NetBIOS Enumeration Wtih nmap & nbstat

NetBIOS Enumeration

With NetBIOS Enumeration we can scan a local area network or a specific target on the intranet and extract NetBIOS information from it like.

- Devices that belong to a domain
- Storage shares on the network
- Domain policies and passwords
- Printers on the network
- Group information and users

NetBIOS

Stands for Network Basic Input Output System and allows communication between different applications running on different systems within a LAN.

The service uses a 16 ASCII character string to identify a device on a local network.

The first 15th characters are for identifying devices, the last 16th character is to identify services.

Services and ports.

- UDP/137 Name service
- UDP/138 Datagram service
- TCP/139 Session service

In this quick guide i am using nmap, nbtstat on Windows, and NBTScan on Kali Linux. NBTSan can be run on Windows to if you what to try it there.

You can find several tools on all platforms that you can use for NetBIOS Enumeration, if you wish to test some other tools.

DISCLAIMER: This software/tutorial is for educational purposes only. Please don’t use it for illegal activity. The author is not responsible for the use of the application or the users action.

Common NetBIOS Name Table (NBT) names

NetBIOS Code	Type	Information
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<host name><03>	UNIQUE	Messenger service
<use rname><03>	UNIQUE	Logged-in user
<20>	UNIQUE	File Server Service

NetBIOS Code	Type	Information
<21>	UNIQUE	RAS Client Service
<22>	UNIQUE	Microsoft Exchange
<1B>	UNIQUE	Domain Master Browser
<1C>	GROUP	Domain Controllers
<1D>	GROUP	Master Browser
<INet~Services>	GROUP	IIS

Requirements

- Kali Linux
- NBTScan
- Nmap
- Windows AD
- Windows client on the same LAN as the Windows AD

Step 1: NetBIOS Enumeration With nbtstat in Windows

Open a CMD in windows and type in the fallowing syntax.

```
nbtstat -A 192.168.100.11
```

```
Ethernet0:
Node IpAddress: [192.168.100.12] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    ONLINE-IT      <00>  GROUP       Registered
    SRV1           <00>  UNIQUE      Registered
    ONLINE-IT      <1C>  GROUP       Registered
    SRV1           <20>  UNIQUE      Registered
    ONLINE-IT      <1B>  UNIQUE      Registered

    MAC Address = 01:0c:29:3c:83:4e


Npcap Loopback Adapter:
Node IpAddress: [169.254.33.233] Scope Id: []

    Host not found.

C:\>
```

Step 2: NetBIOS Enumeration With NBTScan

NBTScan is by default installed on Kali Linux, but there is a Windows version as well.

NOTE: You need to open the tool in CMD for it to work in Windows.

We can use the tool to scan a whole network or just one target.

```
C:\NBTScan>nbtscan.exe  192.168.100.11-254
```

```
Doing NBT name scan for addresses from 192.168.100.11-254

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.11   SRV1             <server>  <unknown>        01:0c:29:3c:83:4e
192.168.100.12   SRV2             <server>  <unknown>        01-0a-49-67-b8-01

C:\NBTScan>
```

Adding more arguments to the syntax to extract more information.

```
C:\NBTScan>nbtscan.exe -v 192.168.100.11
```

```
Doing NBT name scan for addresses from 192.168.100.11


NetBIOS Name Table for Host 192.168.100.11:

Incomplete packet, 191 bytes long.
Name             Service          Type
----------------------------------------
ONLINE-IT        <00>              GROUP
SRV1             <00>             UNIQUE
ONLINE-IT        <1c>              GROUP
SRV1             <20>             UNIQUE
ONLINE-IT        <1b>             UNIQUE

Adapter address: 01:0c:29:3c:83:4e
----------------------------------------

C:\NBTScan>
```

You can find more arguments in NBTScan:s official documentation.

Step 3: NetBIOS Enumeration With Nmap Scripting Engine

To run the nbstat.nse script, open Nmap and run the following syntax.

```
nmap -sV 192.168.100.11 --script nbstat.nse -v
```

```
Host script results:
```

```
| nbstat: NetBIOS name: SRV1, NetBIOS user: <unknown>, NetBIOS MAC:
01:0c:29:3c:83:4e (VMware)

| Names:

|   ONLINE-IT<00>        Flags: <group><active>

|   SRV1<00>             Flags: <unique><active>

|   ONLINE-IT<1c>        Flags: <group><active>

|   SRV1<20>             Flags: <unique><active>

|_  ONLINE-IT<1b>        Flags: <unique><active>



NSE: Script Post-scanning.

Initiating NSE at 17:50

Completed NSE at 17:50, 0.00s elapsed

Initiating NSE at 17:50

Completed NSE at 17:50, 0.00s elapsed

Read data files from: C:\Program Files (x86)\Nmap

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 141.97 seconds

           Raw packets sent: 1033 (45.436KB) | Rcvd: 1011 (41.756KB)
```

Conclusion

As we can see it easy to extract information with NetBIOS Enumeration techniques and tools.

We have used tools on both Windows and Linux and scanned an AD server on the domain.

To countermeasure NetBIOS enumeration you need to disable the service, however some old applications still relays on NetBIOS communication.

Check out the Ethical Hacking notes for more Kali Linux quick guides.

How To Scan a Network With Nmap

How To Scan With Nmap

Nmap is a great tool to learn, the application have the ability to scan and map networks and much more, it is a great tool for everybody that works in IT.

It is the first tool i use when i want troubleshot, we can do regular ping or a ping sweeps that scans a range of the subnet or the whole subnet.

The application also offers host discovery, port discovery, operating system version discovery, MAC address, services, exploit and vulnerability detection.

Another great tool to use while learning nmap is Wireshark, It is highly recommended to run Wireshark wile using nmap, following the flow of network traffic will help you analyze and visuals the scans.

We will try some of the popular scanning method that can be used with nmap.

This guide is just meant to give you high level understanding on how to use the different scanning techniques.

Please don't scan networks or host you are not authorized to do. The networks and hosts scanned in the guide is my home lab.

If you want a more in-depth explanation on how you can use nmap and the switches, i recommend that you read "The Official Nmap Project Guide to Network Discovery and Security Scanning".

Save Output To Txt/Xml File

Description	Command	Example
Save output to file	nmap -oN [file.txt] [Target]	nmap -oN file.txt 192.168.100.11
Save output as XML	nmap -oX [file.xml] [Target]	nmap -oX file.xml192.168.100.11
Save in all formats	nmap -oA [file] [Target]	nmap -oA file 192.168.100.11

Basic Scanning

Description	Command	Example
Scan a single host	nmap [Target]	nmap 192.168.100.100
Scan multiple targets	nmap [Target1, Target2]	nmap 192.168.100.10,192.168.100.100

Description	Command	Example
Scan a range of IP address	nmap [IP Range]	nmap 192.168.100.10-99
Scan a Class C subnet	nmap [IP/CDIR]	nmap 192.168.100.0/24
Resolve FQDN	nmap [FQDN]	nmap www.eaxmple.com

Quick Scans

Description	Command	Example
Ping scan	nmap -sP [Target]	nmap -sP 192.168.100.11
Ping Scan – disable port scanining	nmap -sn [Target]	nmap -sn 192.168.100.0/24

-sP switch can be used when you want to make a quick ping, the host or hosts will replay to ICMP ping packets.

```
nmap -sP 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:05 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.84 seconds
```

The **-sn** switch is used to to sweep a network without doing any port scans.

```
nmap -sn 192.168.100.0/24

Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-02 00:02 W. Europe Daylight Time
Nmap scan report for 192.168.100.1
Host is up (0.0010s latency).
Nmap scan report for srv1.online-it.nu (192.168.100.11)
Host is up (0.0020s latency).
Nmap scan report for 192.168.100.13
```

```
Host is up (0.0010s latency).
Nmap scan report for srv7.home.local (192.168.100.17)
Host is up (0.0011s latency).
Nmap scan report for 192.168.100.100
Host is up (0.0013s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.82 seconds
```

Banner Grabbing & Service Detection

Description	Command	Example
Detect OS	nmap -O [Target]	nmap -O 192.168.100.11
Detect OS & Services	nmap -A [Target]	nmap -A 192.168.100.11
Detect Services	nmap -sV [Target]	nmap -sV 192.168.100.11

The **-O** switch scans for operating system details. This type of scan can be used to identify the operating system of the scanned host and the services the host is running.

```
nmap -O 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:12 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.00032s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016 build 10586 - 14393
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.96 seconds
```

Port Scans Types

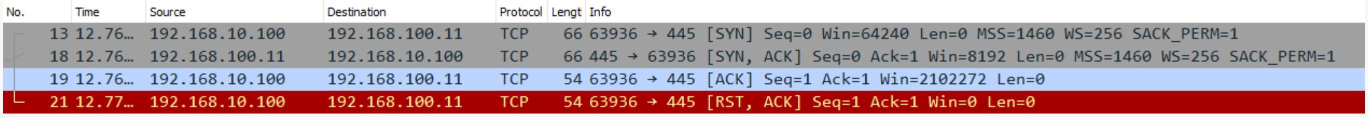
Description	Command	Example
Scan a single Port	nmap -p [Port] [Target]	nmap -p 80 192.168.100.11
Scan a range of ports	nmap -p [Port-Port] [Target]	nmap -p 20-99 192.168.100.11
Scan the first 100 ports	nmap -F [Port] [Target]	nmap -F 192.168.100.11
Scan using TCP Handshake	nmap -sT [Target]	nmap -sT 192.168.100.11
Scan using TCP SYN (Stealth)	nmap -sS [Target]	nmap -sS 192.168.100.11
Scan UDP port	nmap -sU [Target]	nmap -sU 192.168.100.11

The **-sT** switch creates a full TCP handshake with the target. This is considered more accurate than SYN scan but is slower and can be easy detected by firewalls and IDS.

```
nmap -sT 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:18 W. Europe Daylight Time

Nmap scan report for 192.168.100.11
Host is up (1.0s latency).
Not shown: 986 closed ports
PORT     STATE    SERVICE
25/tcp   filtered smtp
53/tcp   open     domain
88/tcp   open     kerberos-sec
110/tcp  filtered pop3
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
389/tcp  open     ldap
```

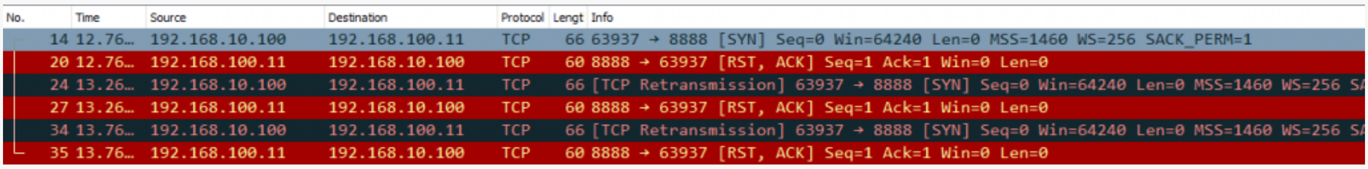
```
445/tcp  open     microsoft-ds
464/tcp  open     kpasswd5
593/tcp  open     http-rpc-epmap
636/tcp  open     ldapssl
3268/tcp open     globalcatLDAP
3269/tcp open     globalcatLDAPssl
3389/tcp open     ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 219.83 seconds
```

Analysing the scan in wireshark we can see that the open port is responding to the handshake.



No.	Time	Source	Destination	Protocol	Lengt	Info
13	12.76…	192.168.10.100	192.168.100.11	TCP	66	63936 → 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
18	12.76…	192.168.100.11	192.168.10.100	TCP	66	445 → 63936 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
19	12.76…	192.168.10.100	192.168.100.11	TCP	54	63936 → 445 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
21	12.77…	192.168.10.100	192.168.100.11	TCP	54	63936 → 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

If the port is closed on the host, then the target host will respond with a RST+ACK packets.



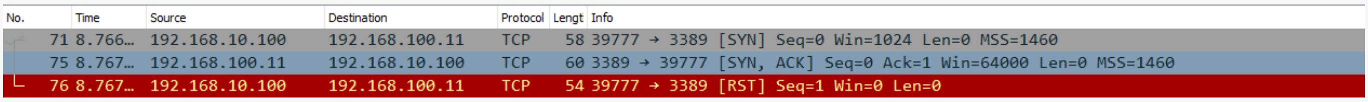
No.	Time	Source	Destination	Protocol	Lengt	Info
14	12.76…	192.168.10.100	192.168.100.11	TCP	66	63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	12.76…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.26…	192.168.10.100	192.168.100.11	TCP	66	[TCP Retransmission] 63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
27	13.26…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34	13.76…	192.168.10.100	192.168.100.11	TCP	66	[TCP Retransmission] 63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
35	13.76…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The **-sS** switch sends only a TCP SYN packet and waits for a TCP ACK. If it receives an ACK on the specific probed port then it response with a RST packet, in this way the scan can be undetected by the firewall. If the scanned port is closed on the target host, then target will only respond with a RST packet.

```
nmap -sS 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-26 21:24 W. Europe Daylight Time
Nmap scan report for 192.168.100.11

Host is up (0.0013s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
```

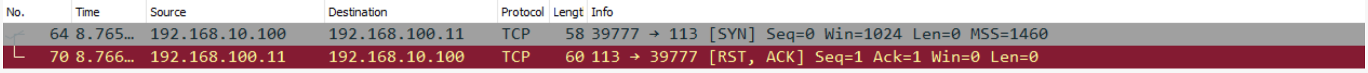
```
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.31 seconds
```

Analysing the packets in wireshark we can see that we first send a SYN packet to the scanned port on the target host, if it port is opened the target will response wit a SYN+ACK packet and we respond back with a RST packet.



No.	Time	Source	Destination	Protocol	Lengt	Info
71	8.766…	192.168.10.100	192.168.100.11	TCP	58	39777 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
75	8.767…	192.168.100.11	192.168.10.100	TCP	60	3389 → 39777 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
76	8.767…	192.168.10.100	192.168.100.11	TCP	54	39777 → 3389 [RST] Seq=1 Win=0 Len=0

If the port is closed on the scanned target the we will get a RST+ACK back.



No.	Time	Source	Destination	Protocol	Lengt	Info
64	8.765…	192.168.10.100	192.168.100.11	TCP	58	39777 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
70	8.766…	192.168.100.11	192.168.10.100	TCP	60	113 → 39777 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The **-sU** switch will scan after UDP ports, UDP is a connectionless protocol, UDP packets dose not have any ACK flag set, the UDP protocol don’t require the reviser to confirm that he revised a UDP packet.

If the there is a firewall enabled on the host or on the network you will get a response back “open|filtered ports” and a list of ports that are blocked by the firewall.

```
nmap -sU 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:58 W. Europe Daylight Time
```

```
Nmap scan report for 192.168.100.11
Host is up (0.0016s latency).
Not shown: 997 open|filtered ports
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
389/udp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 17.27 seconds
```

If the firewall is disabled then they will be no response back.

Inverse Scans

Description	Command	Example
Xmas scan	nmap -sX [Target]	nmap -sX 192.168.100.11
FIN scan	nmap -sF [Target]	nmap -sF 192.168.100.11
TCP Null scan	nmap -sN [Target]	nmap -sN 192.168.100.11
ACK scan	nmap -sA [Target]	nmap -sA 192.168.100.11

The **-sX** switch is called a Xmas Scan, when you scan a network or a target host with Xmax scan, the xmas scan sends a packet that contains multiple flags, the packet contains the URG, PSH & FIN flags. If the host have closed ports, it will respond with a single RST packet. If the ports are open on the host, then the host will respond as an open ports. Modern operating systems, firewalls and IDS drops this kind of packets if they are properly configured.

We will run the xmax scan against a windows server with firewall enabled.

```
nmap -sX 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:07 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are open|filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 27.62 seconds
```

Observe the line “All 1000 scanned ports on 192.168.100.11 are open|filtered” the output is showing that all scanned ports are “open|filtered”. This means that the firewall are enabled on the target host.

Lets try the same scan but this time we will disable the firewall on our target host.

```
nmap -sX 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:13 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.100.11 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.78 seconds
```

Now we get “All 1000 scanned ports on 192.168.100.11 are closed” this indicates that the firewall disabled.

The **-sF** switch scans the the host with a FIN scan, a FIN scan sends a packet with only the FIN flag set, this allows the packet to pass the firewall. If the port is open you will not get any respond, if the port is closed the target will respond with a RST packet.

When the firewall is enabled on the target the output will have a “open|filtered” response.

```
nmap -sF 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 17:51 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are open|filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 27.19 seconds
```

If the firewall is disabled on the target the output will have a “are closed” response.

```
nmap -sF 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 18:06 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.100.11 are closed

Nmap done: 1 IP address (1 host up) scanned in 6.29 seconds
```

The **-sN** switch will scan the target with a NULL scan, the scan sends a packet without any flags set. if the NULL packet is sent to an open port, the will be no response back. If the NULL packet is sent to a close port, it will respond with a RST packet. This type of scan is easy to detect due that there are no reason to send a TCP packet without a flag.

When using the NULL scan the target will respond similar to the FIN and Xmaz scans.

The **-sA** switch send a packet with the ACK flag set when scanning a host, when the target receive the ACK packet it will replay with a RST packet. if the port is closed and the firewall is enabled the firewall will block the target host response and there will be no response back.

Observe the output in namp when the firewall is enabled.

```
nmap -sA 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:36 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.100.11 are filtered
```

```
Nmap done: 1 IP address (1 host up) scanned in 27.58 seconds
```

If the firewall is enabled the “All 1000 scanned ports on 192.168.100.11 are filtered” line will comeback with the “**filtered**” value. The “filtered” response shows that a firewall is enabled in the system.

Running the same command against a target with a disabled firewall, the output will have a different value.

```
nmap -sA 192.168.100.11

Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-30 19:39 W. Europe Daylight Time
Nmap scan report for 192.168.100.11
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.100.11 are unfiltered

Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
```

The response back on the “All 1000 scanned ports on 192.168.100.11 are unfiltered” is coming back with the “unfiltered” value. The response back means that there are no firewall enabled on the target.

Firewall Evasion

Description	Command
Idle zombie scan	nmap -sI [zombie] [target]
Use a decoy	nmap -D RND: [number] [target]
Fragment packets	nmap -f [target]
Specify MTU	nmap –mtu [MTU] [target]
Randomize scan order	nmap –randomize-hosts [target]
Send bad checksums	nmap –badsum [target]
Specify source port	nmap –source-port [port] [target]

Description	Command
Spoof MAC Address	nmap –spoof-mac [MAC|0|vendor] [target]

The **-sI** is called a Idle scan or a zombie scan is a stealth technique, when using the a zombie scan packets revised on the scanned host cant be traced back the sender, all network traffic to the target host are going trough a second host on the network called “zombie”.

For a more detail explanation on how the idle scan work i recommend to read the official nmap documentation at https://nmap.org/book/idlescan.html

The **-f** switch is used to fragment probes into 8-byte packets, the scan will split the TCP header up to several packet, it is a very effective way to hide thee and make it harder for intrusion detection systems to the detect the scans.

The **-D** switch is used to hide port scans by using one or more decoys IP address,the network traffic on the scanned host will appear coming from the decoys IP address.

The **–source-port** switch is used to manually specify the source port number of a probe.

The **–-randomize-hosts** switch is used to randomize the scanning order of the specified ping sweap or a range scan.

Script Engines

Description	Command
Run script	nmap –script [script.nse] [target]
Run scripts	nmap –script [expression] [target
Run scripts by category	nmap –script [cat] [target]
Run multiple scripts categories	nmap –script [cat1,cat2,cat3] [target]

Description	Command
Update script database	nmap –script-updatedb
Script categories	all
	discovery
	default
	auth
	external
	malware
	vuln
	intrusive
	safe

Useful scans

Find Information about IP address

```
nmap --script=asn-query,whois,ip-geolocation-maxmind [target]
```

Detect Heart bleed SSL vulnerability

```
nmap -sV -p 443 --script=ssl-heartbleed [target]
```

Scan for DDOS reflection UDP services

```
nmap –sU –A –PN –n –pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-
```

```
sysdescr [target]
```

Scan HTTP Service

Get page titles

```
nmap --script=http-title [target]
```

Get HTTP headers

```
nmap --script=http-headers [target]
```

Recommended sites

https://highon.coffee/blog/nmap-cheat-sheet/

Conclusion

We have looked into some of the scanning techniques we can use with nmap.

Check out the Ethical Hacking notes for more Kali Linux quick guides.

How To Crack WPA/WPA2 Hash Using HashCat

How To Crack WPA/WPA2 With HashCat

The tutorial will illustrate how to install and configure HashCat on a Windows client and crack the captured PMKID or .hccap files using a wordlist dictionary attack.

“Hashcat is the self-proclaimed world’s fastest password recovery tool. It had a proprietary code base until 2015, but is now released as free software. Versions are available for Linux, OS X, and Windows and can come in CPU-based or GPU-based variants.”

The WPA2 handshake can be captured on a Linux compatible client like Kali Linux with a supported WiFi card running on VirtualBox. Then converted to the right format depending on the captured method and moved over to the Windows client to be cracked.

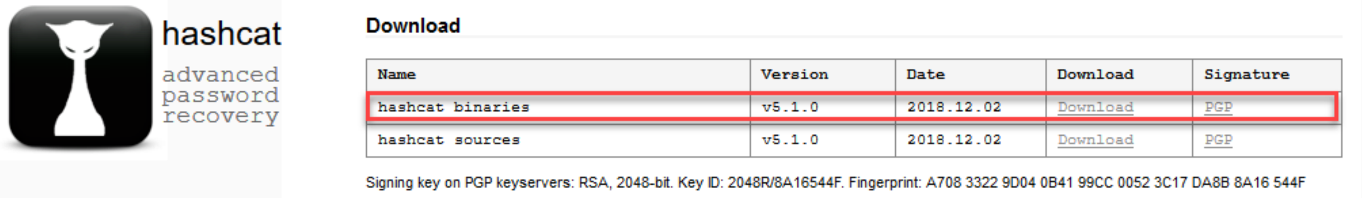
Use the guides Capturing WPA2 and Capturing WPA2 PMKID to capture the WPA2 handshake. For this test we will use the famous “Rockyou” wordlist.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.

Step 1: Download HashCat

Hashcat do not require any installation, it is a portable program it requires you to unpack the downloaded archive.

1. First you need to download Hashcat binaries from https://hashcat.net/hashcat/
2. Navigate to the location where you saved the downloaded file, and unzip the file



Download

Name	Version	Date	Download	Signature
hashcat binaries	v5.1.0	2018.12.02	Download	PGP
hashcat sources	v5.1.0	2018.12.02	Download	PGP

Signing key on PGP keyservers: RSA, 2048-bit. Key ID: 2048R/8A16544F. Fingerprint: A708 3322 9D04 0B41 99CC 0052 3C17 DA8B 8A16 544F

Step 2: Download Wordlist

They are numerous wordlists out on the web, for this test we are going to use the famous “rockyou”.

1. Open the hashcat folder on your hard drive and create a new folder called “wordlist”
2. Download the rockyou.txt wordlist from this Link.
3. Save the downloaded file in the new folder “wordlist”

Step 3: Prepare Your Captured WPA2 Handshake

Depending on the method you used to capture the handshake you either must format the cap file to 2500 hash-mode or the PMKID file to hashcat 16800 hash-mode .

For how to format the files please see the guides Capturing WPA2 and Capturing WPA2 PMKID.

In this lab we are using a captured PMKID and a pcpa handshake formatted to hashcat readable format. “HonnyP01.hccapx ” and ” HonnyP02.16800″.

I’m using two different home routers from D-Link and Technicolor for this experiment, both WiFi routers are owed by me.

- The “HonnyP01.hccapx” file is captured from the D-Link router.
- The ” HonnyP02.16800″ file is captured from the Technicolor router.

Step 4: Start Hashcat

You need to run hashcat in CMD or PowerShell. In this example we will use CMD to execute our commands and crack the handshake.

Open CMD and navigate to the hashcat folder.

```
C:\>cd hashcat-5.1.0
C:\hashcat-5.1.0>
```

Type hashcat64 -h to display all options

```
C:\hashcat-5.1.0>hashcat64 -h
```

```
 ===+============
  1 | CPU
  2 | GPU
  3 | FPGA, DSP, Co-Processor

- [ Workload Profiles ] -

  # | Performance | Runtime | Power Consumption | Desktop Impact
 ===+=============+=========+===================+=================
  1 | Low         |   2 ms  | Low               | Minimal
  2 | Default     |  12 ms  | Economic          | Noticeable
  3 | High        |  96 ms  | High              | Unresponsive
  4 | Nightmare   | 480 ms  | Insane            | Headless

- [ Basic Examples ] -

  Attack-          | Hash- |
  Mode             | Type  | Example command
==================+=======+==================================================
==========
  Wordlist         | $P$   | hashcat -a 0 -m 400 example400.hash example.dict
  Wordlist + Rules | MD5   | hashcat -a 0 -m 0 example0.hash example.dict -r
rules/best64.rule
  Brute-Force      | MD5   | hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a
  Combinator       | MD5   | hashcat -a 1 -m 0 example0.hash example.dict
example.dict

If you still have no idea what just happened, try the following pages:

* https://hashcat.net/wiki/#howtos_videos_papers_articles_etc_in_the_wild
* https://hashcat.net/faq/

C:\hashcat-5.1.0>
```

Step 5: Crack WPA2

In the First example we will illustrate how to get the password from a converted pcap file “.hccapx”.

Copy your converted file to the hashcat folder, in this example i am copying the file HonnyP01.hccapx to my hashcat folder.

Next we will start hashcat and use the wordlist rockyou, type in the parameters below in CMD.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 2500 the format type
- -w 3 workload-profile 3
- HonnyP01.hccapx the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

Hashcat will start processing the file, if you are successful the terminal will display the hash and the password.

```
Watchdog: Temperature abort trigger set to 90c

Dictionary cache hit:
* Filename..: wordlist\rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
```

Here we can see that hashcat was able to match the hash to a password in the wordlist, in this lab the password to the D-Link WiFi is “password”. You can chose to let the application run trough the wordlist or press “q” to quit.

```
Approaching final keyspace - workload adjusted.


Session..........: hashcat
```

```
Status...........: Cracked
Hash.Type........: WPA-EAPOL-PBKDF2
Hash.Target......: HonnyP01.hccapx
Time.Started.....: Fri Jan 18 20:13:27 2019 (42 secs)
Time.Estimated...: Fri Jan 18 20:14:09 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   230.7 kH/s (46.06ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 18/25 (72.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 14344384/14344384 (100.00%)
Rejected.........: 4734913/14344384 (33.01%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:24-49
Candidates.#1....: $HEX[303531313037353434] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 66c Fan: 44% Util: 97% Core:1949MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 20:13:12 2019
Stopped: Fri Jan 18 20:14:10 2019

C:\hashcat-5.1.0>
```

You can display the cracked password with the “show” command or by running the same command again, all cracked hashes will be stored in the “hashcat.potfile” in the hashcat folder.

To display the cracked password in CDM type the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
```

```
C:\hashcat-5.1.0>hashcat64 -m 2500 -w3 HonnyP01.hccapx "wordlist\rockyou.txt" --
show
7005312a9933d3a57065450f0749f210:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
2fed89e93e2cd63175f435db16ca75f0:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
fcaf4223879e125e10a272f9234256fe:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
7617ef601966436708eae3ad2c02d295:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
```

```
8b5ddfc6bade402e38e2ce023449bf07:84c9b26a9e90:f4bf80c7ec46:HonnyP01:password
C:\hashcat-5.1.0>
```

In the next example we will run the same command except now we use the 16800 mode to run the dictionary attack against formatted PMKID file captured from the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt"
```

- hashcat64 the binary
- -m 16800 the format type
- -w 3 workload-profile 3
- HonnyP02.16800 the formatted file
- “wordlist\rockyou.txt” the path to the wordlist

```
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c4988...47487a
Time.Started.....: Fri Jan 18 23:12:55 2019 (27 secs)
Time.Estimated...: Fri Jan 18 23:13:22 2019 (0 secs)
Guess.Base.......: File (wordlist\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   268.6 kH/s (51.75ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 11008839/14344384 (76.75%)
Rejected.........: 3636039/11008839 (33.03%)
Restore.Point....: 10261572/14344384 (71.54%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: aldohizo123 -> Juelle98
Hardware.Mon.#1..: Temp: 68c Fan: 43% Util: 95% Core:1847MHz Mem:4006MHz Bus:16

Started: Fri Jan 18 23:12:48 2019
Stopped: Fri Jan 18 23:13:24 2019
```

```
C:\hashcat-5.1.0>
```

Here we can see that the cracked password is “adsladsl” for the Technicolor router.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 "wordlist\rockyou.txt" --
show
17a40e5b92e3815f6111554b1c80f4d9*c4ea1d1f7d93*c498808d7d5f*4c656f6e20322e342047487a
:adsladsl

C:\hashcat-5.1.0>
```

Extra: Brute Force Attack And Rule based attack

You can let hashcat brute force the file with the command bellow.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 HonnyP02.16800 ?l?l?l?l?l?l?l?l
```

Or use ruled base attack.

```
C:\hashcat-5.1.0>hashcat64 -m 16800 -w 3 -r rules\best64.rule
"wordlist\rockyou.txt"
```

Conclusion

Your home or office WiFi can be hacked if you are using a weak password, as always a strong and complex password is still the best defense against an attacker.

DISCLAIMER: This software/tutorial is for educational purposes only. It should not be used for illegal activity. The author is not responsible for its use or the users action.