How To Scan a Network With Hping3

Hping3

Hping3 is a command-line oriented TCP/IP packet assembler and analyser and works like Nmap.

The application is able to send customizes TCP/IP packets and display the reply as ICMP echo packets, even more Hping3 supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features like DDOS flooding attacks.

Hping3 can be used to perform:

- OS fingerprinting
- ICMP pings
- Traceroute
- Port scanning

- Firewall testing
- Test IDSes
- Network testing and auditing
- MTU discovery
- Exploit and vulnerabilities discovery
- DDOS and ICMP flooding

Hping3 comes pre-installed with Kali Linux but and can also be installed on most Linux distros, also you need to run the commands with sudo privileges. Visit the official documentation at to learn more on how you can use Hping3
http://www.hping.org/documentation.php

Useful Options

-h	Show this help
-v	Show version
-c	Packet count
-i	–interval
	–flood
-V	Verbose mode
-D	Debugging
-f	Fragment packets
-Q	Display sequence number

-0	RAW IP mode
-1	ICMP mode
-2	UDP mode
-8	SCAN mode
-9	listen mode

-F	Set the FIN flag
-S	Set the SYN flag
-P	Set the PUSH flag

-A	Set the ACK flag
-U	Set the URG flag

Commands

Send a ACK packet to a target

```
hping3 –A 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): A set, 40 headers + 0 data bytes
len=46 ip=192.168.100.11 ttl=128 id=29627 sport=0 flags=R seq=0 win=32767 rtt=4.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29628 sport=0 flags=R seq=1 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29629 sport=0 flags=R seq=2 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29632 sport=0 flags=R seq=3 win=32767 rtt=2.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29633 sport=0 flags=R seq=4 win=32767 rtt=0.6
ms
len=46 ip=192.168.100.11 ttl=128 id=29634 sport=0 flags=R seq=5 win=32767 rtt=8.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29635 sport=0 flags=R seq=6 win=32767 rtt=7.1
ms
len=46 ip=192.168.100.11 ttl=128 id=29636 sport=0 flags=R seq=7 win=32767 rtt=7.0
ms
len=46 ip=192.168.100.11 ttl=128 id=29637 sport=0 flags=R seq=8 win=32767 rtt=5.0
ms
```

Use the -c option to decide on how many packets to send, in this example i am setting the count option to 5.

```
hping3 -A -c 5 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): A set, 40 headers + 0 data bytes
len=46 ip=192.168.100.11 ttl=128 id=30010 sport=0 flags=R seq=0 win=32767 rtt=7.9
ms
len=46 ip=192.168.100.11 ttl=128 id=30011 sport=0 flags=R seq=1 win=32767 rtt=7.0
ms
len=46 ip=192.168.100.11 ttl=128 id=30012 sport=0 flags=R seq=2 win=32767 rtt=7.6
ms
len=46 ip=192.168.100.11 ttl=128 id=30013 sport=0 flags=R seq=3 win=32767 rtt=5.1
ms
len=46 ip=192.168.100.11 ttl=128 id=30014 sport=0 flags=R seq=4 win=32767 rtt=4.0
ms

--- 192.168.100.11 hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.0/6.3/7.9 ms
```

Create a SYN packet and use the scan mode to scan port 1-1000 on a target.

```
hping3 -S -8 1-1000 192.168.100.11
```

```
Scanning 192.168.100.11 (192.168.100.11), port 1-1000
1000 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
   53 domain     : .S..A... 128 55677 64240    46
   88 kerberos   : .S..A... 128 55933 64240    46
  135 epmap      : .S..A... 128 56189 64240    46
  139 netbios-ssn: .S..A... 128 56445 64240    46
  389 ldap       : .S..A... 128 56701 64240    46
  445 microsoft-d: .S..A... 128 56957 64240    46
  464 kpasswd    : .S..A... 128 57213 64240    46
  593            : .S..A... 128 52863 64240    46
  636 ldaps      : .S..A... 128 53375 64240    46
All replies received. Done.
Not responding ports: (199 smux) (202 at-nbp) (203 ) (204 at-echo) (299 ) (300 )
(301 ) (306 ) (307 ) (308 ) (309 ) (312 ) (313 ) (407 ) (500 isakmp) (514 shell)
(723 ) (729 ) (743 ) (761 ) (763 ) (764 ) (766 ) (767 ) (768 ) (769 ) (772 ) (782 )
(783 spamd) (784 ) (790 ) (791 ) (793 ) (794 ) (798 ) (799 ) (802 ) (803 ) (804 )
```

```
(805 ) (808 omirr) (809 ) (810 ) (811 ) (812 ) (813 ) (817 ) (818 ) (819 ) (820 )
(821 ) (822 ) (823 ) (824 ) (825 ) (827 ) (828 ) (829 ) (831 ) (832 ) (833 ) (834 )
(836 ) (837 ) (838 ) (839 ) (840 ) (841 ) (842 ) (843 ) (844 ) (845 ) (846 ) (847 )
(848 ) (849 ) (854 ) (855 ) (858 ) (878 ) (879 ) (880 ) (881 ) (911 ) (912 ) (913 )
(918 )
root@iPhone:~#
```

Send a UDP scan mode to send UDP request on port 80 to a target, if the UDP port is open then you will get a respond back, great to use when the target have blocked ICMP ping.

```
hping3 -2 192.168.100.17 -c 2 -p 80
```

Create a ping packet and use the ICMP mode.

```
hping3 -1 -c 4 192.168.100.11
```

```
HPING 192.168.100.11 (eth0 192.168.100.11): icmp mode set, 28 headers + 0 data
bytes
len=46 ip=192.168.100.11 ttl=128 id=34163 icmp_seq=0 rtt=8.1 ms
len=46 ip=192.168.100.11 ttl=128 id=34164 icmp_seq=1 rtt=5.9 ms
len=46 ip=192.168.100.11 ttl=128 id=34167 icmp_seq=2 rtt=4.0 ms
len=46 ip=192.168.100.11 ttl=128 id=34168 icmp_seq=3 rtt=3.0 ms

--- 192.168.100.11 hping statistic ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 3.0/5.2/8.1 ms
root@iPhone:~#
```

Traceroute to a target using ICM mode and show verbose.

```
hping3 --traceroute -V -1 192.168.100.11
```

```
using eth0, addr: 172.168.200.110, MTU: 1500
HPING google.com (eth0 216.58.211.142): icmp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.168.200.2 name=_gateway
hop=1 hoprtt=3.9 ms
hop=2 TTL 0 during transit from ip=192.168.10.1 name=UNKNOWN
hop=2 hoprtt=2.0 ms
hop=3 TTL 0 during transit from ip=10.33.221.74 name=UNKNOWN
hop=3 hoprtt=8.9 ms
hop=4 TTL 0 during transit from ip=88.129.174.18 name=gbg1.dr8.a3network.se
hop=4 hoprtt=8.9 ms
hop=5 TTL 0 during transit from ip=88.129.128.62 name=gbg1.a7network.se
hop=5 hoprtt=8.0 ms
hop=6 TTL 0 during transit from ip=85.8.9.16 name=gbg1.cr1.a3network.se
hop=6 hoprtt=6.9 ms
hop=7 TTL 0 during transit from ip=85.8.10.20 name=sto2.cr1.a3network.se
```

Traceroute to determined if port 443 is open, set that local traffic is generated from source port 8080

```
hping3 --traceroute -V -S -p 443 -s 8080 google.com
```

```
using eth0, addr: 172.168.200.110, MTU: 1500
HPING google.com (eth0 216.58.211.142): S set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.168.200.2 name=_gateway
hop=1 hoprtt=8.9 ms
len=46 ip=216.58.211.142 ttl=128 id=34374 tos=0 iplen=44
sport=443 flags=SA seq=8 win=64240 rtt=13.8 ms
seq=905581660 ack=1390210946 sum=3cce urp=0

len=46 ip=216.58.211.142 ttl=128 id=34376 tos=0 iplen=44
sport=443 flags=SA seq=9 win=64240 rtt=13.9 ms
seq=277232268 ack=486133387 sum=5a24 urp=0

len=46 ip=216.58.211.142 ttl=128 id=34377 tos=0 iplen=44
```

```
sport=443 flags=SA seq=10 win=64240 rtt=13.0 ms
seq=1939483389 ack=2029365982 sum=8498 urp=0

len=46 ip=216.58.211.142 ttl=128 id=34378 tos=0 iplen=44
sport=443 flags=SA seq=11 win=64240 rtt=12.9 ms
seq=90127368 ack=1561834414 sum=c208 urp=0
```

Use the TTL in tracerout to check load balancing devices IP address.

```
hping3 -S 192.168.100.100 -p 80 -T --ttl 13 --tr-keep-ttl -n
```

Ping a subnet and don’t scan in order, instead randomize the scan. Use the –rand-dest and the interface -I eth0 operators.

```
hping3 -1 192.168.100.x --rand-dest -I eth0
```

Send a ICMP packet to request a timestamp from a target, if the target have the ICMP responses blocked it wont respond to ICMP packets however it might allow response to timestamp request.

```
hping3 -1 192.168.100.17 --icmp-ts -c 3
```

Malicious Commands

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, always perform the attacks on your own lab system.

Common used parameters.

- The –flood parameter, activates the fastest packet sending mode
- The -p “destport” parameter, specifies the destination port
- The –spoof parameter, specifies which IP address to be spoofed
- The -rand-source parameter, activates a random source address
- The –interface parameter, used to specify interface

Main attack flags.

- The -S parameter sets the SYN flag
- The -A parameter sets the ACK flag
- The -F parameter sets the FIN flag
- The -R parameter sets the RESET flag
- The -P parameter sets the PUSH flag
- The -U parameter sets the URGENT flag

To start a SYN flood attack run the command bellow

NOTE: When running the commands hping3 will ***not*** show any output, it is working in the background.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S
```

Use hping3 to run a SYN flood attack with a inactive spoofed IP address from the network.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S --spoof [INACTIVE_IP]
```

SYN flood attack with with random source IP address.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -S --rand-source
```

ACK flood attack.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -A
```

FIN flood attack.

```
hping3 --flood -p [DST_PORT] [VICTIM_IP] -F
```

Conclusion

In this lab we have covered the basic commands you can do in hping3, we assembled TCP and UDP packets and used them to scan networks and discovered devices, as always when doing this kind of scans make sore you are authorized to scan the network and devices you are scanning.

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
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

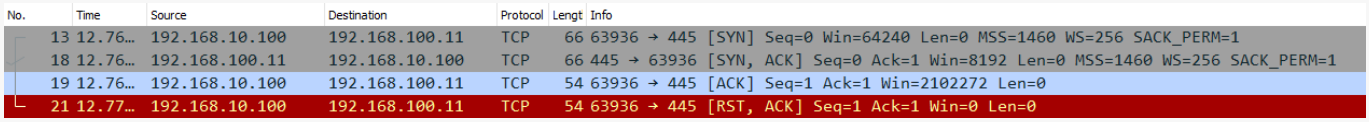
Description	Command	Example
Scan a single Port	nmap -p [Port] [Target]	nmap -p 80 192.168.100.11
Scan a range of ports	nmap -p [Port-Port] [Target]	nmap -p 20-99 192.168.100.11
Scan the first 100 ports	nmap -F [Port] [Target]	nmap -F 192.168.100.11
Scan using TCP Handshake	nmap -sT [Target]	nmap -sT 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
```

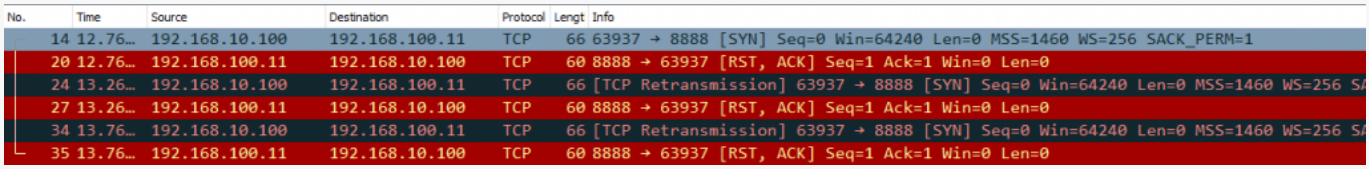
```
Nmap done: 1 IP address (1 host up) scanned in 219.83 seconds
```

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.



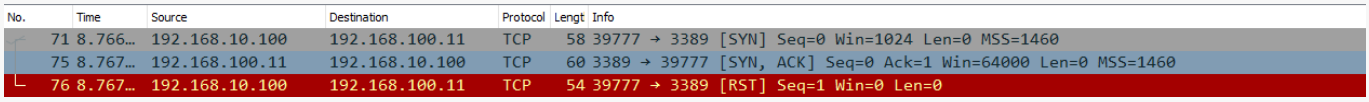
No.	Time	Source	Destination	Protocol	Lengt	Info
14	12.76…	192.168.10.100	192.168.100.11	TCP	66	63937 → 8888 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
20	12.76…	192.168.100.11	192.168.10.100	TCP	60	8888 → 63937 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	13.26…	192.168.10.100	192.168.100.11	TCP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

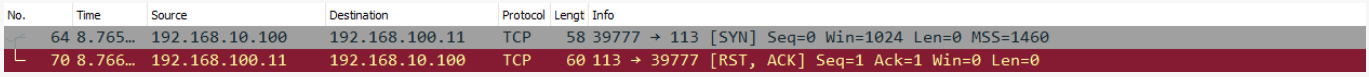
```
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

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]
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]
Update script database	nmap –script-updatedb
Script categories	all
	discovery
	default
	auth
	external
	malware

Description	Command
	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.

Footprinting and Reconnaissance

Footprinting and Reconnaissance

Footprinting is the process of using various tools and techniques to understand and learn the targets infrastructure and vulnerabilities.

In the initial phase we wan to find out as much as possible from gathering information that is publicly available without actually interacting with the scanned target. This kind of attack can be passive or pseudonymous.

Here are some of the of information you can gathered about a target during footprinting.

- Websites
- Alternative Websites
- Domain names
- Network blocks
- Specific IP addresses
- Network services and applications
- System architecture

- Authentication mechanisms
- Access control mechanisms
- Employee email & Phone numbers
- Contact addresses

In this lab we will use tools like ping, tracert and search engines to obtain information about a our target.

lets start with the basic ping command. In this lab series i will use www.hackthissite.org to try out my attacks.

“Hack This Site is a free training ground for users to test and expand their hacking skills. Our community is dedicated to facilitating an open learning environment by providing a series of hacking challenges, articles, resources, and discussion of the latest happenings in hacker culture. We are an online movement of artists, activists, hackers and anarchists who are organizing to create new worlds.”

Open CMD and ping a your favorite site, i am pinging www.hackthissite.org

```
C:\>ping www.hackthissite.org

Pinging www.hackthissite.org [137.74.187.102] with 32 bytes of data:
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45
Reply from 137.74.187.102: bytes=32 time=40ms TTL=45

Ping statistics for 137.74.187.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 40ms, Average = 40ms

C:\>
```

We can see that the site replied with its IP address which is 137.74.187.102.

Now when we have the IP address we can use tracert to see the path the trafic is taking from your client to www.hackthissite.org

```
C:\>tracert 137.74.187.102

Tracing route to hackthissite.org [137.74.187.102]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.10.1
  2     1 ms     1 ms     1 ms  h85-209-118-1.cust.a3fiber.se [85.209.118.1]
  3     1 ms     1 ms     1 ms  gsl-bbr-1-be102.net.comhem.se [213.200.167.80]
  4     4 ms     9 ms     6 ms  gbg1.dr2.a3network.se [88.129.174.24]
  5     1 ms     1 ms     1 ms  gbg1.a3network.se [88.129.128.62]
  6     1 ms     1 ms     1 ms  gbg1.cr1.a3network.se [85.8.9.16]
  7     7 ms     7 ms     7 ms  sto2.cr1.a3network.se [85.8.10.20]
  8    29 ms    18 ms    18 ms  s-b10-link.telia.net [213.248.93.188]
  9    18 ms    17 ms    19 ms  s-bb4-link.telia.net [62.115.119.80]
 10    33 ms    33 ms    33 ms  ffm-bb4-link.telia.net [62.115.138.105]
 11    34 ms    51 ms    30 ms  ffm-b1-link.telia.net [62.115.137.169]
 12    39 ms    39 ms    39 ms  be100-163.fra-5-a9.de.eu [178.33.100.250]
 13   222 ms    44 ms    45 ms  be103.rbx-g2-nc5.fr.eu [94.23.122.240]
 14     *        *        *     Request timed out.
 15     *       40 ms     *     vl7.vss-10b-6k.fr.eu [178.33.100.218]
 16    40 ms    40 ms    40 ms  hackthissite.org [137.74.187.102]

Trace complete.

C:\>
```

With the tracert command we can fallow the trafic trough all routers and firewalls until we arrive to the website.

Use www.netcraft.com To Obtain More Data

Open www.netcraft.com in your web browser, In the right menu under “What’s that site running?” enter www.hackthissite.org the result page will open. Here we can see all the subdomains the site have.

Results for hackthissite.org

Found 4 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.hackthissite.org		october 2003	sharktech	freebsd
2.	hackthissite.org		september 2007	sharktech	unknown
3.	radio.hackthissite.org		august 2011	sharktech	freebsd
4.	mirror.hackthissite.org		august 2011	ovh static ip	freebsd

On the result page click on the site report next to the domain name, a new page will load with information like email address, physical addresses, OS versions, Web Server version and a lot more.

Use WHOIS to obtain domain name information

WHOIS is a database that have information about domains and information about the people that own them. Using this tool give you the potential to gather personal information about the people that you can later use when doing social engineering. As well as collecting information as:

- Information about the owner
- Contact information
- Location
- Domain name servers
- The IP address
- The date of created

There several ways to use “WHOIS” like online services, applications and from command line, use the method that you are that you are comfortable with. If you are using a windows client then you need to download WHOIS, there is no need to install anything if you are using Kali Linux.

In this example we will show you how to use WHOIS from windows command line. Download WHOIS from Microsoft from https://docs.microsoft.com/en-us/sysinternals/downloads/whois and extract the files to the C:\ drive root.

Open CMD and type in whois [-v] domainname [whois.server]

```
C:\>whois -v hackthissite.org

Whois v1.20 - Domain information lookup
Copyright (C) 2005-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to ORG.whois-servers.net...
Server ORG.whois-servers.net returned the following for HACKTHISSITE.ORG

Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2019-01-14T03:31:05Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2019-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registrant Organization: Whois Privacy Protection Service, Inc.
Registrant State/Province: WA
Registrant Country: US
Name Server: C.NS.BUDDYNS.COM
Name Server: F.NS.BUDDYNS.COM
Name Server: G.NS.BUDDYNS.COM
Name Server: H.NS.BUDDYNS.COM
Name Server: J.NS.BUDDYNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-02-09T22:32:34Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Use internet archives to get old versions of websites

“The Internet Archive, a 501(c)(3) non-profit, is building a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, the print disabled, and the general

public”

Use internet archives like the wayback machine to get old versions of sites and check if you can find vulnerabilities or if you can extract other useful information from old versions of the site.

Use Google Hacking

Google hacking is an information gathering technique that uses Google search queries to identify vulnerabilities in web applications, gather information of individual targets, discover errors, disclosing sensitive data, discover credentials and other sensitive information.For more information on google hacking scripts please search https://www.exploit-db.com

The cache operator finds the recent cache value of a website.

```
cache:www.hackthissite.org
```

The link operator lists pages linking to a specific domain or URL.

```
link:www.hackthissite.org
```

The info operator displays information about a page.

```
info:www.hackthissite.org
```

The site operator restricts the search to a specific site.

```
site:www.hackthissite.org
```

The allinurl operator only returns specified keyword in URL.

```
allinurl:network camera
```

The allintitle operator returns specified keyword in title.

```
allintitle:online-it.nu
```

Website gathering tools

There are many tools one can use to extract and gather information from the targets websites. Below are some examples of browsers plugins and applications that you can use.

- Web Data Extractor 8.3 Link
- Firebug plugin for Chrome
- HTTrack Website Copier For Windows Link

Gathering information from DNS

If the target have some kind of public facing server then they will have some kind of a DNS servers, we can use DNS to gather information about email servers and other servers that the target is utilizing by analyzing the record types of the DNS server. List of DNS records typs.

There are many tools online and offline you can use to gather information about DNS, in this example we are using nslookup, to use nslookup open command line in windows or

shell in linux and type in nslookup and the FQDN or the IP address of the target.

Below are some examples of DNS query’s.

```
# Check DNS A record
C:\>nslookup
Default Server:  8.8.8.8
Address:  8.8.8.8

> set type=a
> www.google.se
Server:  8.8.8.8
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.se
Address:  216.58.207.227
```

```
# Check DNS mx record
C:\>nslookup
Default Server:  8.8.8.8
Address:  8.8.8.8

> set type=mx
> live.se
Server:  8.8.8.8
Address:  8.8.8.8

Non-authoritative answer:
live.se MX preference = 10, mail exchanger = eur.olc.protection.outlook.com

eur.olc.protection.outlook.com  internet address = 104.47.126.33
eur.olc.protection.outlook.com  internet address = 104.47.124.33
```

We have looked at the basic tools you can utility’s when footprinting a target, we have looked on how to find information of a target without interacting whit the target.

The are allot of tools you can use under the footprinting phase, as always google is your best friend, there is tons of information out there.

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