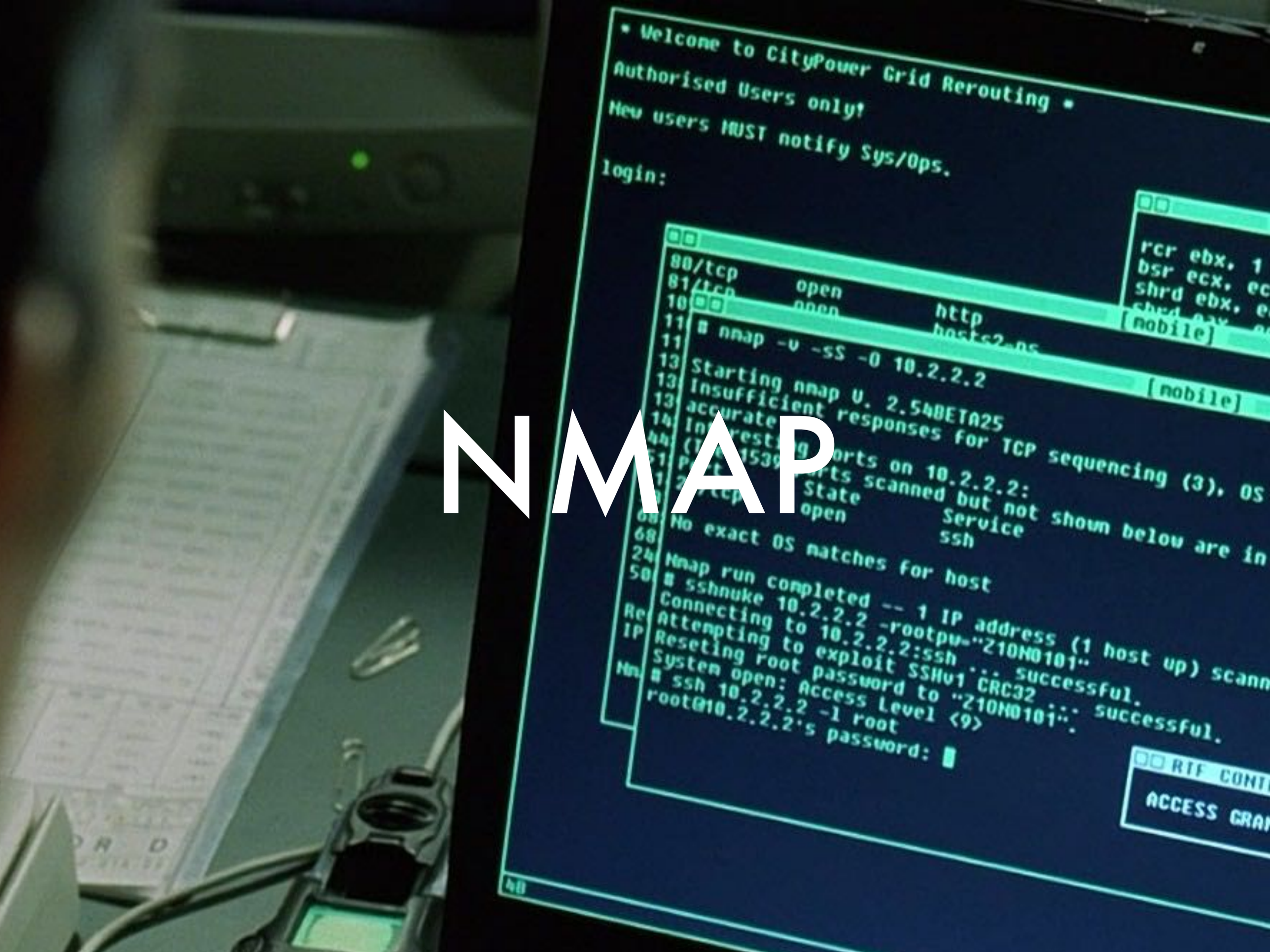
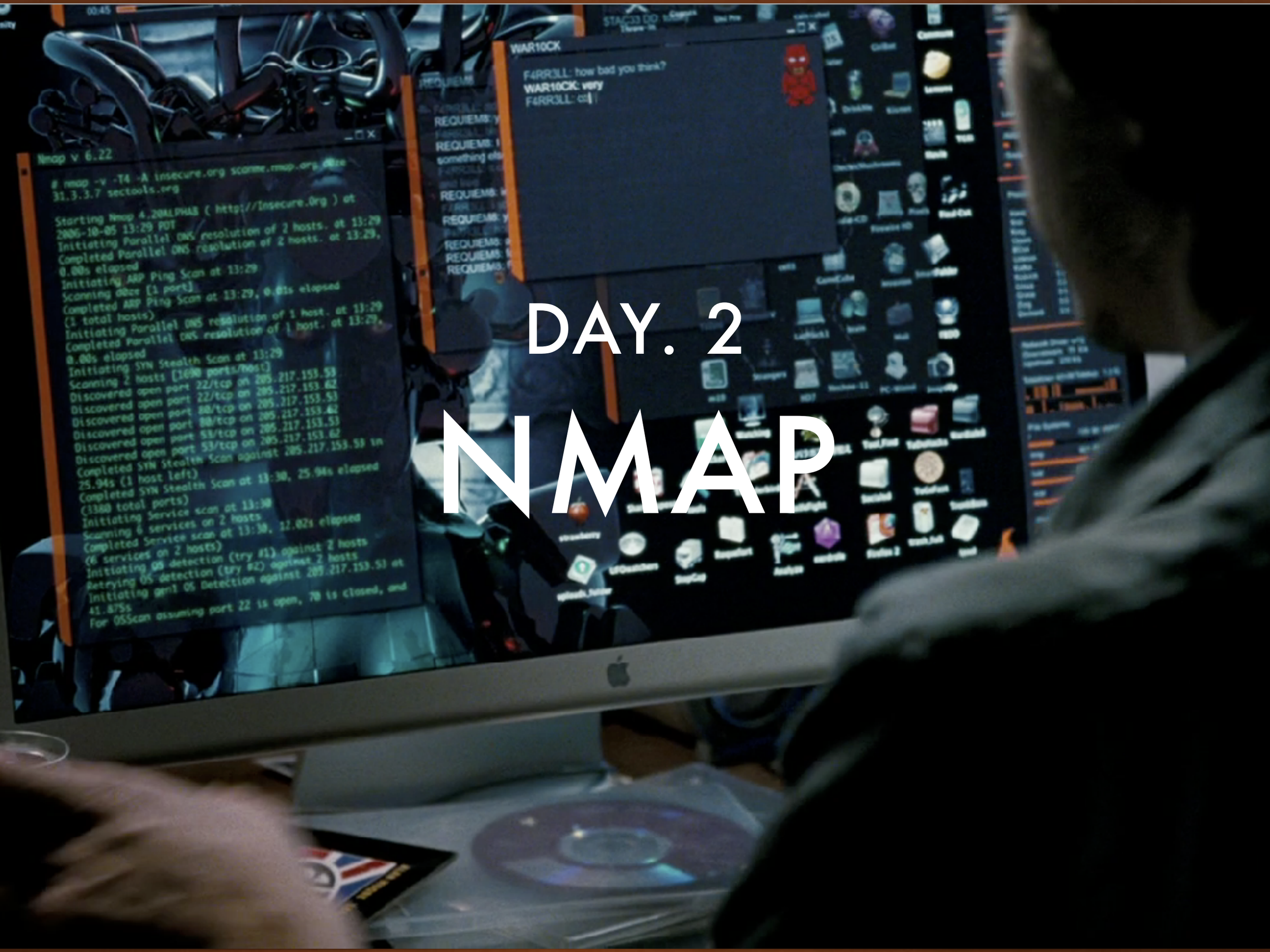

* Welcome to CityPower Grid Rerouting *
Authorised Users only!
New users MUST notify Sys/Ops.
login:
80/tcp open http
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS
accurate
Interesting ports on 10.2.2.2:
State Service
open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scann
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32
Reseting root password to "Z1ON0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
ACCESS GRAN

NMAP


WAR10CK
F4RR3LL: how bad you think?
WAR10CK: very
F4RR3LL:
Nmap v 6.22
DAY. 2
NMAP

AGENDA DAY 2

- Advanced Scanning Options
  - Firewall/ IDS Evasion and spoofing
  - Timing and Performance Options
    - IPv6 Scanning
- Output Options
- Debugging and Troubleshooting

FIREWALL/IDS EVASION AND SPOOFING

NMAP ADVANCED OPTIONS

FIREWALL/IDS EVASION

- Firewall, IDS/IPS can make mapping a network exceedingly difficult.
- Nmap offers many features to help understand these complex networks, and to verify that filters are working as intended. It even supports mechanisms for bypassing poorly implemented defenses.
- Launch an FTP bounce scan, idle scan, fragmentation attack, or try to tunnel through one of your own proxies.

FIREWALL/IDS EVASION

WINDOWS FIREWALL VS ZONE ALARM

```
root@kali:~# nmap  192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 00:01 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 00:01 (0:00:00 remaining)
Nmap scan report for 192.168.2.103
Host is up (0.036s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 40.75 seconds
root@kali:~# nmap  192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 00:01 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.2.103 are filtered
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 34.42 seconds
root@kali:~#
```

PORT SCANNING TECHNIQUES

TCP NULL, FIN, AND XMAS SCANS

- -sN; -sF; -sX (TCP NULL, FIN, and Xmas scans)
- These three scan types (even more are possible with the --scanflags option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between open and closed ports.
- When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK.

PORT SCANNING TECHNIQUES

TCP ACK SCAN

- -sA (TCP ACK scan)
- This scan is different than the others discussed so far in that it never determines open (or even openlfiltered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

PORT SCANNING TECHNIQUES

TCP ACK SCAN

```
bash-3.2# nmap -sA -Pn 192.168.176.226

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 21:41 WIB
Nmap scan report for 192.168.176.226
Host is up (0.00010s latency).
All 1000 scanned ports on 192.168.176.226 are unfiltered
MAC Address: 00:0C:29:BA:E6:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.24 seconds
bash-3.2#
```

PORT SCANNING TECHNIQUES

FTP BOUNCE SCAN

- -b FTP relay host (FTP bounce scan) .
- This scan is different than the others discussed so far in that it never determines open (or even openlfiltered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.
- The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

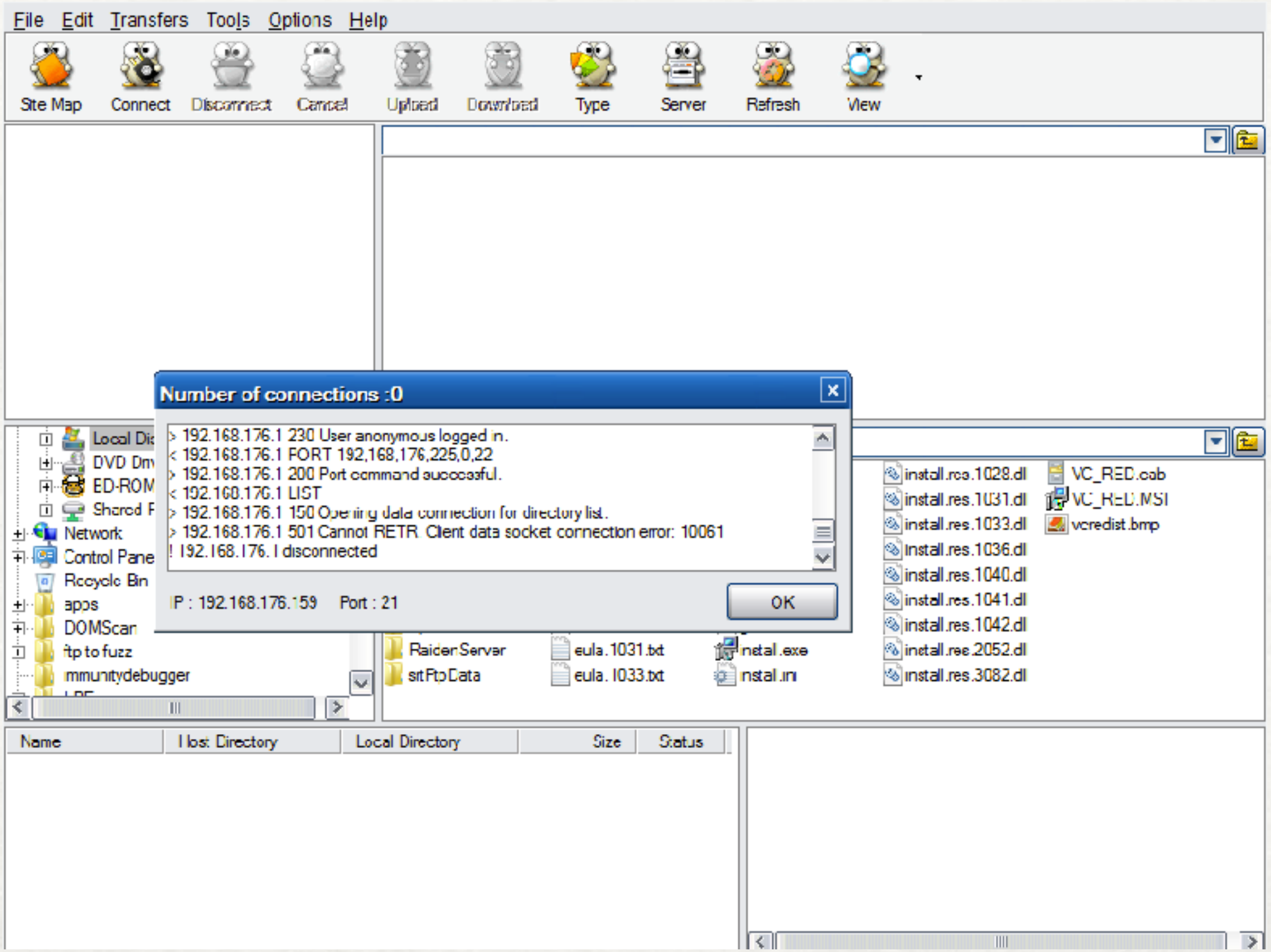
BASIC SCANNING

PORT SCANNING TECHNIQUES

```
bash-3.2# nmap -Pn -p21 -b anonymous:test@192.168.176.159 127.0.0.1

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 17:27 WIB
Nmap scan report for raiser (127.0.0.1)
Host is up.
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds
bash-3.2# nmap -Pn -p22 -b anonymous:test@192.168.176.159 192.168.176.225

Starting Nmap 7.00 ( https://nmap.org ) at 2016-07-27 17:27 WIB
Nmap scan report for 192.168.176.225
Host is up.
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 10.13 seconds
bash-3.2#
```

BASIC SCANNING

PORT SCANNING TECHNIQUES



FIREWALL/IDS EVASION

FRAGMENT PACKETS

- -f : fragment packets

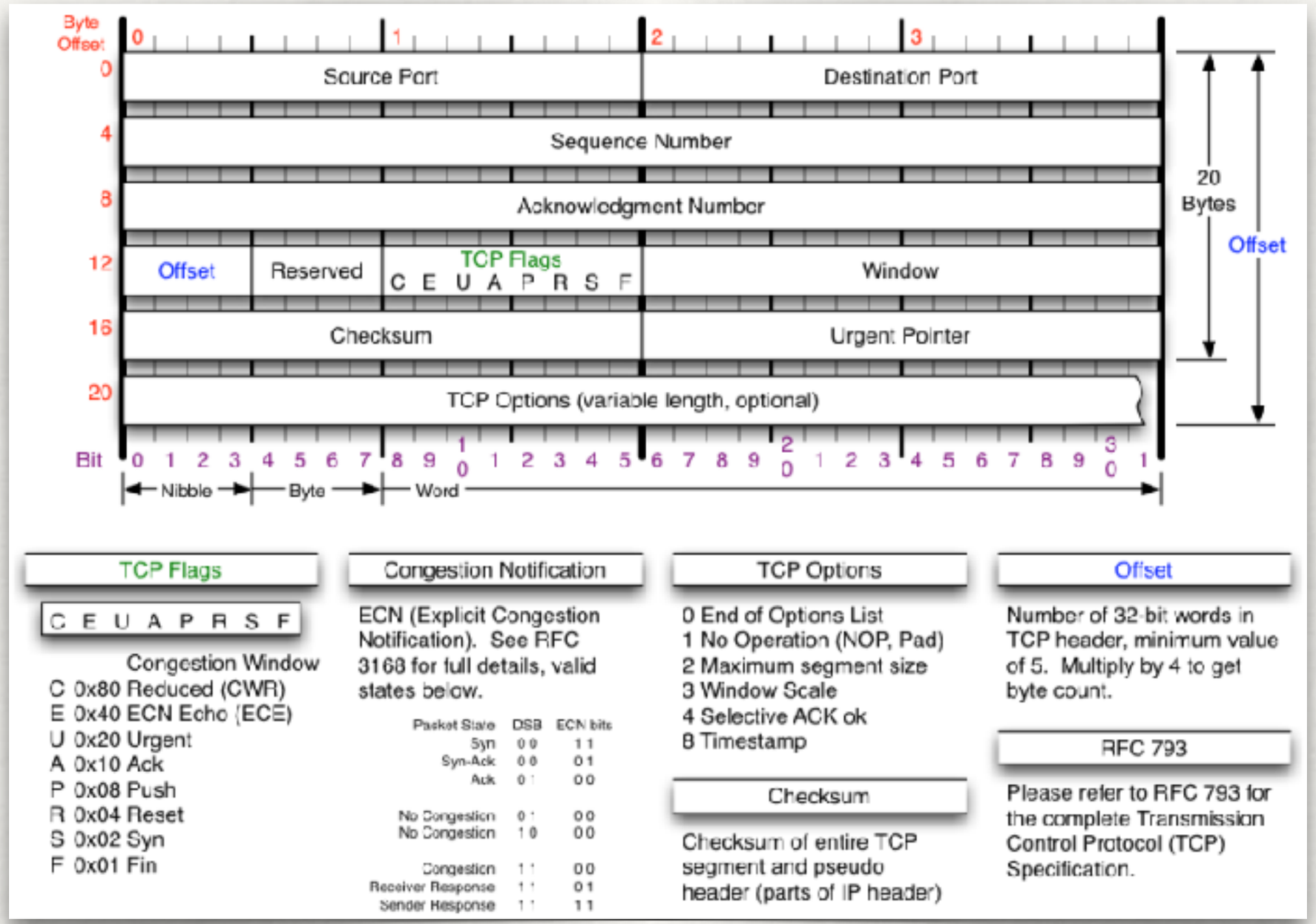
The -f option causes the requested scan (including ping scans) to use tiny fragmented IP packets.

The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing.

Specify this option once, and Nmap splits the packets into eight bytes or less after the IP header. So a 20-byte TCP header would be split into three packets. Two with eight bytes of the TCP header, and one with the final four. Of course each fragment also has an IP header.

FIREWALL/IDS EVASION

FRAGMENT PACKETS



FIREWALL/IDS EVASION

FRAGMENT PACKETS

```
root@kali:~# nmap -PS -p135 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-05 23:26 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00063s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds
root@kali:~# nmap -f -PS -p135 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-05 23:27 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00073s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
root@kali:~#
```

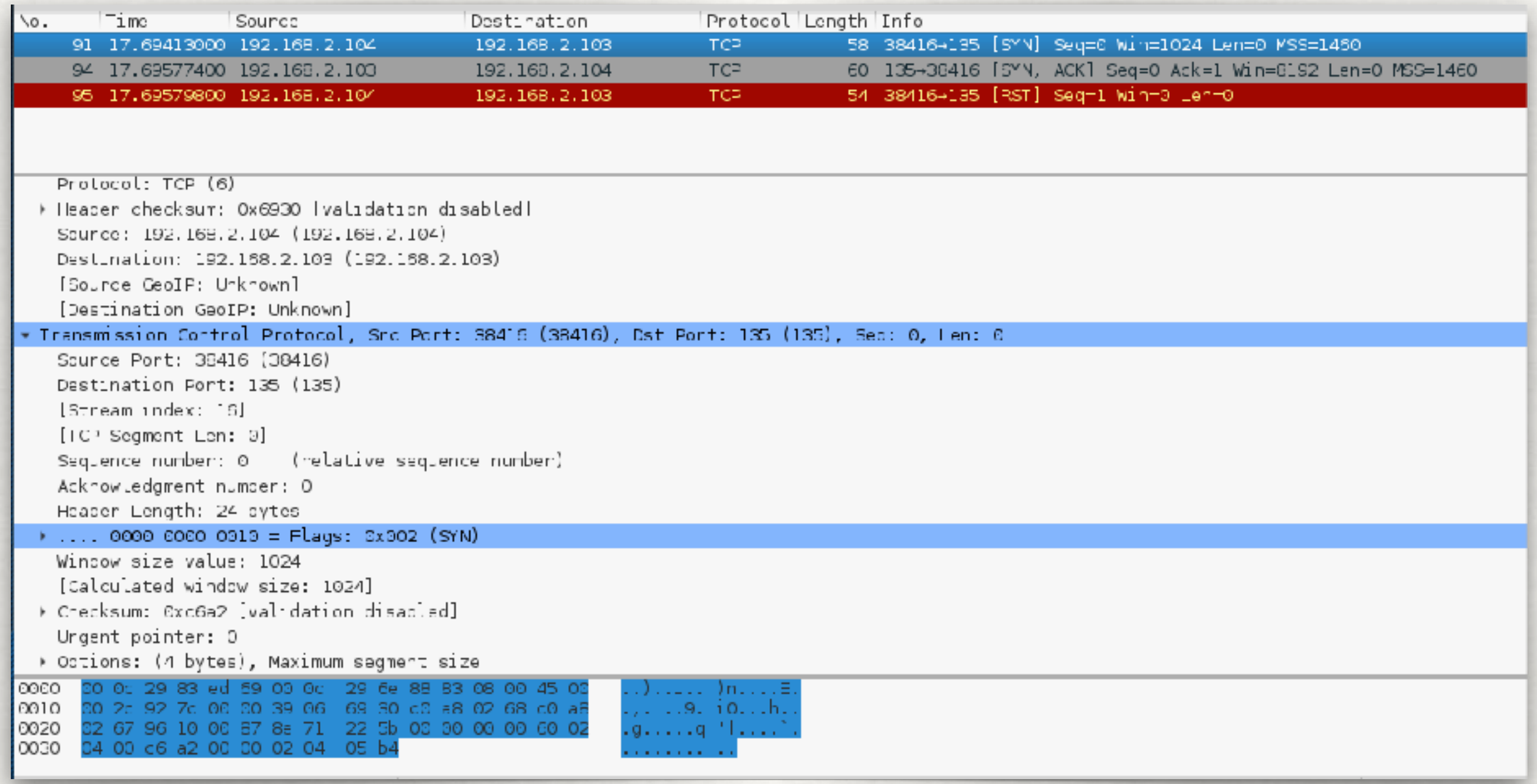
FIREWALL/IDS EVASION

FRAGMENT PACKETS

- Install Wireshark
- Copy VM

FIREWALL/IDS EVASION

WIRESHARK CAPTURE



FIREWALL/IDS EVASION

WIRESHARK CAPTURE

No.	Time	Source	Destination	Protocol	Length	Info
9	4.253785000	192.168.2.104	192.168.2.108	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=0, ID=dbae) [Reassembled in #1
10	4.254017000	192.168.2.104	192.168.2.108	IPv4	42	Fragmented IP protocol (proto=TCP 6, off=8, ID=dbae) [Reassembled in #1
11	4.254215000	192.168.2.104	192.168.2.108	TCP	42	61811→135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	4.255509000	192.168.2.108	192.168.2.104	TCP	60	135→61811 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
15	4.255536000	192.168.2.104	192.168.2.108	TCP	54	61811→135 [RST] Seq=1 Win=0 Len=0

```
    [Destination GeoIP: Unknown]
  ▸ [3 IPv4 Fragments (24 bytes): #9(8), #10(8), #11(8)]
▾ Transmission Control Protocol, Src Port: 61811 (61811), Dst Port: 135 (135), Seq: 0, Len: 0
    Source Port: 61811 (61811)
    Destination Port: 135 (135)
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 0
    Header Length: 24 bytes
  ▸ .... 0000 0000 0010 = Flags: 0x002 (SYN)
    Window size value: 1024
    [Calculated window size: 1024]
  ▸ Checksum: 0x0664 [validation disabled]
    Urgent pointer: 0
  ▸ Options: (4 bytes), Maximum segment size
```

```
0000  00 0c 29 83 ed 69 00 0c  29 6e 88 83 08 00 45 00   ..)..i.. )n....E.
0010  00 1c db ae 00 02 25 06  3e 0c c0 a8 02 68 c0 a8   ......%. >....h..
0020  02 67 f1 73 00 87 02 94  05 b4                     .g.s.... ..
```

FIREWALL/IDS EVASION

FRAGMENT PACKETS

--mtu (using the specified Maximum Transmission Unit)

Or you can specify your own offset size with the --mtu option.

Don't also specify -f if you use —mtu.

If your host OS is causing problems, try the **--send-eth** option to bypass the IP layer and send raw ethernet frames.

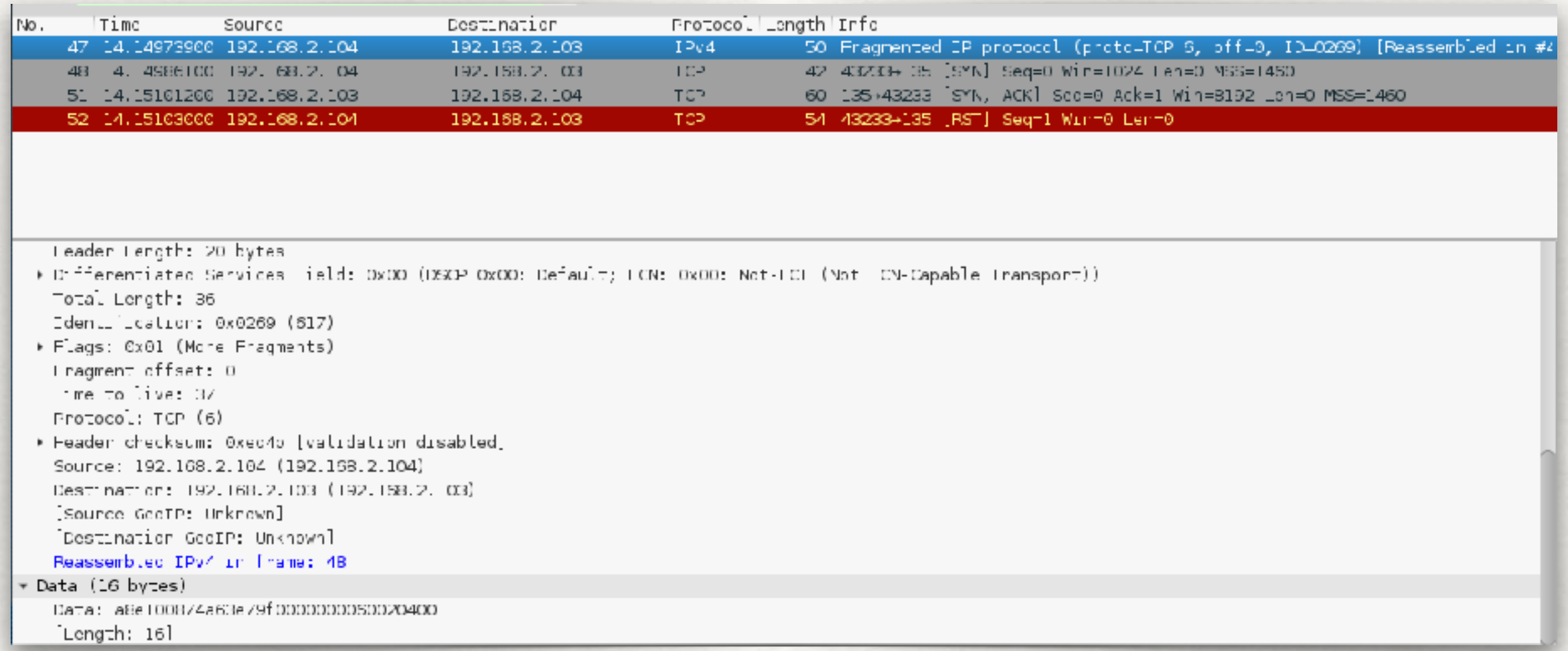
FIREWALL/IDS EVASION

FRAGMENT PACKETS

```
root@kali:~# nmap --mtu 16 -PS -p135 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-05 23:48 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00096s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE



FIREWALL/IDS EVASION

NMAP

- Fragmentation is only supported for Nmap's raw packet features, which includes TCP and UDP port scans (except connect scan and FTP bounce scan) and OS detection. Features such as version detection and the Nmap Scripting Engine generally don't support fragmentation because they rely on your host's TCP stack to communicate with target services.

FIREWALL/IDS EVASION

DECOY

- -D <decoy1>[,<decoy2>][,ME][,...] (Cloak a scan with decoys)

Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too.

It is generally an effective technique for hiding your IP address.

Thus their IDS might report 5–10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys.

You can also use RND to generate a random, non-reserved IP address, or RND:<number> to generate <number> addresses.

FIREWALL/IDS EVASION

DECOY

- Decoys are used in the initial ping scan (using ICMP, SYN, ACK, or whatever), during the actual port scanning phase and also used during remote OS detection (-O).
- Decoys do not work with version detection or TCP connect scan
- Using too many decoys may slow your scan and potentially even make it less accurate. Also, some ISPs will filter out your spoofed packets, but many do not restrict spoofed IP packets at all.

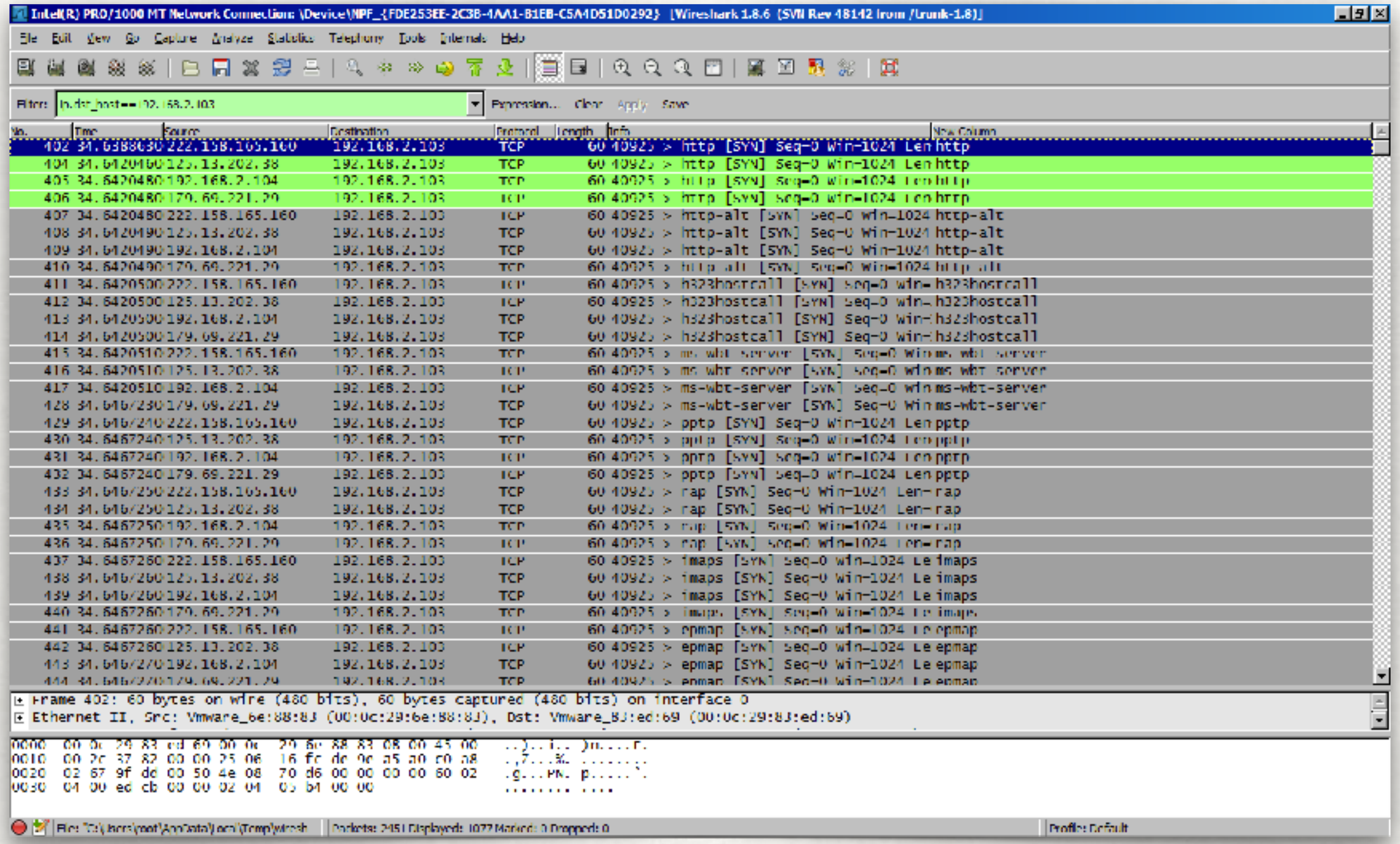
FIREWALL/IDS EVASION

DECOY SCANS

```
root@kali:~# nmap -D RND:3 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 00:18 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0058s latency).
Not shown: 985 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.25 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE



FIREWALL/IDS EVASION

DECOY

This can be defeated through router path tracing, response-dropping, and other active mechanisms.

Note that the hosts you use as decoys should be up or you might accidentally SYN flood your targets. Also it will be pretty easy to determine which host is scanning if only one is actually up on the network.

Use IP addresses instead of names (so the decoy networks don't see you in their nameserver logs).

FIREWALL/IDS EVASION

SPOOF SOURCE ADDRESS

- -S <IP_Address> (Spoof source address)

In some circumstances, Nmap may not be able to determine your source address (Nmap will tell you if this is the case). In this situation, use -S with the IP address of the interface you wish to send packets through.

Another possible use of this flag is to spoof the scan to make the targets think that someone else is scanning them

The -e option and -Pn are generally required for this sort of usage.

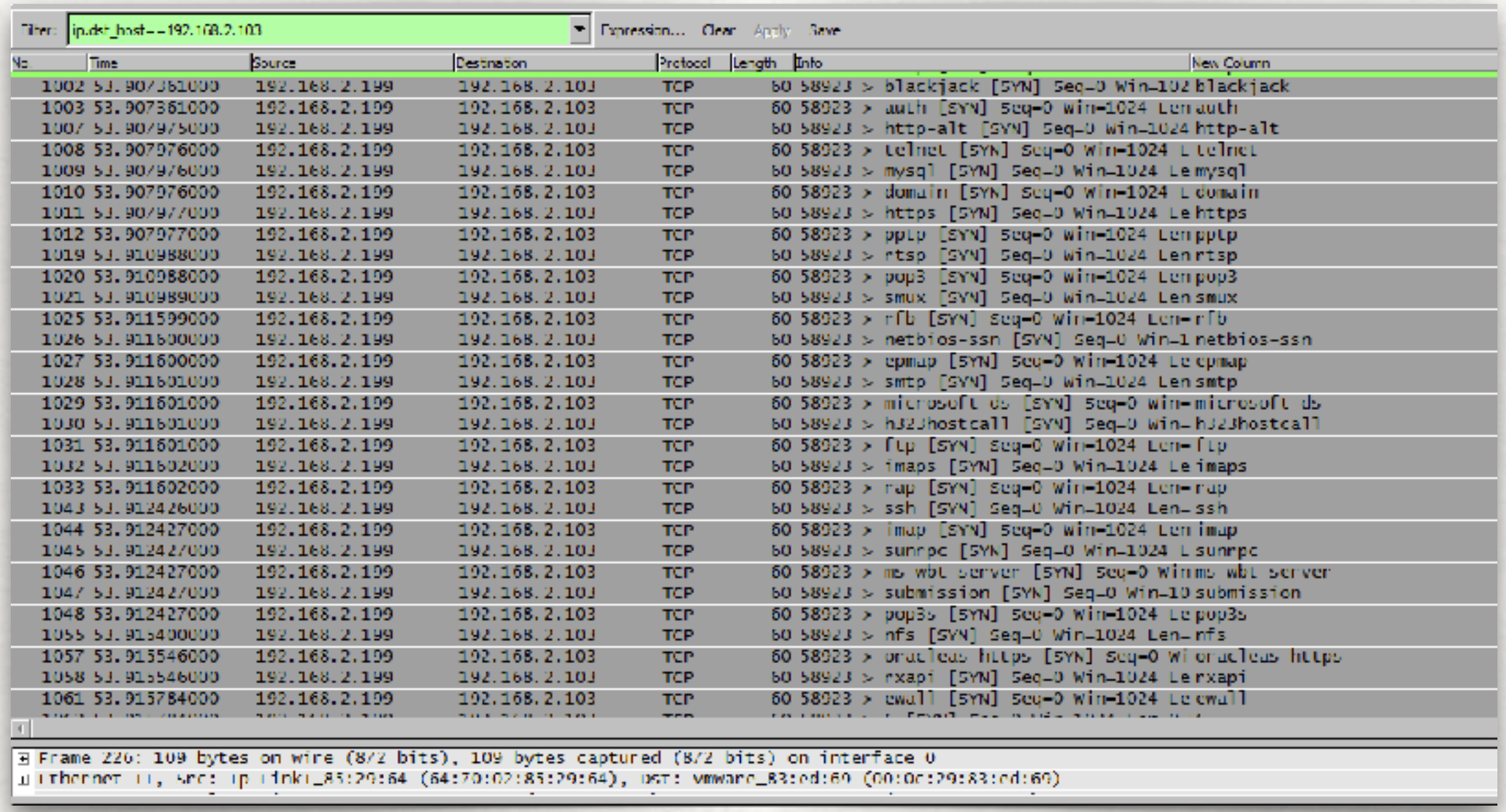
FIREWALL/IDS EVASION

SPOOF SOURCE ADDRESS

```
root@kali:~# nmap -e eth0 -S 192.168.2.199 192.168.2.103
WARNING: If -S is being used to fake your source address, you may also have to u
se -e <interface> and -Pn . If you are using it to specify your real source add
ress, you can ignore this warning.

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 12:08 EDT
NSOCK ERROR [0.0810s] mksock_bind_addr(): Bind to 192.168.2.199:0 failed (IOD #1
): Cannot assign requested address (99)
Nmap scan report for 192.168.2.103
Host is up (0.0013s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.71 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

SPOOF SOURCE ADDRESS



FIREWALL/IDS EVASION

USE SPECIFIED INTERFACE

- -e <interface> (Use specified interface)

Tells Nmap what interface to send and receive packets on. Nmap should be able to detect this automatically, but it will tell you if it cannot.

FIREWALL/IDS EVASION

SPECIFY INTERFACE

```
root@kali:~# nmap -e eth0 -S 192.168.2.199 192.168.2.103
WARNING: If -S is being used to fake your source address, you may also have to u
se -e <interface> and -Pn . If you are using it to specify your real source add
ress, you can ignore this warning.

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 02:08 EDT
\SOCK ERROR [0.0810s] mksock bind addr(): Bind to 192.168.2.199:0 failed (IOD #1
): Cannot assign requested address (99)
\nap scan report for 192.168.2.103
-ost is up (0.0013s latency).
\ot shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss realsecure
912/tcp   open     apex mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
VAC Address: 00:0C:29:83:ED:69 (VMware)

\nap done: 1 IP address (1 host up) scanned in 15.71 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

USE SPOOF SOURCE PORT NUMBER

- --source-port <portnumber>; -g <portnumber>

Nmap will send packets from define port.

Most scanning operations that use raw sockets, including SYN and UDP scans, support the option completely.

The option notably doesn't have an effect for any operations that use normal operating system sockets, including DNS requests, TCP connect scan, version detection, and script scanning

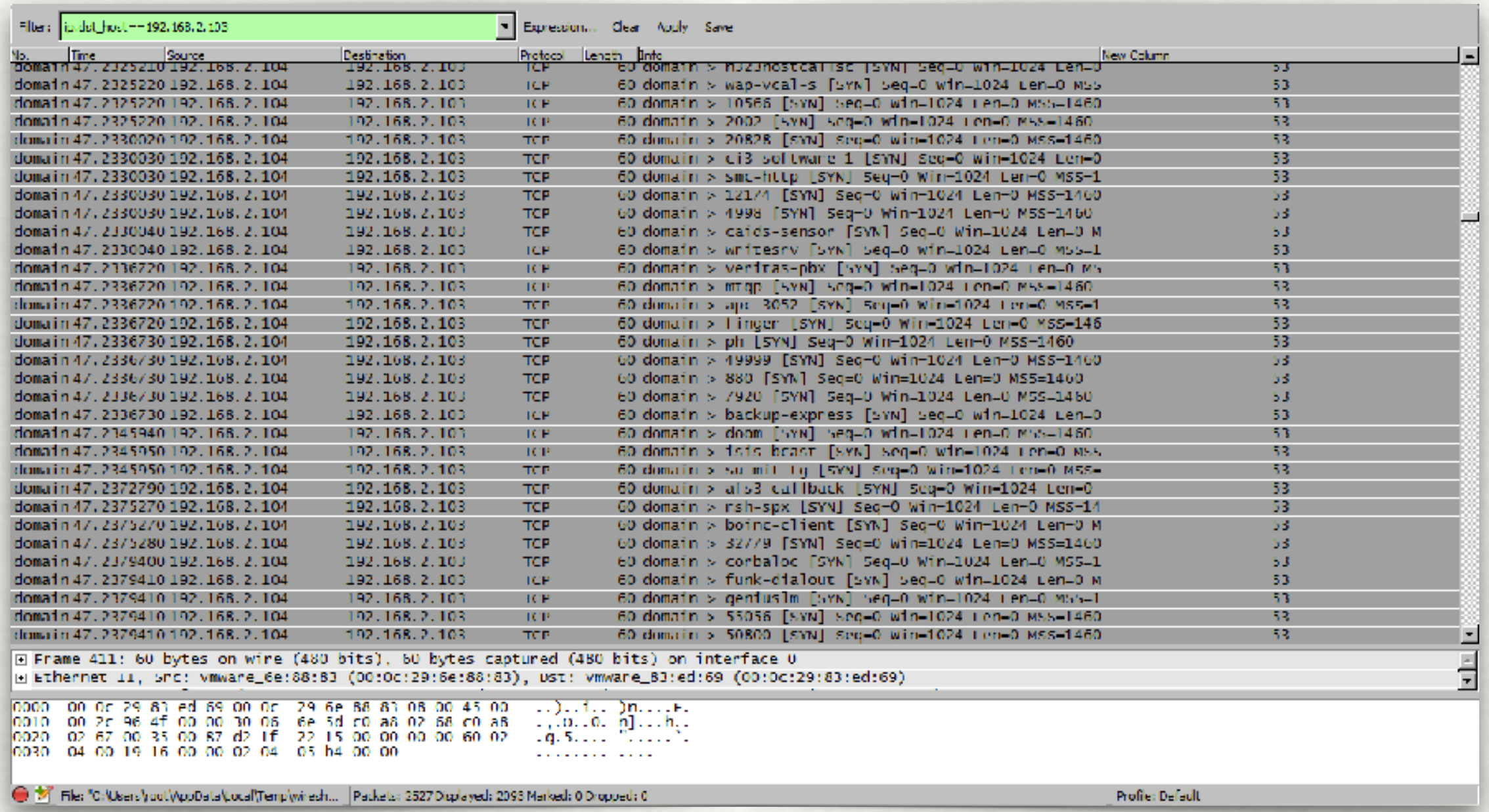
FIREWALL/IDS EVASION

SPOOF SOURCE PORT

```
root@kali:~# nmap --source-port 53 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 02:37 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0016s latency).
Not shown: 984 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
554/tcp  open     rtsp
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
1025/tcp filtered NFS-or-IIS
1026/tcp open     LSA-or-nterm
1027/tcp open     IIS
1028/tcp open     unknown
1029/tcp open     ms-lsa
1030/tcp open     iad1
2869/tcp open     icslap
3389/tcp open     ms-wbt-server
5357/tcp open     wsdapi
10243/tcp open    unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.89 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE



FIREWALL/IDS EVASION

APPEND DATA TO SENT PACKETS

--data <hex string>

This option lets you include binary data as payload in sent packets.

--data 0xdeadbeef and --data \xCA\xFE\x09

--data-string <string>

This option lets you include a regular string as payload in sent packets.

--data-string “Scan test"

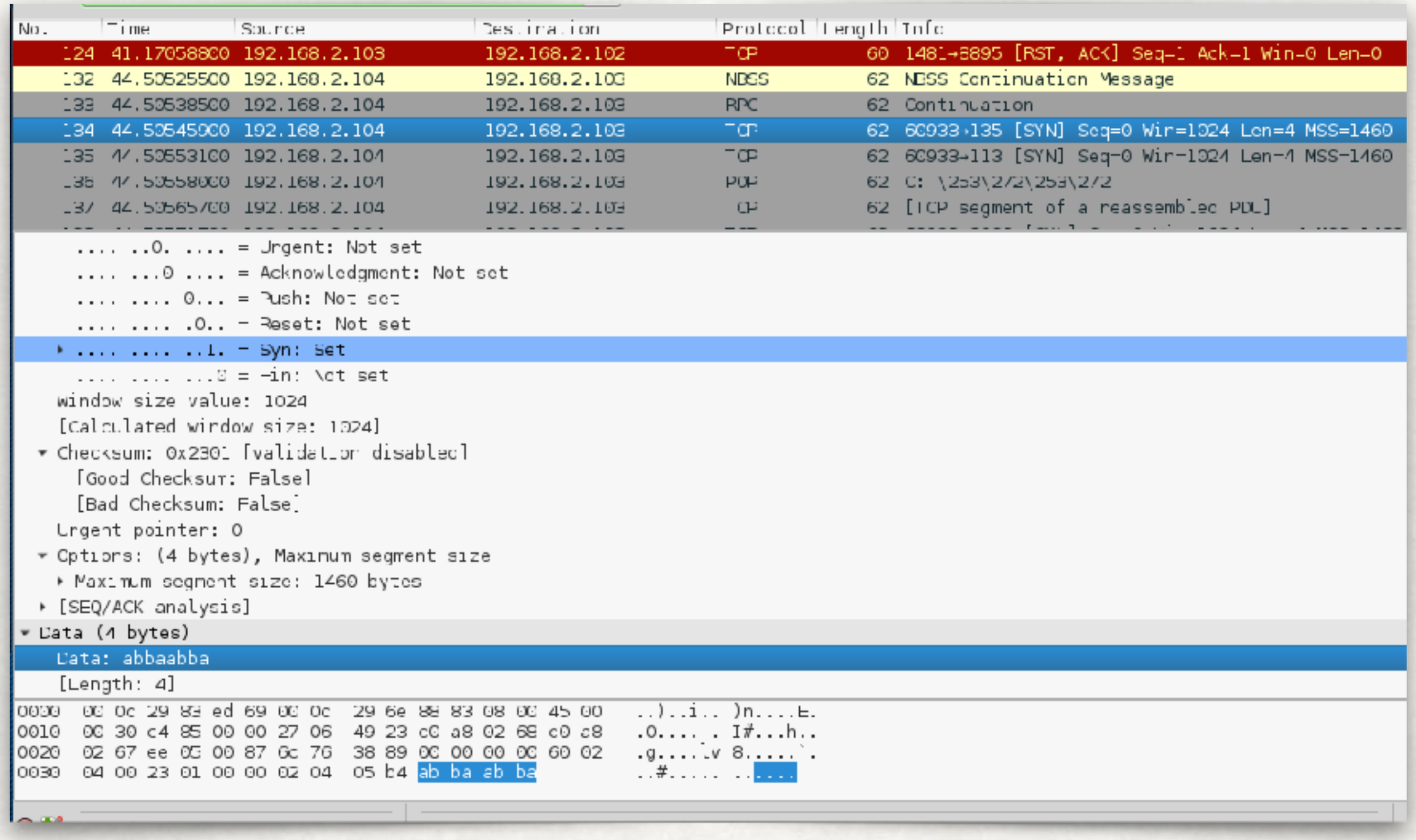
FIREWALL/IDS EVASION

APPEND DATA

```
root@kali:~# nmap --data 0xabbaabba 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 02:45 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00064s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 17.35 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE



FIREWALL/IDS EVASION

APPEND DATA TO SENT PACKETS

--data-length <number>

This option tells Nmap to append the given number of random bytes to most of the packets it sends, and not to use any protocol-specific payloads.

TCP packets are generally 40 bytes and ICMP echo requests are just 28. Some UDP ports and IP protocols get a custom payload by default.

--data-length 0 for no random or protocol-specific payloads.

FIREWALL/IDS EVASION

APPEND DATA

```
root@kali:~# nmap --data-length 55 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 02:54 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0017s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.85 seconds
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE

No.	Time	Source	Destination	Protocol	Length	Info
8	2.914864000	192.168.2.104	192.168.2.103	POP	113	C: \230/\2255\26
9	2.915078000	192.168.2.104	192.168.2.103	NBSS	113	NBSS Continuatio
10	2.915164000	192.168.2.104	192.168.2.103	SSL	113	Continuation Dat
11	2.915216000	192.168.2.104	192.168.2.103	TCP	113	56803→80 [SYN] S
12	2.915287000	192.168.2.104	192.168.2.103	TCP	113	[TCP segment of
13	2.915392000	192.168.2.104	192.168.2.103	TELNET	113	Telnet Data ...
14	2.915460000	192.168.2.104	192.168.2.103	TCP	113	56803→8888 [SYN]
15	2.915522000	192.168.2.104	192.168.2.103	PPTP	113	Unknown control
16	2.915586000	192.168.2.104	192.168.2.103	TCP	113	56803→8080 [SYN]
17	2.915645000	192.168.2.104	192.168.2.103	SMUX	113	
20	2.917954000	192.168.2.103	192.168.2.104	TCP	60	199→56803 [RST,
21	2.920077000	192.168.2.104	192.168.2.103	TCP	113	56803→1025 [SYN]
22	2.920188000	192.168.2.104	192.168.2.103	RTSP	113	Continuation

```
[Time since reference or first frame: 2.915392000 seconds]
Frame Number: 13
Frame Length: 113 bytes (904 bits)
Capture Length: 113 bytes (904 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:telnet]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
▸ Ethernet II, Src: Vmware_6e:88:83 (00:0c:29:6e:88:83), Dst: Vmware_83:ed:69 (00:0c:29:83:ed:69)
```

FIREWALL/IDS EVASION

SPECIFIED IP OPTIONS

--ip-options <S|R [route]|L [route]|T|U ... >; --ip-options <hex string>

For example, \x01\x07\x04\x00*36\x01 is a hex string containing 36 NULL bytes.

--ttl <value> (Set IP time-to-live field)

Sets the IPv4 time-to-live field in sent packets to the given value.

FIREWALL/IDS EVASION

RANDOMIZE TARGET HOST

--randomize-hosts

Tells Nmap to shuffle each group of up to 16384 hosts before it scans them. This can make the scans less obvious to various network monitoring systems, especially when you combine it with slow timing options.

FIREWALL/IDS EVASION

RANDOMIZE HOSTS

```
root@kali:~# nmap -PS -sn --randomize-hosts 192.168.2.100-254
Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 03:20 EDT
Nmap scan report for 192.168.2.107
Host is up (0.26s latency).
MAC Address: A4:F1:E8:9A:89:65 (Unknown)
Nmap scan report for 192.168.2.108
Host is up (0.26s latency).
MAC Address: 00:1C:7B:75:A3:EC (Castlenet Technology)
Nmap scan report for 192.168.2.103
Host is up (0.00019s latency).
MAC Address: 00:0C:29:83:ED:69 (VMware)
Nmap scan report for 192.168.2.100
Host is up (0.00013s latency).
MAC Address: 20:C9:D0:DB:93:9F (Apple)
Nmap scan report for 192.168.2.102
Host is up (0.26s latency).
MAC Address: 28:CF:DA:00:B1:B1 (Apple)
Nmap scan report for 192.168.2.104
Host is up.
Nmap done: 155 IP addresses (6 hosts up) scanned in 29.10 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

SPOOF MAC ADDRESS

--spoof-mac <MAC address, prefix, or vendor name>

Asks Nmap to use the given MAC address for all of the raw ethernet frames it sends. This option implies --send-eth to ensure that Nmap actually sends ethernet-level packets.

If it is simply the number 0, Nmap chooses a completely random MAC address for the session

Valid --spoof-mac argument examples are Apple, 0, 01:02:03:04:05:06, deadbeefcafe, 0020F2, and Cisco

FIREWALL/IDS EVASION

SPOOF MAC ADDRESS

```
root@kali:~# nmap -p135 --spoof-mac 01:02:03:04:05:06 192.168.2.103
Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 03:25 EDT
Spoofing MAC address 01:02:03:04:05:06 (No registered vendor)
Nmap scan report for 192.168.2.103
Host is up (0.00048s latency).
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:0C:29:83:ED:69 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
root@kali:~#
```

FIREWALL/IDS EVASION

WIRESHARK CAPTURE

No.	Time	Source	Destination	Protocol	Length	Info
2	0.695192000	192.168.2.104	192.168.2.103	TCP	58	55093→135 [SYN] Seq=0 Win=102
3	0.696207000	192.168.2.103	192.168.2.104	TCP	60	135→55093 [SYN, ACK] Seq=0 Ac
9	3.711587000	192.168.2.103	192.168.2.104	TCP	60	[TCP Retransmission] 135→5509

```
Encapsulation type: Ethernet (1)
Arrival Time: Aug  6, 2016 03:25:15.484388000 EDT
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1470468315.484388000 seconds
[Time delta from previous captured frame: 0.695192000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.695192000 seconds]
Frame Number: 2
Frame Length: 58 bytes (464 bits)
Capture Length: 58 bytes (464 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP SYN/FIN]
[Coloring Rule String: tcp.flags & 0x02 || tcp.flags.fin == 1]
▸ Ethernet II, Src: Woonsang_04:05:06 (01:02:03:04:05:06), Dst: Vmware_83:ed:69 (00:0c:29:83:ed:69)
▾ Internet Protocol Version 4, Src: 192.168.2.104 (192.168.2.104), Dst: 192.168.2.103 (192.168.2.103)
    Version: 4
```

```
0000  00 0c 29 83 ed 69 01 02  03 04 05 06 08 00 45 00   ..)..i.. ......E.
0010  00 2c 8a 8d 00 00 2e 06  7c 1f c0 a8 02 68 c0 a8   .,...... |....h..
0020  02 67 d7 35 00 87 74 3b  d1 7d 00 00 00 00 60 02   .g.5..t; .}....`.
0030  04 00 f0 90 00 00 02 04  05 b4                     ........ ..
```

FIREWALL/IDS EVASION

RELAY TCP CONNECTIONS THROUGH A CHAIN OF PROXIES

--proxies <Comma-separated list of proxy URLs>

Asks Nmap to establish TCP connections with a final target through supplied chain of one or more HTTP or SOCKS4 proxies. Proxies can help hide the true source of a scan or evade certain firewall restrictions, but they can hamper scan performance by increasing latency.

proto://host:port (Valid protocols are HTTP and SOCKS4.)

#nmap --proxies socks4://202.44.56.78:8090 -p80 -sV -vv google.com

Warning: this feature is still under development and has limitations. It is implemented within the nsock library and thus has no effect on the ping, port scanning and OS discovery phases of a scan. Only NSE and version scan benefit from this option so far—other features may disclose your true address. SSL connections are not yet supported, nor is proxy-side DNS resolution (hostnames are always resolved by Nmap).

TIMING AND PERFORMANCE

NMAP ADVANCED OPTIONS

TIMING AND PERFORMANCE

- Many Nmap features have configurable timing options.
- Timing options can be used to speed up or slow down scanning operations depending on needs

TIMING AND PERFORMANCE

TIMING TEMPLATES

- -T<0-5>: Set timing template (higher is faster)

Template	Name	Notes
-T0	Paranoid	Extremely slow
-T1	Sneaky	Useful for avoiding intrusion detection
-T2	Polite	Unlikely to interfere with the target system
-T3	Normal	This is the default timing template
-T4	Aggressive	Produces faster results on local networks
-T5	Insane	Very fast and aggressive scan

TIMING AND PERFORMANCE

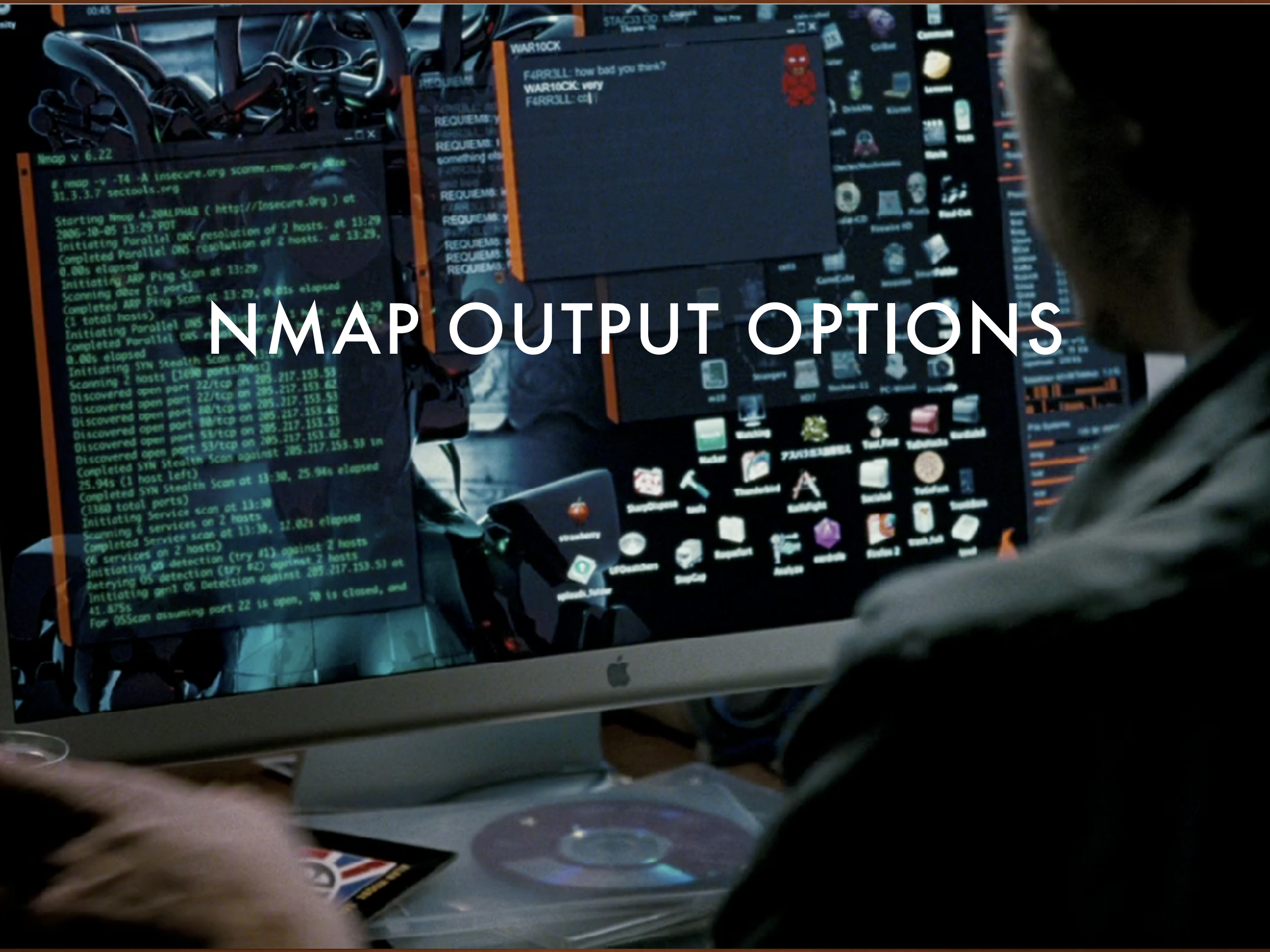
TIMING TEMPLATES

```
root@kali:~/Desktop/result# nmap -T4 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 03:02 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0013s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1039/tcp  open     sbl
1042/tcp  open     afrog
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.38 seconds
```

TIMING AND PERFORMANCE

OTHER OPTIONS

- --max-retries numtries (Specify the maximum number of port scan probe retransmissions) .
- --host-timeout time (Give up on slow target hosts) .
- --scan-delay time; --max-scan-delay time (Adjust delay between probes) .



NMAP OUTPUT OPTIONS

NMAP OUTPUT

Nmap offers several options for creating formatted output.

1. Interactive/stdout Output
2. Save Output to a Text File
3. Save Output to XML File
4. Grepable Output
5. Output All Supported File Types
6. sl<rIpt kIddi3 Output

NMAP OUTPUT

INTERACTIVE OUTPUT

Interactive output is what Nmap prints to the stdout stream, which usually appears on the terminal window you executed Nmap from.

NMAP OUTPUT

INTERACTIVE OUTPUT

```
root@kali:~# nmap 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 05:55 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0017s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
root@kali:~#
```

NMAP OUTPUT

NORMAL OUTPUT

-oN: Normal Output

It is similar to interactive output, except that notes which lose relevance once a scan completes are removed.

It is assumed that the file will be read after Nmap completes, so estimated completion times and new open port alerts are redundant to the actual completion time and the ordered port table.

Since output may be saved a long while and reviewed among many other logs, Nmap prints the execution time, command-line arguments, and Nmap version number on the first line.

NMAP OUTPUT

NORMAL OUTPUT

```
root@kali:~# nmap 192.168.2.103 -oN /root/Desktop/result/nmap103.txt

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 05:58 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.29 seconds
```

NMAP OUTPUT

NORMAL OUTPUT

Open ▾ | nmap103.txt ~/Desktop/result | Save

```
# Nmap 7.12 scan initiated Sat Aug  6 05:58:15 2016 as: nmap -oN /root/Desktop/result/
nmap103.txt 192.168.2.103
Nmap scan report for 192.168.2.103
Host is up (0.0028s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA or nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iadl
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

# Nmap done at Sat Aug  6 05:58:32 2016    1 IP address (1 host up) scanned in 16.29 seconds
```

NMAP OUTPUT

XML OUTPUT

-oX: XML Output

XML, the extensible markup language

The XML format includes more information than the others and is extensible enough that new features can be added without breaking existing programs that use it. It can be parsed by standard XML parsers, which are available for all popular programming languages

NMAP OUTPUT

XML OUTPUT

```
root@kali:~# nmap 192.168.2.103 -oX /root/Desktop/result/nmap103xml.txt

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 10:17 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0012s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.77 seconds
root@kali:~#
```

NMAP OUTPUT

XML OUTPUT

Open | nmap103xml.txt ~/Desktop/result | Save

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.12 scan initiated Sat Aug  6 10:17:37 2016 as: nmap -oX /root/Desktop/result/
nmap103xml.txt 192.168.2.103 -->
<nmaprun scanner="nmap" args="nmap -oX /root/Desktop/result/nmap103xml.txt 192.168.2.103"
start="1470493057" startstr="Sat Aug  6 10:17:37 2016" version="7.12"
xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1000"
services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,1
>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1470493057" endtime="1470493072"><status state="up" reason="arp-response"
reason_ttl="0"/>
<address addr="192.168.2.103" addrtype="ipv4"/>
<address addr="00:0C:29:83:ED:69" addrtype="mac" vendor="VMware"/>
<hostnames>
</hostnames>
<ports><extraports state="closed" count="984">
<extrareasons reason="resets" count="984"/>
</extraports>
<port protocol="tcp" portid="135"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="msrpc" method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="netbios-ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="microsoft-ds" method="table" conf="3"/></port>
<port protocol="tcp" portid="554"><state state="open" reason="syn-ack" reason_ttl="128"/
><service name="rtsp" method="table" conf="3"/></port>
<port protocol="tcp" portid="902"><state state="open" reason="syn-ack" reason_ttl="128"/
```

NMAP OUTPUT

GREPABLE OUTPUT

-oG: Grepable Output

This output format is covered last because it is deprecated.

It is a simple format that lists each host on one line and can be trivially searched and parsed with standard Unix tools such as grep, awk, cut, sed, diff, and Perl.

NMAP OUTPUT

GREPABLE OUTPUT

```
root@kali:~# nmap 192.168.2.103 -oG /root/Desktop/result/nmap103grep.txt

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-06 21:10 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00076s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 16.29 seconds
root@kali:~#
```

NMAP OUTPUT

GREPABLE OUTPUT

Open | nmap103grep.txt ~/Desktop/result | Save

```
# Nmap 7.12 scan initiated Sat Aug  6 21:10:34 2016 as: nmap -oG /root/Desktop/result/
nmap103grep.txt 192.168.2.103
Host: 192.168.2.103 ()  Status: Up
Host: 192.168.2.103 ()  Ports: 135/open/tcp//msrpc///, 139/open/tcp//netbios-ssn///, 445/
open/tcp//microsoft-ds///, 554/open/tcp//rtsp///, 902/open/tcp//iss-realsecure///, 912/open/
tcp//apex-mesh///, 1025/filtered/tcp//NFS-or-IIS///, 1026/open/tcp//LSA-or-nterm///, 1027/
open/tcp//IIS///, 1028/open/tcp//unknown///, 1029/open/tcp//ms-lsa///, 1030/open/tcp//
iad1///, 2869/open/tcp//icslap///, 3389/open/tcp//ms-wbt-server///, 5357/open/tcp//
wsdapi///, 10243/open/tcp//unknown///   Ignored State: closed (984)
# Nmap done at Sat Aug  6 21:10:49 2016 -- 1 IP address (1 host up) scanned in 16.29 seconds
```

NMAP OUTPUT

ALL OUTPUT

-oA: All Output

The **-oA** parameter saves the output of a scan in text, grepable, and XML formats.

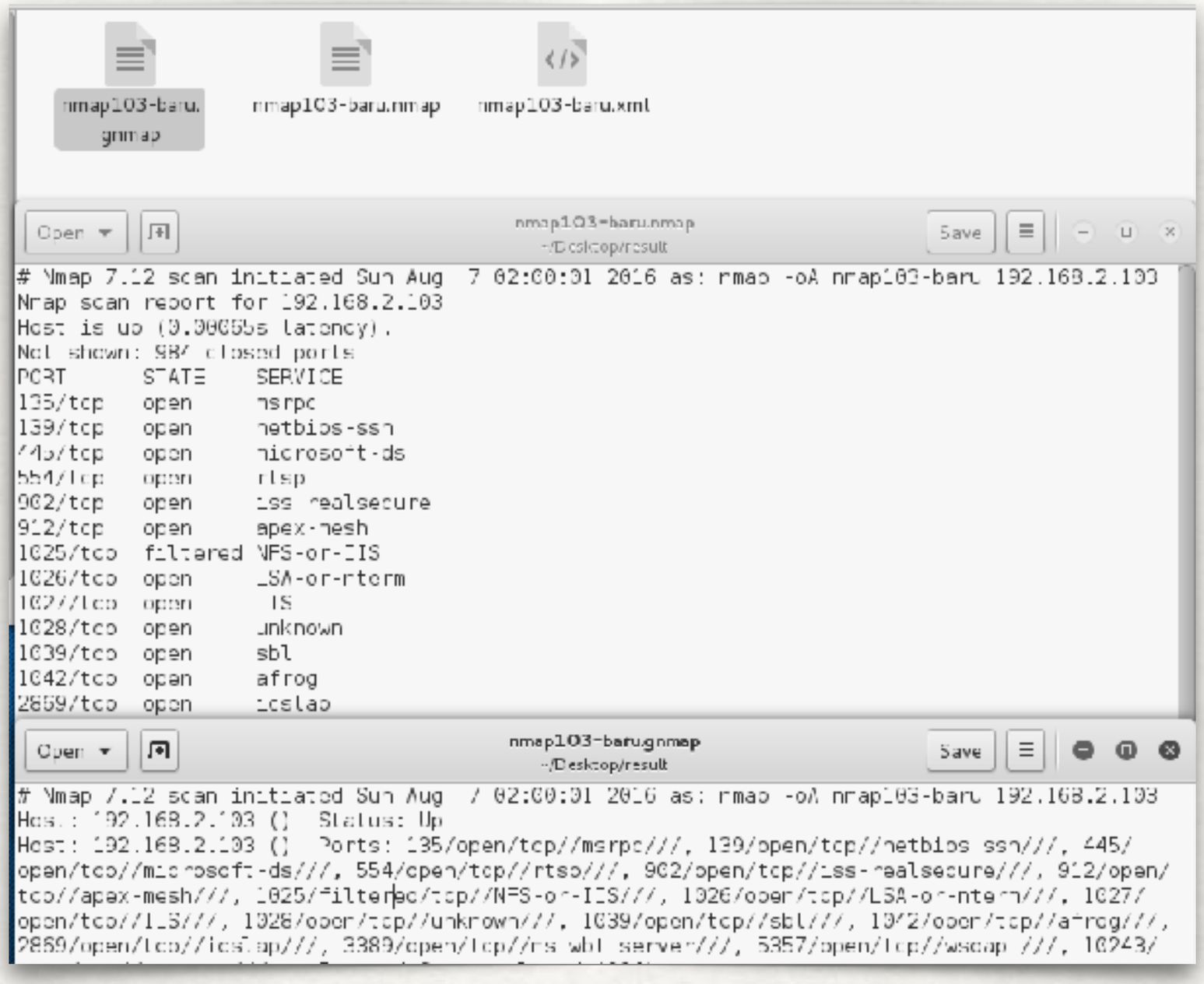
NMAP OUTPUT

ALL OUTPUT

```
root@kali:~/Desktop/result# nmap -oA nmap103-baru 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:00 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00065s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1039/tcp  open     sbl
1042/tcp  open     afrog
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
root@kali:~/Desktop/result#
```

NMAP OUTPUT

ALL OUTPUT



NMAP OUTPUT

$CRIPT KIDDI3 0UTPUT

-oS: $crIpT kIddI3 0uTPut

Script kiddie output is like interactive output, except that it is post-processed to better suit the 'l33t HaXXorZ!

NMAP OUTPUT

$CRIPT KIDDI3 0UTPUT

```
root@kali:~# nmap -Pn 192.168.2.103 -oS /root/Desktop/result/nmap103skript.txt

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 00:21 EDT
Nmap scan report for 192.168.2.103
Host is up (0.0011s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
1028/tcp  open     unknown
1029/tcp  open     ms-lsa
1030/tcp  open     iad1
2869/tcp  open     icslap
3389/tcp  open     ms-wbt-server
5357/tcp  open     wsdapi
10243/tcp open     unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.44 seconds
root@kali:~#
```

NMAP OUTPUT

$CRIPT KIDDI3 0UTPUT

Open | nmap1O3skript.txt ~/Desktop/result | Save

```
$tart|ng nMap 7.12 ( HtTPz://NmAp.0rg ) at 2016-08-07 00:21 eDT
NmaP scAn r3p0rt fOr 192.168.2.103
HO$t !s up (0.0011S lAt3Ncy).
not $h0Wn: 984 CloSed pOrTs
P0rt      ST4Te    S3RV!C3
135/tCp   0pen     m$rPc
139/tcp   opeN     neTb!0z-s$n
445/tcp   open     M!croSoft-Ds
554/tcp   0p3n     rt$p
902/tcp   open     i$s-reals3cur3
912/Tcp   op3n     apex-M3sh
1025/tcP  filtered nFz-0r-I|s
1026/tcp  opEn     LS4-or-nt3rM
1027/tcp  0pen     1Iz
1028/Tcp  open     unkn0wn
1029/tcp  op3N     mz-l$A
1030/tcp  0pEn     !ad1
2869/tCp  0p3n     Ic$lAp
3389/Tcp  op3n     mz-wbT-$3rvEr
5357/TCp  0pEn     w$daP1
10243/tcp 0pen     unknOwn
M4C addr3ss: 00:0c:29:83:3D:69 (VMwar3)

Nmap d0ne: 1 iP aDdR3$s (1 hoSt up) scanned in 15.44 SEC0ndz
```

NMAP OUTPUT

CREATE HTML OUTPUT

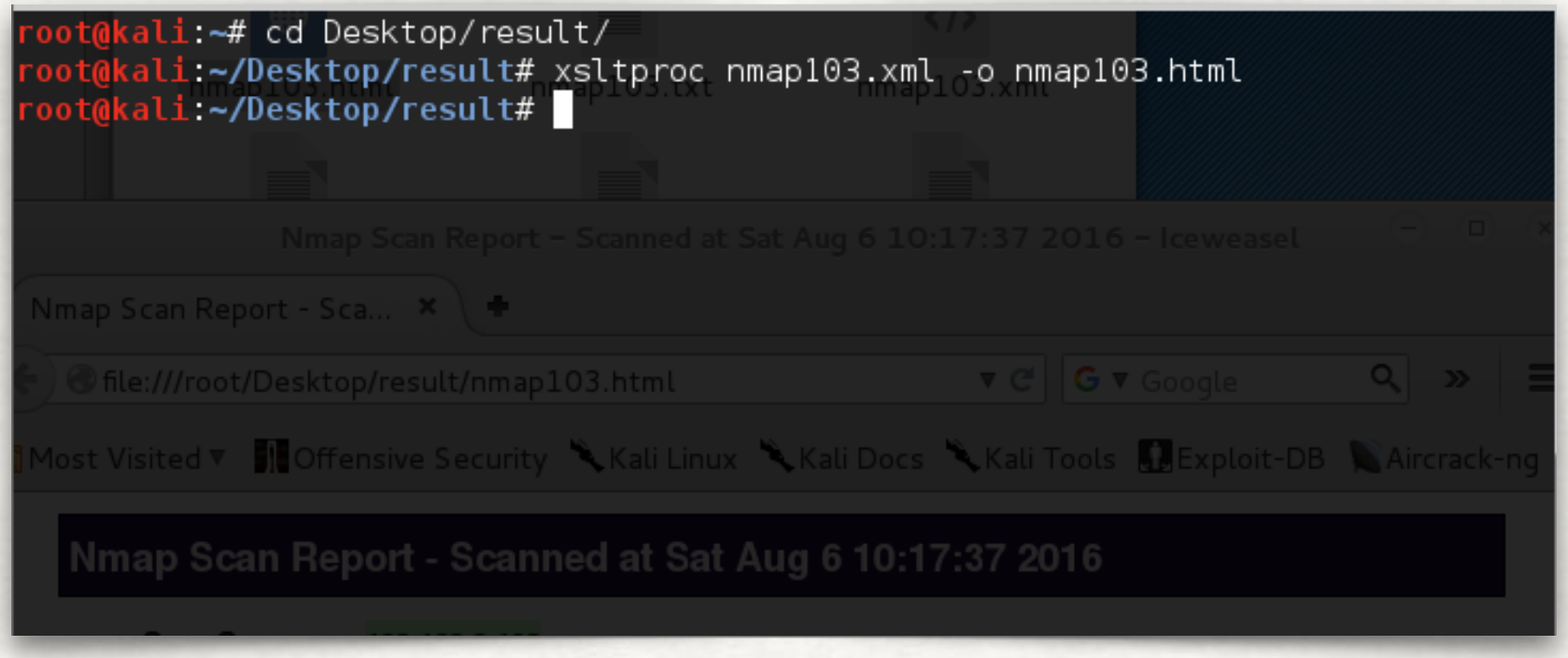
- Nmap does not have an option for saving scan results in HTML, however it is possible to convert XML output to HTML automatically.
- An Nmap XML output file usually contains a reference to an XSL stylesheet called nmap.xsl that describes how the transformation takes place.

```
<?xml-stylesheet href="/usr/share/nmap/nmap.xsl" type="text/xsl"?>

<?xml-stylesheet href="http://nmap.org/svn/docs/nmap.xsl"
type="text/xsl"?>
```

- Using **xslproc** to generate xml output to html.

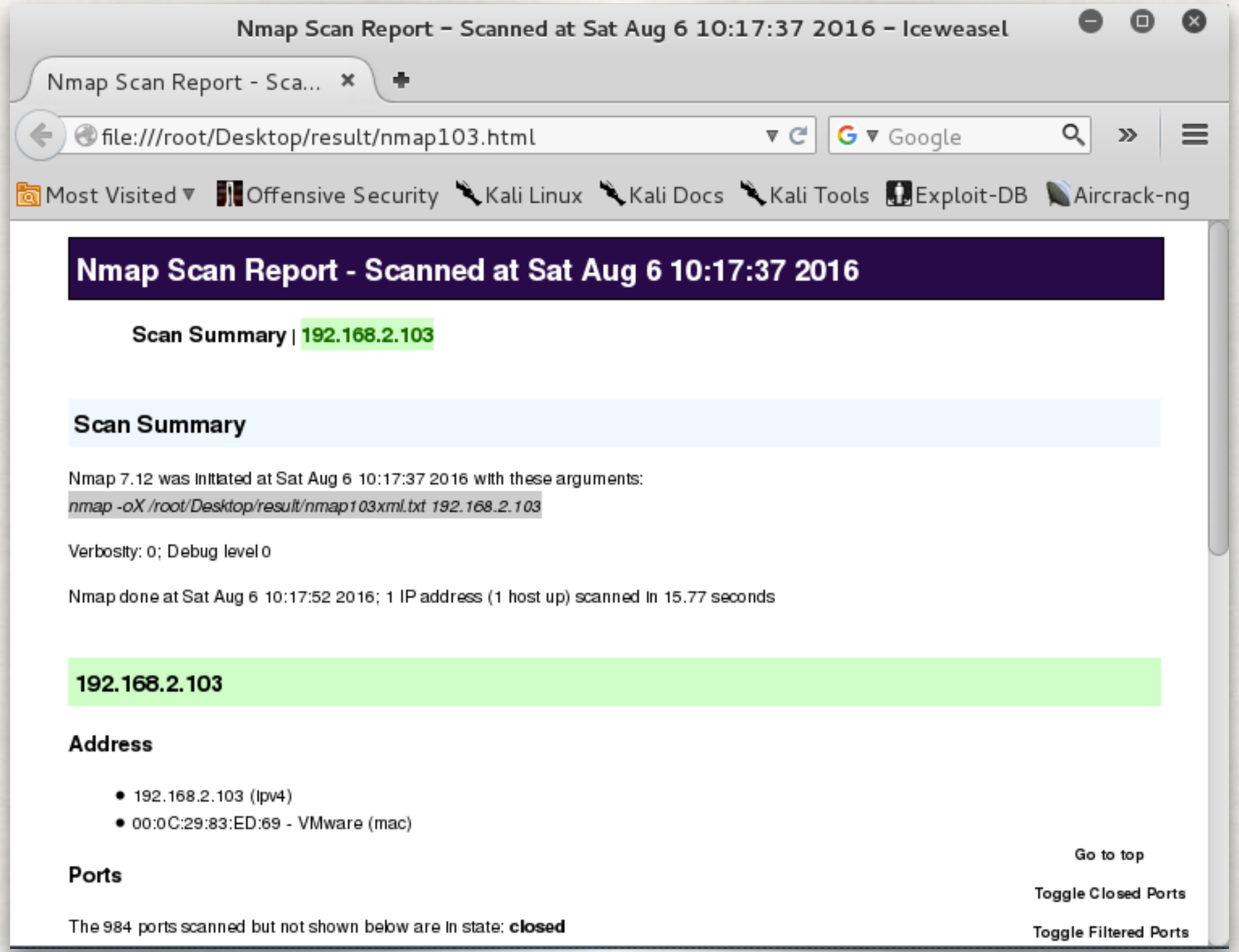
NMAP OUTPUT

CREATE HTML OUTPUT



NMAP OUTPUT

CREATE HTML OUTPUT



NMAP DEBUGGING AND TROUBLESHOOTING

NMAP DEBUGGING

VERBOSITY

-v (Increase verbosity level) .

Increases the verbosity level, causing Nmap to print more information about the scan in progress. Open ports are shown as they are found and completion time estimates are

provided when Nmap thinks a scan will take more than a few minutes. Use it twice or more for even greater verbosity: -vv, or give a verbosity level directly, for example -v3..

NMAP DEBUGGING

VERBOSITY

```
root@kali:~/Desktop/result# nmap -v 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 01:43 EDT
Initiating ARP Ping Scan at 01:43
Scanning 192.168.2.103 [1 port]
Completed ARP Ping Scan at 01:43, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:43
Completed Parallel DNS resolution of 1 host. at 01:43, 13.00s elapsed
Initiating SYN Stealth Scan at 01:43
Scanning 192.168.2.103 [1000 ports]
Discovered open port 139/tcp on 192.168.2.103
Discovered open port 554/tcp on 192.168.2.103
Discovered open port 135/tcp on 192.168.2.103
Discovered open port 3389/tcp on 192.168.2.103
Discovered open port 5357/tcp on 192.168.2.103
Discovered open port 1027/tcp on 192.168.2.103
Discovered open port 1028/tcp on 192.168.2.103
Discovered open port 10243/tcp on 192.168.2.103
Discovered open port 445/tcp on 192.168.2.103
Discovered open port 912/tcp on 192.168.2.103
Discovered open port 902/tcp on 192.168.2.103
Discovered open port 1039/tcp on 192.168.2.103
Discovered open port 2869/tcp on 192.168.2.103
Discovered open port 1042/tcp on 192.168.2.103
Discovered open port 1026/tcp on 192.168.2.103
Completed SYN Stealth Scan at 01:43, 2.32s elapsed (1000 total ports)
Nmap scan report for 192.168.2.103
Host is up (0.00068s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
```

NMAP DEBUGGING

VERBOSITY

```
root@kali:~/Desktop/result# nmap -v3 -p 135-500  192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 01:44 EDT
Initiating ARP Ping Scan at 01:44
Scanning 192.168.2.103 [1 port]
Completed ARP Ping Scan at 01:44, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:44
Completed Parallel DNS resolution of 1 host. at 01:44, 13.01s elapsed
DNS resolution of 1 IPs took 13.01s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF:
 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 01:44
Scanning 192.168.2.103 [366 ports]
Discovered open port 139/tcp on 192.168.2.103
Discovered open port 135/tcp on 192.168.2.103
Discovered open port 445/tcp on 192.168.2.103
Completed SYN Stealth Scan at 01:44, 1.11s elapsed (366 total ports)
Nmap scan report for 192.168.2.103
Host is up, received arp-response (0.00057s latency).
Scanned at 2016-08-07 01:44:15 EDT for 14s
Not shown: 363 closed ports
Reason: 363 resets
PORT    STATE SERVICE      REASON
135/tcp open  msrpc        syn-ack ttl 128
139/tcp open  netbios-ssn  syn-ack ttl 128
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: 00:0C:29:83:ED:69 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds
           Raw packets sent: 430 (18.904KB) | Rcvd: 367 (14.680KB)
```

NMAP DEBUGGING

DEBUGGING

-d (Increase debugging level) .

Debugging output is useful when a bug is suspected in Nmap, or if you are simply confused as to what Nmap is doing and why. As this feature is mostly intended for developers.

-d1-9

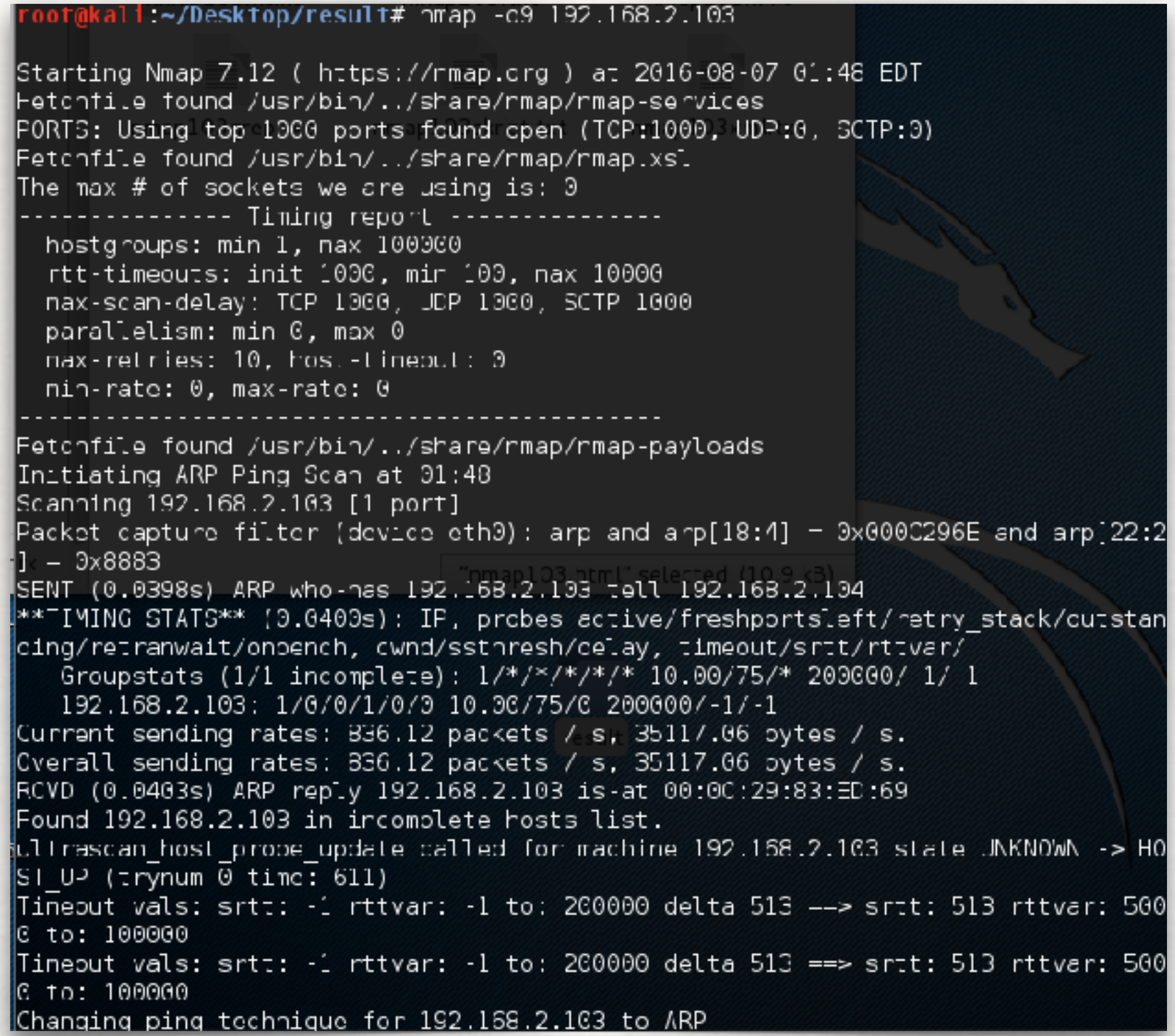
NMAP DEBUGGING

DEBUGGING

```
root@kali:~/Desktop/result# nmap -d 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 01:48 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Initiating ARP Ping Scan at 01:48
Scanning 192.168.2.103 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x000C296E and arp[22:2
] = 0x8883
Completed ARP Ping Scan at 01:48, 0.00s elapsed (1 total hosts)
Overall sending rates: 733.14 packets / s, 30791.79 bytes / s.
mass_rdns: Using DNS server 192.168.2.1
Initiating Parallel DNS resolution of 1 host. at 01:48
mass_rdns: 13.00s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 3]
Completed Parallel DNS resolution of 1 host. at 01:48, 13.00s elapsed
DNS resolution of 1 IPs took 13.00s. Mode: Async [#: 1, OK: 0, NX: 0, DR: 1, SF:
 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 01:48
Scanning 192.168.2.103 [1000 ports]
Packet capture filter (device eth0): dst host 192.168.2.104 and (icmp or icmp6 o
r (tcp or udp or sctp) and (src host 192.168.2.103)))
Discovered open port 3389/tcp on 192.168.2.103
Discovered open port 135/tcp on 192.168.2.103
Discovered open port 554/tcp on 192.168.2.103
Discovered open port 445/tcp on 192.168.2.103
Discovered open port 1026/tcp on 192.168.2.103
```

NMAP DEBUGGING

DEBUGGING



NMAP DEBUGGING

REASON

--reason (Host and port state reasons) .

Shows the reason each port is set to a specific state and the reason each host is up or down. This option displays the type of the packet that determined a port or hosts state.

For example, A RST packet from a closed port or an echo reply from an alive host. The information Nmap can provide is determined by the type of scan or ping. The SYN scan and SYN

ping (-sS and -PS) are very detailed, but the TCP connect scan (-sT) is limited by the implementation of the connect system call. This feature is automatically enabled by the debug option (-d). and the results are stored in XML log files even if this option is not specified.

NMAP DEBUGGING

REASON

```
root@kali:~/Desktop/result# nmap   reason 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 01:52 EDT
Nmap scan report for 192.168.2.103
Host is up, received arp-response (0.00036s latency).
Not shown: 985 closed ports
Reason: 985 resets
PORT      STATE    SERVICE         REASON
135/tcp   open     msrpc           syn ack ttl 128
139/tcp   open     netbios-ssn     syn-ack ttl 128
445/tcp   open     microsoft-ds    syn-ack ttl 128
554/tcp   open     rtsp            syn-ack ttl 128
902/tcp   open     iss-realsecure  syn-ack ttl 128
912/tcp   open     apex-mesh       syn-ack ttl 128
1025/tcp  filtered NFS-or-IIS      no-response
1026/tcp  open      SA-or-nterm    syn-ack ttl 128
1027/tcp  open     IIS             syn ack ttl 128
1028/tcp  open     unknown         syn-ack ttl 128
1039/tcp  open     sbl             syn-ack ttl 128
1042/tcp  open     afrog           syn-ack ttl 128
2869/tcp  open     icslap          syn-ack ttl 128
5357/tcp  open     wsdapi          syn-ack ttl 128
10243/tcp open     unknown         syn-ack ttl 128
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.43 seconds
root@kali:~/Desktop/result#
```

NMAP DEBUGGING

PERIODIC RESULT

--stats-every time (Print periodic timing stats) .

Periodically prints a timing status message after each interval of time. The time is a specification of the kind described in the section called "TIMING AND PERFORMANCE"; so for example, use --stats-every 10s to get a status update every 10 seconds. Updates are printed to interactive output (the screen) and XML output.

NMAP DEBUGGING

PERIODIC RESULT

```
root@kali:~/Desktop/result# nmap --stats-every 5s  192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:06 EDT
Stats: 0:00:05 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
SYN Stealth Scan Timing: About 98.67% done; ETC: 02:07 (0:00:00 remaining)
Nmap scan report for 192.168.2.103
Host is up (0.00094s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
554/tcp   open     rtsp
902/tcp   open     iss-realsecure
912/tcp   open     apex-mesh
1025/tcp  filtered NFS-or-IIS
1026/tcp  open     LSA-or-nterm
1027/tcp  open     IIS
```

NMAP DEBUGGING

PACKET TRACE

--packet-trace (Trace packets and data sent and received) .

Causes Nmap to print a summary of every packet sent or received. This is often used for debugging, but is also a valuable way for new users to understand exactly what Nmap is doing under the covers.

To avoid printing thousands of lines, you may want to specify a limited number of ports to scan, such as -p20-30. If you only care about the goings on of the version detection subsystem, use --version-trace instead.

If you only care about script tracing, specify --script-trace. With --packet-trace, you get all of the above.

NMAP DEBUGGING

PACKET TRACE

```
root@kali:~/Desktop/result# nmap --packet-trace --script-trace -p135-140  192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:15 EDT
SENT (0.0581s) ARP who has 192.168.2.103 tell 192.168.2.104
RCVD (0.0586s) ARP reply 192.168.2.103 is-at 00:0C:29:83:ED:59
NSOCK INFO [0.0660s] nsock_ioc_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0670s] nsock_connect_udp(): UDP connection requested to 192.168.2.1:53 (IOD #1) EID 8
NSOCK INFO [0.0670s] nsock_read(): Read request from IOD #1 [192.168.2.1:53] (timeout: -1ms) EID 18
NSOCK INFO [0.0670s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192.168.2.1:53]
NSOCK INFO [0.0670s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [192.168.2.1:53]
NSOCK INFO [0.0670s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [192.168.2.1:53]
NSOCK INFO [0.2790s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [192.168.2.1:53] (148 bytes)
NSOCK INFO [0.2790s] nsock_read(): Read request from IOD #1 [192.168.2.1:53] (timeout: -1ms) EID 34
NSOCK INFO [4.0660s] nsock_write(): Write request for 44 bytes to IOD #1 EID 43 [192.168.2.1:53]
NSOCK INFO [4.0660s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [192.168.2.1:53]
NSOCK INFO [4.1460s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 34 [192.168.2.1:53] (137 bytes)
NSOCK INFO [4.1460s] nsock_read(): Read request from IOD #1 [192.168.2.1:53] (timeout: -1ms) EID 50
NSOCK INFO [8.0700s] nsock_write(): Write request for 44 bytes to IOD #1 EID 59 [192.168.2.1:53]
NSOCK INFO [8.0700s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [192.168.2.1:53]
NSOCK INFO [8.7910s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 50 [192.168.2.1:53] (137 bytes)
NSOCK INFO [8.7910s] nsock_read(): Read request from IOD #1 [192.168.2.1:53] (timeout: -1ms) EID 66
NSOCK INFO [13.0710s] nsock_iod_delete(): nsock_ioc_delete (IOD #1)
NSOCK INFO [13.0710s] nevent_delete(): nevent_delete on event #66 (type READ)
SENT (13.0729s) TCP 192.168.2.104:52279 > 192.168.2.103:135 S ttl=39 id=44830 iplen=44  seq=3656263236 win=1024 <mss 1460>
SENT (13.0730s) TCP 192.168.2.104:52279 > 192.168.2.103:139 S ttl=54 id=57090 iplen=44  seq=3656263236 win=1024 <mss 1460>
SENT (13.0731s) TCP 192.168.2.104:52279 > 192.168.2.103:137 S ttl=49 id=30094 iplen=44  seq=3656263236 win=1024 <mss 1460>
SENT (13.0732s) TCP 192.168.2.104:52279 > 192.168.2.103:130 S ttl=40 id=33004 iplen=44  seq=3656263236 win=1024 <mss 1460>
SENT (13.0734s) TCP 192.168.2.104:52279 > 192.168.2.103:136 S ttl=41 id=40576 iplen=44  seq=3656263236 win=1024 <mss 1460>
SENT (13.0735s) TCP 192.168.2.104:52279 > 192.168.2.103:140 S ttl=39 id=45164 iplen=44  seq=3656263236 win=1024 <mss 1460>
RCVD (13.0743s) ICMP [192.168.2.103 > 192.168.2.104 Port 52279 unreachable (type=3/code=3) iplen=40
SENT (14.1760s) TCP 192.168.2.104:52280 > 192.168.2.103:136 S ttl=47 id=39900 iplen=44  seq=3656323773 win=1024 <mss 1460>
SENT (14.1762s) TCP 192.168.2.104:52280 > 192.168.2.103:138 S ttl=49 id=4750 iplen=44  seq=3656323773 win=1024 <mss 1460>
SENT (14.1764s) TCP 192.168.2.104:52280 > 192.168.2.103:137 S ttl=54 id=42152 iplen=44  seq=3656323773 win=1024 <mss 1460>
SENT (14.1766s) TCP 192.168.2.104:52280 > 192.168.2.103:139 S ttl=38 id=52216 iplen=44  seq=3656323773 win=1024 <mss 1460>
SENT (14.1767s) TCP 192.168.2.104:52280 > 192.168.2.103:135 S ttl=54 id=42522 iplen=44  seq=3656323773 win=1024 <mss 1460>
RCVD (14.1784s) TCP 192.168.2.103:136 > 192.168.2.104:52280 RA ttl=128 id=9796 iplen=40  seq=0 win=0
RCVD (14.1786s) TCP 192.168.2.103:138 > 192.168.2.104:52280 RA ttl=128 id=9797 iplen=40  seq=0 win=0
RCVD (14.1787s) TCP 192.168.2.103:137 > 192.168.2.104:52280 RA ttl=128 id=9798 iplen=40  seq=0 win=0
```

NMAP DEBUGGING

OTHER OPTIONS

--open (Show only open (or possibly open) ports) .

Specify --open to only see hosts with at least one open, openl filtered, or unfiltered port, and only see ports in those states.

--iflist (List interfaces and routes) .

Prints the interface list and system routes as detected by Nmap. This is useful for debugging routing problems or device mischaracterization (such as Nmap treating a PPP connection as ethernet).

NMAP DEBUGGING

OTHER OPTIONS

```
root@kali:~/Desktop/result# nmap --open 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:23 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00030s latency).
Not shown: 984 closed ports, 1 filtered port
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1028/tcp  open  unknown
1039/tcp  open  sbl
1042/tcp  open  afrog
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 00:0C:29:83:ED:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

NMAP DEBUGGING

OTHER OPTIONS

```
root@kali:~/Desktop/result# nmap --iflist 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:24 EDT
************************INTERFACES************************
DEV  (SHORT) IP/MASK                      TYPE     UP MTU   MAC
eth0 (eth0)  192.168.2.104/24             ethernet up 1500  00:0C:29:6E:88:83
eth0 (eth0)  fe80::20c:29ff:fe6e:8883/64  ethernet up 1500  00:0C:29:6E:88:83
lo   (lo)    127.0.0.1/8                  loopback up 65536
lo   (lo)    ::1/128                      loopback up 65536

**************************ROUTES**************************
DST/MASK                        DEV  METRIC GATEWAY
192.168.2.0/24                  eth0 0
0.0.0.0/0                       eth0 1024   192.168.2.1
::1/128                         lo   0
fe80::20c:29ff:fe6e:8883/128    lo   0
::1/128                         lo   256
fe80::/64                       eth0 256
ff00::/8                        eth0 256

root@kali:~/Desktop/result#
```

NMAP MISCELLANEOUS OPTIONS

NMAP MISCELLANEOUS OPTIONS

IPV6 SCAN

-6 (Enable IPv6 scanning) .

Nmap has IPv6 support for its most popular features. Ping scanning, port scanning, version detection, and the Nmap Scripting Engine all support IPv6. The command syntax is the same as usual except that you also add the -6 option. Of course, you must use IPv6 syntax if you specify an address rather than a hostname.

An address might look like 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, so hostnames are recommended. The output looks the same as usual, with the IPv6 address on the "interesting ports" line being the only IPv6 giveaway.

While IPv6 hasn't exactly taken the world by storm, it gets significant use in some (usually Asian) countries and most modern operating systems support it. To use Nmap with IPv6, both the source and target of your scan must be configured for IPv6.

NMAP DEBUGGING

IPV6 SCAN

```
root@kali:~/Desktop/result# nmap -6 -vv fe80::20c:29ff:fe6e:8883

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:47 EDT
Initiating Parallel DNS resolution of 1 host. at 02:47
Completed Parallel DNS resolution of 1 host. at 02:47, 13.00s elapsed
Initiating SYN Stealth Scan at 02:47
Scanning fe80::20c:29ff:fe6e:8883 [1000 ports]
Completed SYN Stealth Scan at 02:47, 0.01s elapsed (1000 total ports)
Nmap scan report for fe80::20c:29ff:fe6e:8883
Host is up, received localhost-response (0.0000050s latency).
All 1000 scanned ports on fe80::20c:29ff:fe6e:8883 are closed because of 1000 resets

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.06 seconds
           Raw packets sent: 1000 (64.000KB) | Rcvd: 2000 (124.000KB)
root@kali:~/Desktop/result#
```

NMAP MISCELLANEOUS OPTIONS

AGGRESSIVE SCAN

-A (Aggressive scan options) .

This option enables additional advanced and aggressive options. Presently this enables OS detection (-O), version scanning (-sV), script scanning (-sC) and traceroute (--traceroute).. More features may be added in the future. The point is to enable a comprehensive set of scan options without people having to remember a large set of flags.

However, because script scanning with the default set is considered intrusive, you should not use -A against target networks without permission. This option only enables features, and not timing options (such as -T4) or verbosity options (-v) that you might want as well. Options which require privileges (e.g. root access) such as OS detection and traceroute will only be enabled if those privileges are available.

NMAP DEBUGGING

AGGRESSIVE SCAN

```
root@kali:~/Desktop/result# nmap -A 192.168.2.103

Starting Nmap 7.12 ( https://nmap.org ) at 2016-08-07 02:50 EDT
Nmap scan report for 192.168.2.103
Host is up (0.00076s latency).
Not shown: 984 closed ports
PORT      STATE    SERVICE          VERSION
135/tcp   open     msrpc            Microsoft Windows RPC
139/tcp   open     netbios-ssn      Microsoft Windows 98 netbios-ssn
445/tcp   open     microsoft-ds     Microsoft Windows 10 microsoft-ds
554/tcp   open     rtsp?
902/tcp   open     ssl/vmware-auth  VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open     vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1025/tcp  filtered NFS or IIS
1026/tcp  open     msrpc            Microsoft Windows RPC
1027/tcp  open     msrpc            Microsoft Windows RPC
1029/tcp  open     msrpc            Microsoft Windows RPC
1038/tcp  open     msrpc            Microsoft Windows RPC
1042/tcp  open     msrpc            Microsoft Windows RPC
2869/tcp  open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open     tcpwrapped
| ssl-cert: Subject: commonName=WIN-REINUH5DONW
| Not valid before: 2016-04-23T15:11:00
|_Not valid after:  2016-10-23T15:11:00
| ssl-date: 2016-08-07T06:52:45+00:00; 0s from scanner time.
5357/tcp  open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| http-title: Service Unavailable
10243/tcp open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
MAC Address: 00:0C:29:83:CD:69 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
```

NMAP MISCELLANEOUS OPTIONS

OTHER OPTIONS

-V; --version (Print version number) .

Prints the Nmap version number and exits.

-h; --help (Print help summary page) .

Prints a short help screen with the most common command flags. Running Nmap without any arguments does the same thing.

--resume filename (Resume aborted scan) .

Cancel NMAP by pressing ctrl-C. Restarting the whole scan from the beginning may be undesirable. Fortunately, if normal (-oN) or grepable (-oG) logs were kept, the user can ask Nmap to resume scanning with the target it was working on when execution ceased. Simply specify the --resume option and pass the normal/grepable output file as its argument. No other arguments are permitted, as Nmap parses the output file to use the same ones specified previously.

REFERENCE

- NMAP Manual
- NMAP Online book (free content) - https://nmap.org/book/