w przypadku zapory bezstanowej nie będzie blokować pakietów ACK, a porty będą wyświetlane jako niefiltrowane.

Skanowanie okna TCP

Skanowanie okna (-sW) jest prawie takie samo jak skanowanie ACK, z tą różnicą, że pokazuje otwarte i zamknięte porty.

Jak to zrobić...

Przyjrzyjmy się różnicom między normalnym skanowaniem a skanowaniem TCP:

1. Polecenie do uruchomienia to:

```
nmap -sW x.x.x.x
```

2. Przyjrzyjmy się porównaniu różnic między normalnym skanowaniem a skanowaniem okna TCP:

```
root@kali:~# nmap -Pn 1 [redacted]
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:18 MSK
Nmap scan report for 180.[redacted]
Host is up.
All 1000 scanned ports on 180.[redacted] are filtered
```

3. Różnicę między dwoma skanami możemy zobaczyć na poniższym zrzucie ekranu:

```
root@kali:~# nmap -sW 1
Starting Nmap 7.01 ( https://nmap.org ) at 2016-12-18 20:33 MSK
Nmap scan report for 1
Host is up (0.00035s latency).
PORT      STATE SERVICE
1/tcp    open  tcpmux
3/tcp    open  compressnet
4/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
```

Skanowanie w trybie bezczynności

Skanowanie w trybie bezczynności to zaawansowana technika, w której nie można powiązać żadnych pakietów wysłanych do celu z maszyną atakującego. Wymaga określenia hosta zombie.

Jak to zrobić...

Polecenie wykonania skanowania w trybie bezczynności to:

```
nmap -sI zombiehost.com domain.com
```

Jak to działa...

Skanowanie w trybie bezczynności działa na podstawie przewidywalnego IPID lub identyfikatora fragmentacji IP hosta zombie. Najpierw sprawdzany jest IPID hosta zombie, a następnie żądanie połączenia jest podszywane z tego hosta do hosta docelowego. Jeśli port jest otwarty, potwierdzenie jest wysyłane z powrotem do hosta zombie, który resetuje (RST) połączenie, ponieważ nie ma historii otwierania takiego połączenia. Następnie atakujący ponownie sprawdza IPID na zombie; jeśli zmienił się o jeden krok, oznacza to, że od celu otrzymano RST. Ale jeśli IPID zmienił się o dwa kroki, oznacza to, że host zombie otrzymał pakiet od hosta docelowego i na hoście zombie był RST, co oznacza, że port jest otwarty.

Wyszukiwanie otwartych katalogów

W poprzednim przepisie omówiliśmy, jak znaleźć otwarte porty w sieciowym adresie IP lub nazwie domeny. Często widzimy programistów uruchamiających serwery WWW na różnych portach. Czasami programiści mogą również pozostawiać katalogi nieprawidłowo skonfigurowane, które mogą zawierać dla nas ciekawe informacje. Omówiliśmy już dirsearch w poprzednim rozdziale; tutaj przyjrzymy się alternatywom.

Narzędzie dirb

Narzędzie dirb jest dobrze znanym narzędziem, którego można użyć do siłowego otwierania katalogów. Chociaż jest ogólnie powolne i nie obsługuje wielowątkowości, nadal jest świetnym sposobem na znalezienie katalogów/podkatalogów, które mogły zostać pozostawione otwarte z powodu błędnej konfiguracji.

Jak to zrobić...

Wpisz następujące polecenie, aby uruchomić narzędzie:

dirb https://domain.com

Poniższy zrzut ekranu pokazuje dane wyjściowe poprzedniego polecenia:

```
root@kali:~# dirb https://google.com
-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Sun Dec 18 22:15:29 2016
URL_BASE: https://google.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: https://google.com/ ----
+ https://google.com/2001 (CODE:301|SIZE:224)
```

Jest jeszcze więcej...

W dirb są też inne opcje, które mogą się przydać:

- a: aby określić agenta użytkownika
- c: aby określić plik cookie
- H: aby wprowadzić niestandardowy nagłówek
- X: aby określić rozszerzenie pliku

Wykonywanie głębokiej magii za pomocą DMitry

Narzędzie Deepmagic Information Gathering Tool (DMitry) to aplikacja typu open source z wiersza poleceń, zakodowana w języku C. Ma możliwość zbierania subdomen, adresów e-mail, informacji whois itd. o celu.

Jak to zrobić...

Aby dowiedzieć się więcej o DMitry, wykonaj poniższe kroki:

1. Używamy prostego polecenia:

```
dmitry -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali: ~  
root@kali:~# dmitry -h  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
dmitry: invalid option -- 'h'  
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host  
-o      Save output to %host.txt or to file specified by -o file  
-i      Perform a whois lookup on the IP address of a host  
-w      Perform a whois lookup on the domain name of a host  
-n      Retrieve Netcraft.com information on a host  
-s      Perform a search for possible subdomains  
-e      Perform a search for possible email addresses  
-p      Perform a TCP port scan on a host  
* -f    Perform a TCP port scan on a host showing output reporting filtered ports  
* -b    Read in the banner received from the scanned port  
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )  
*Requires the -p flagged to be passed
```

2. Następnie próbujemy wykonać skanowanie poczty e-mail, whois, portu TCP i wyszukiwanie subdomeny za pomocą następującego polecenia:

```
dmitry -s -e -w -p domain.com
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# dmitry -s -e -w -p google.com  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
HostIP:216.58.220.206  
HostName:google.com  
  
Gathered Inic-whois information for google.com  
-----  
Domain Name: GOOGLE.COM  
Registrar: MARKMONITOR INC.  
Sponsoring Registrar IANA ID: 292  
Whois Server: whois.markmonitor.com  
Referral URL: http://www.markmonitor.com  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM
```

Polowanie na luki w SSL

Większość dzisiejszych aplikacji internetowych używa SSL do komunikacji z serwerem. sslscan to świetne narzędzie do sprawdzania błędów SSL lub błędnych konfiguracji.

Jak to zrobić...

Aby dowiedzieć się więcej o sslscan, wykonaj następujące kroki:

1. Przyjrzyjmy się podręcznikowi pomocy, aby zobaczyć różne opcje narzędzia:

```
sslscan -h
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# sslscan -h
1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx
Command:
sslscan [Options] [host:port | host]
```

2. Aby uruchomić narzędzie na hoście, wpisujemy:

```
sslscan host.com:port
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# sslscan google.com
Version: 1.10.5-static
OpenSSL 1.0.2e-dev xx XXX xxxx
Testing SSL server google.com on port 443
  TLS renegotiation:
Secure session renegotiation supported
  TLS Compression:
Compression disabled
  Heartbleed:
TLS 1.0 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.2 not vulnerable to heartbleed
```

TLSSled to również alternatywa, której możemy użyć w Kali do wykonywania kontroli SSL.

Eksplorowanie połączeń za pomocą intrace

Narzędzie intrace to świetne narzędzie do enumeracji przeskoków IP w istniejących połączeniach TCP. Może być przydatne do omijania zapory i zbierania większej ilości informacji o sieci.

Jak to zrobić...

Uruchom następujące polecenie:

```
intrace -h hostname.com -p port -s sizeofpacket
```

TLSSLed to również alternatywa, której możemy użyć w Kali do wykonywania kontroli SSL.

```
root@kali:~# intrace -h google.com -p 443 -s 4_
```

Kopanie głęboko z theharvester

Narzędzie theharvester jest świetnym narzędziem do testów penetracyjnych, ponieważ pomaga nam znaleźć wiele informacji o firmie. Można go używać do wyszukiwania kont e-mail, subdomen itd. W tym przepisie nauczymy się, jak używać go do odkrywania danych.

Jak to zrobić...

Polecenie jest dość proste:

```
theharvester -d domain/name -l 20 -b all
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@kali:~# theharvester -d packtpub -l 10 -b linkedin
*****
*
*  TheHarvester
*
* TheHarvester Ver. 2.6
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[-] Searching in LinkedIn..
-
```

Jak to działa...

W poprzednim przepisie -d oznacza nazwę domeny lub słowo kluczowe, które chcemy wyszukać, -l ogranicza liczbę wyników wyszukiwania, a -b oznacza źródło, którego chcemy, aby narzędzie używało podczas zbierania informacji. Narzędzie obsługuje źródła Google, Google CSE, Bing, Bing API, PGP, LinkedIn, Google Profiles, people123, Jigsaw, Twitter i Google Plus.

Znajdowanie technologii stojącej za aplikacjami internetowymi Nie ma sensu rozpoczynać testu penetracyjnego aplikacji internetowej bez znajomości faktycznej technologii, która za nią stoi. Na przykład, byłoby absolutnie bezużyteczne uruchamianie dirsearch w celu wyszukania plików z rozszerzeniem .php, gdy technologią jest w rzeczywistości ASP.NET. Tak więc w tym przepisie nauczymy się używać prostego narzędzia whatweb, aby zrozumieć technologię stojącą za aplikacją internetową. Jest ono domyślnie dostępne w Kali. Można je również zainstalować ręcznie z adresu URL <https://github.com/urbanadventurer/WhatWeb>. Jak to zrobić...

Użycie whatweb można wykonać w następujący sposób:

1. Narzędzie można uruchomić za pomocą następującego polecenia:

Wykrywanie za pomocą Kismet

Kismet to detektor sieci bezprzewodowych warstwy 2. Przydaje się, ponieważ podczas przeprowadzania testów penetracyjnych w środowisku korporacyjnym możemy również potrzebować poszukać sieci bezprzewodowych. Kismet może wykrywać ruch 802.11a/b/g/n. Działa z dowolną kartą bezprzewodową obsługującą tryby monitorowania surowego. W tym przepisie nauczymy się, jak używać Kismet do monitorowania sieci Wi-Fi.

Jak to zrobić...

Aby dowiedzieć się więcej o Kismet, wykonaj następujące kroki:

1. Używamy następującego polecenia, aby uruchomić Kismet:

```
kismet
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```
root@bt: ~
File Edit View Terminal Help
Kismet Sort View Windows
Name      T  C  Ch  Pkts  Size      Kismet
[ --- No networks seen --- ]
Not
Connected

Terminal colors
Some terminals don't display some colors (notably, dark grey)
correctly. The next line of text should read 'Dark grey text':
Dark grey text
Is it visible? If you answer 'No', dark grey
will not be used in the default color scheme. Remember, you
can always change colors to your taste by going to
Kismet->Preferences->Colors.

[ No ] [ Yes ]

INFO: Failed to load preferences file, will use defaults
INFO: Auto-connecting to tcp://localhost:2501
ERROR: Could not connect to Kismet server 'localhost:2501' (Connecti
INFO: Welcome to the Kismet Newcore Client... Press '' or '~' to ac
```

2. Po uruchomieniu interfejsu graficznego zostaniemy poproszeni o uruchomienie serwera, dlatego wybieramy opcję „tak”:


```

root@bt: ~
File Edit View Terminal Help
~ Kismet Sort View Windows
Name T C Ch Pkts Size Kismet
[ --- No networks seen --- ] Not
Connected

No GPS info (GPS not connected)
0
Start Kismet Server
Automatically start Kismet server?
Launch Kismet server and connect to it automatically.
If you use a Kismet server started elsewhere, choose
No and change the Startup preferences.
0 [ No ] [ Yes ]

Data
(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.
ERROR: Could not connect to Kismet server 'localhost:2501'
(Connection refused) will attempt to reconnect in 5 seconds.

```

3. Następnie musimy określić interfejs źródłowy, w naszym przypadku jest to wlan0, więc wpisujemy go. Upewnij się, że interfejs jest w trybie monitora przed zainicjowaniem go w Kismet:

```

root@bt: ~
File Edit View Terminal Help
Kismet Server Console
INFO: Creating network tracker...
ERROR: Reading config file '/root/.kismet//ssid_map.conf': 2 (No such file or
ERROR: Reading config file '/root/.kismet//tag.conf': 2 (No such file or dire
INFO: Creating channel tracker...
INFO: Registering dumpfiles...
INFO: Pcap log in PPI format
INFO: Opened pcapdu
INFO: Opened netxml
INFO: Opened nettxt
INFO: Opened gpsxml
INFO: Opened alert
INFO: Kismet starti
INFO: No packet sou
client, or by
(/usr/local/e
ERROR: Could not co
INFO: Kismet server accepted connection from 127.0.0.1
ERROR: Could not connect to the GPSD server, will reconnect in 10 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 15 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 20 seconds
ERROR: Could not connect to the GPSD server, will reconnect in 25 seconds

pcapdump'
txml'
ttxt'
sxml'
rt'

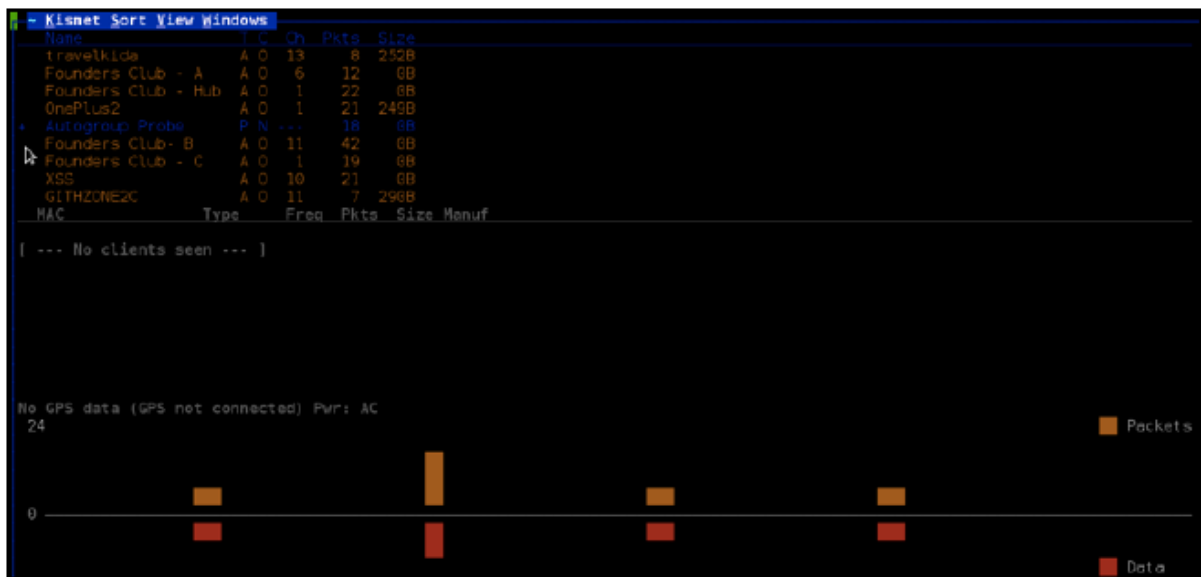
he Kismet

[ Cancel ] [ Add ]

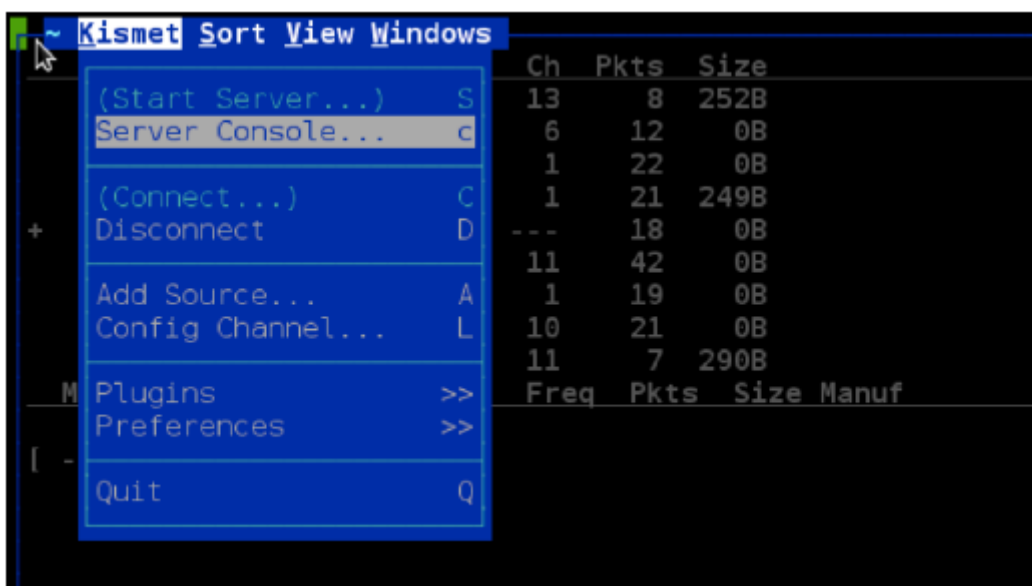
[ Kill Server ] [ Close Console Window ]

```

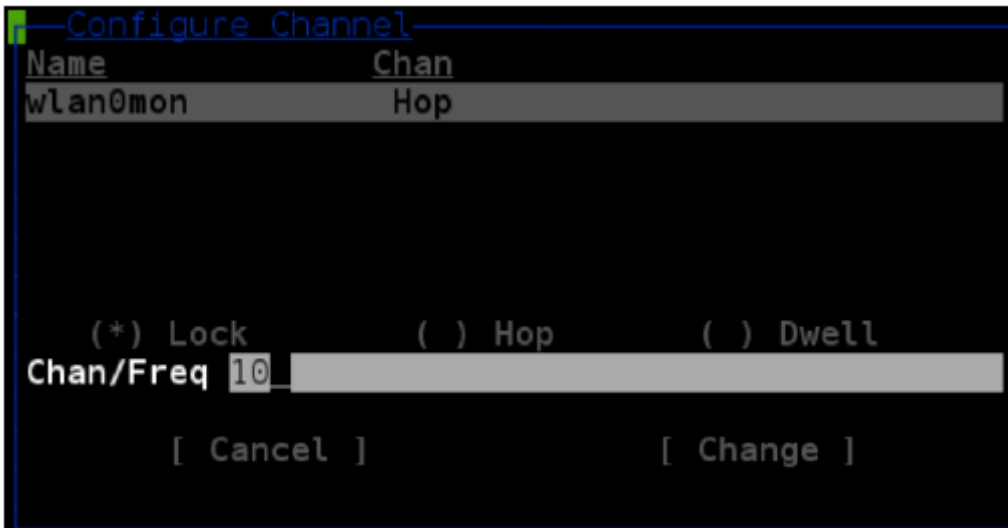
4. Teraz zobaczymy listę wszystkich sieci bezprzewodowych wokół nas:



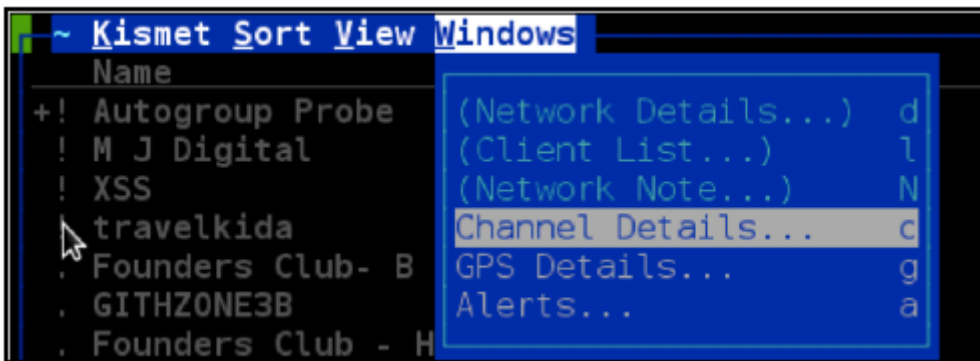
5. Domyślnie Kismet nasłuchuje na wszystkich kanałach, więc możemy określić konkretny kanał, wybierając pozycję Konfiguracja kanału... z menu Kismet:



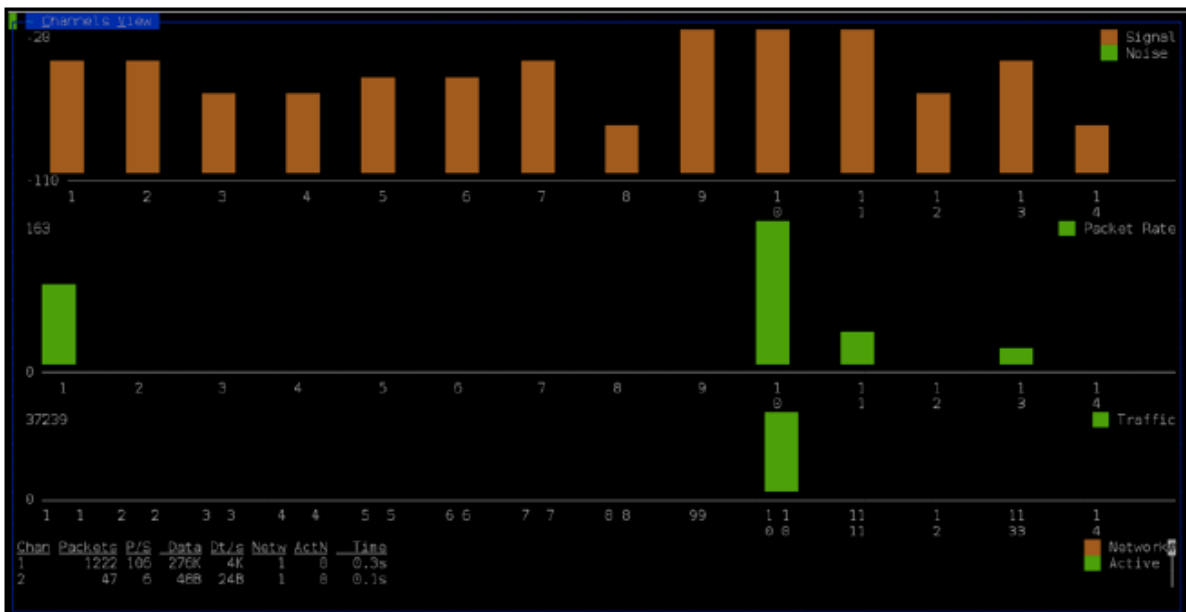
6. Tutaj możemy wybrać numer kanału:



7. Kismet pozwala nam również zobaczyć stosunek sygnału do szumu. Możemy to zobaczyć wybierając Channel Details... w menu Windows:



8. Ten stosunek sygnału do szumu jest bardzo pomocny w czasie wardrivingu:



Testowanie routerów za pomocą Firewall

Narzędzie Firewalk to narzędzie do rozpoznawania zabezpieczeń sieci, które pomaga nam ustalić, czy nasze routery faktycznie wykonują zadanie, do którego zostały powołane. Próbuje ono znaleźć protokoły, na które router/zapora sieciowa zezwoli, a które zablokuje. To narzędzie jest niezwykle przydatne podczas testów penetracyjnych w celu weryfikacji i walidacji zasad zapory sieciowej w środowisku korporacyjnym.

Jak to zrobić...

Oto przepis na użycie Firewalk:

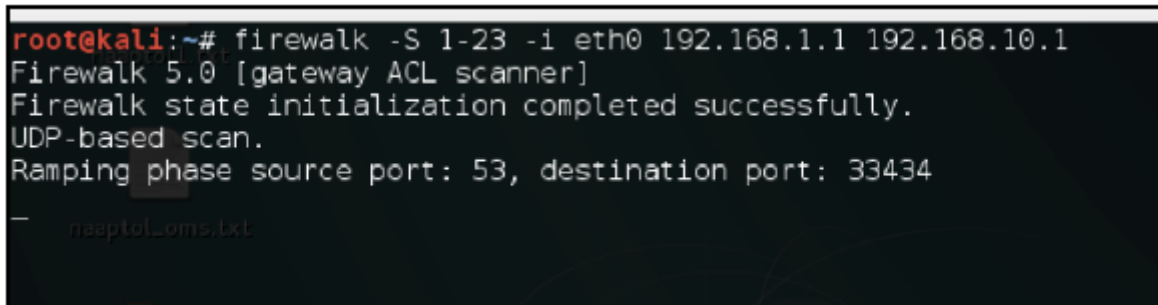
1. Jeśli Firewalk nie zostanie znaleziony, możemy go zainstalować za pomocą:

```
apt install firewalk
```

2. Możemy użyć następującego polecenia, aby uruchomić Firewalk:

```
firewalk -S 1-23 -i eth0 192.168.1.1 192.168.10.1
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:



```
root@kali:~# firewalk -S 1-23 -i eth0 192.168.1.1 192.168.10.1
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 33434
—
nsaptdLoms.txt
```

Jak to działa...

W poprzednim poleceniu `-i` służy do określania interfejsu sieciowego, `-S` służy do określania numerów portów, które chcemy przetestować, a następne dwa to adres IP routera i adres IP hosta, który chcemy sprawdzić na naszym routerze. Nmap zawiera również skrypt do wykonywania firewalk.