Name: Sanchit Monga

Activity 1 – Set up your working environment

(5 p) In your lab report you must include the Username and Password

for accessing MS Windows 10:
username:student
pass:student
for accessing Linux Kali:
username: root
pass:cseclabs

Activity 2 – Use nmap software application

(10 p) In your lab report you must include the exact commands you used, including the actual IP Address you will be using for the <IP Address> field, for the following Port Scanning methods:

Intended instruction	Actual command line used
nmap -sS -v <IP Address>	nmap -sS -v 192.168.58.1
nmap -sT -v <IP Address>	nmap -sT -v 192.168.58.1
nmap -sF -v <IP Address>	nmap -sF -v 192.168.58.1
nmap -sA -v <IP Address>	nmap -sA -v 192.168.58.1

Activity 3 – Port scanning method description

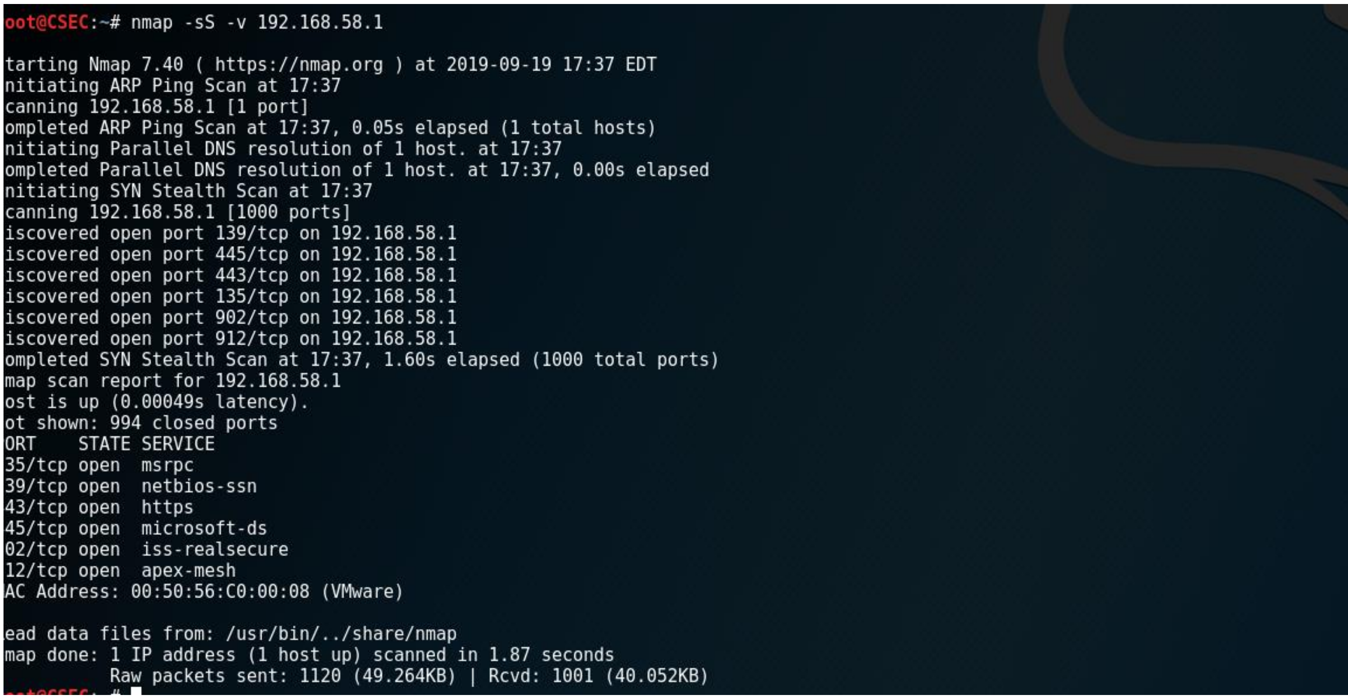
(10 p) Identify the matching Port Scanning method with each nmap command listed and used in the Instructions step **Activity 2,** 1. (a.).

Command line used	Port Scanning method
nmap -sS -v <IP Address>	SYN Scan
nmap -sT -v <IP Address>	Connect Scan
nmap -sF -v <IP Address>	FIN Scan
nmap -sA -v <IP Address>	ACK Scan

For each of the port scanning method used in the Instructions step **Activity 2,** 1. (a.)., include the matching screenshots and corresponding Wireshark captures, using the data collected in Instructions step **Activity 3,** 1. (a.) – (c.).

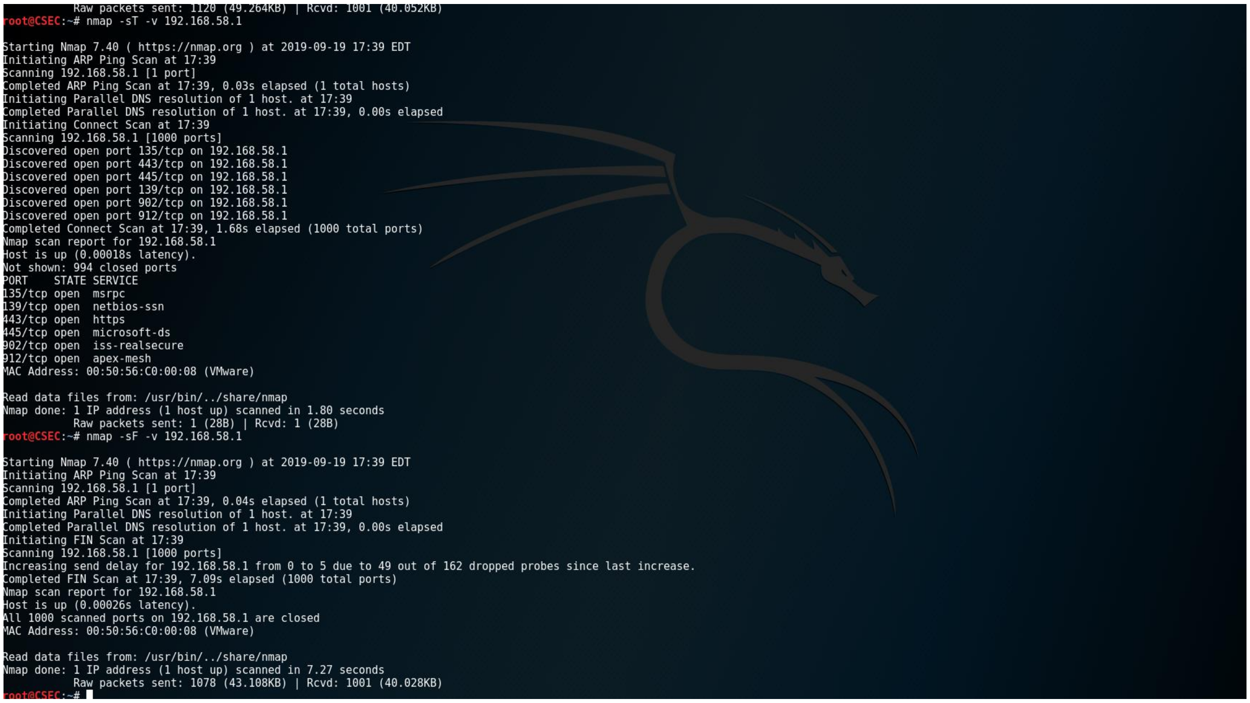
(10 p) screenshots or the actual text of the output from each nmap command listed and used

SYN Scan



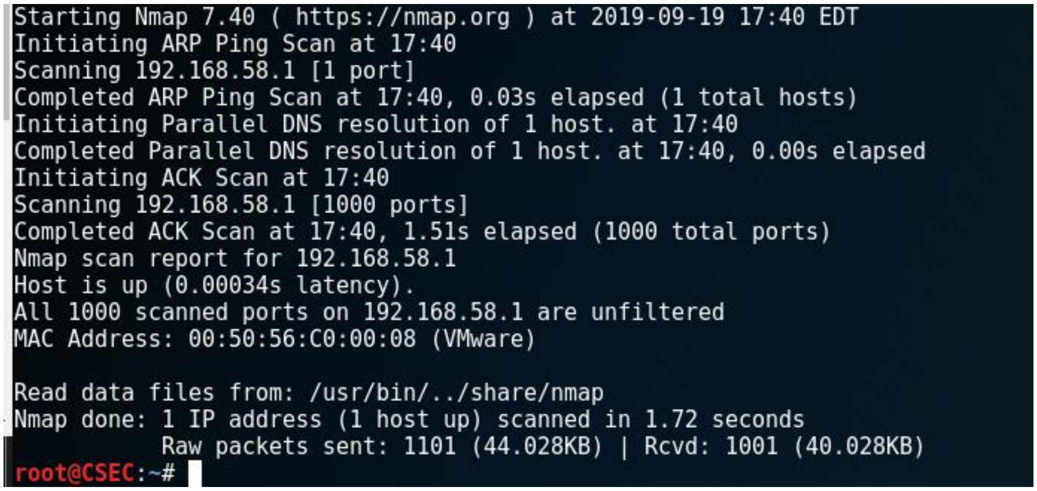
```
oot@CSEC:~# nmap -sS -v 192.168.58.1

tarting Nmap 7.40 ( https://nmap.org ) at 2019-09-19 17:37 EDT
nitiating ARP Ping Scan at 17:37
canning 192.168.58.1 [1 port]
ompleted ARP Ping Scan at 17:37, 0.05s elapsed (1 total hosts)
nitiating Parallel DNS resolution of 1 host. at 17:37
ompleted Parallel DNS resolution of 1 host. at 17:37, 0.00s elapsed
nitiating SYN Stealth Scan at 17:37
canning 192.168.58.1 [1000 ports]
iscovered open port 139/tcp on 192.168.58.1
iscovered open port 445/tcp on 192.168.58.1
iscovered open port 443/tcp on 192.168.58.1
iscovered open port 135/tcp on 192.168.58.1
iscovered open port 902/tcp on 192.168.58.1
iscovered open port 912/tcp on 192.168.58.1
ompleted SYN Stealth Scan at 17:37, 1.60s elapsed (1000 total ports)
map scan report for 192.168.58.1
ost is up (0.00049s latency).
ot shown: 994 closed ports
ORT    STATE SERVICE
35/tcp open  msrpc
39/tcp open  netbios-ssn
43/tcp open  https
45/tcp open  microsoft-ds
02/tcp open  iss-realsecure
12/tcp open  apex-mesh
AC Address: 00:50:56:C0:00:08 (VMware)

ead data files from: /usr/bin/../share/nmap
map done: 1 IP address (1 host up) scanned in 1.87 seconds
          Raw packets sent: 1120 (49.264KB) | Rcvd: 1001 (40.052KB)
```

Connect Scan and FIN Scan



```
          Raw packets sent: 1120 (49.264KB) | Rcvd: 1001 (40.052KB)
root@CSEC:~# nmap -sT -v 192.168.58.1

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-19 17:39 EDT
Initiating ARP Ping Scan at 17:39
Scanning 192.168.58.1 [1 port]
Completed ARP Ping Scan at 17:39, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:39
Completed Parallel DNS resolution of 1 host. at 17:39, 0.00s elapsed
Initiating Connect Scan at 17:39
Scanning 192.168.58.1 [1000 ports]
Discovered open port 135/tcp on 192.168.58.1
Discovered open port 443/tcp on 192.168.58.1
Discovered open port 445/tcp on 192.168.58.1
Discovered open port 139/tcp on 192.168.58.1
Discovered open port 902/tcp on 192.168.58.1
Discovered open port 912/tcp on 192.168.58.1
Completed Connect Scan at 17:39, 1.68s elapsed (1000 total ports)
Nmap scan report for 192.168.58.1
Host is up (0.00018s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 00:50:56:C0:00:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.80 seconds
          Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
root@CSEC:~# nmap -sF -v 192.168.58.1

Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-19 17:39 EDT
Initiating ARP Ping Scan at 17:39
Scanning 192.168.58.1 [1 port]
Completed ARP Ping Scan at 17:39, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:39
Completed Parallel DNS resolution of 1 host. at 17:39, 0.00s elapsed
Initiating FIN Scan at 17:39
Scanning 192.168.58.1 [1000 ports]
Increasing send delay for 192.168.58.1 from 0 to 5 due to 49 out of 162 dropped probes since last increase.
Completed FIN Scan at 17:39, 7.09s elapsed (1000 total ports)
Nmap scan report for 192.168.58.1
Host is up (0.00026s latency).
All 1000 scanned ports on 192.168.58.1 are closed
MAC Address: 00:50:56:C0:00:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.27 seconds
          Raw packets sent: 1078 (43.108KB) | Rcvd: 1001 (40.028KB)
root@CSEC:~# 
```

ACK Scan:

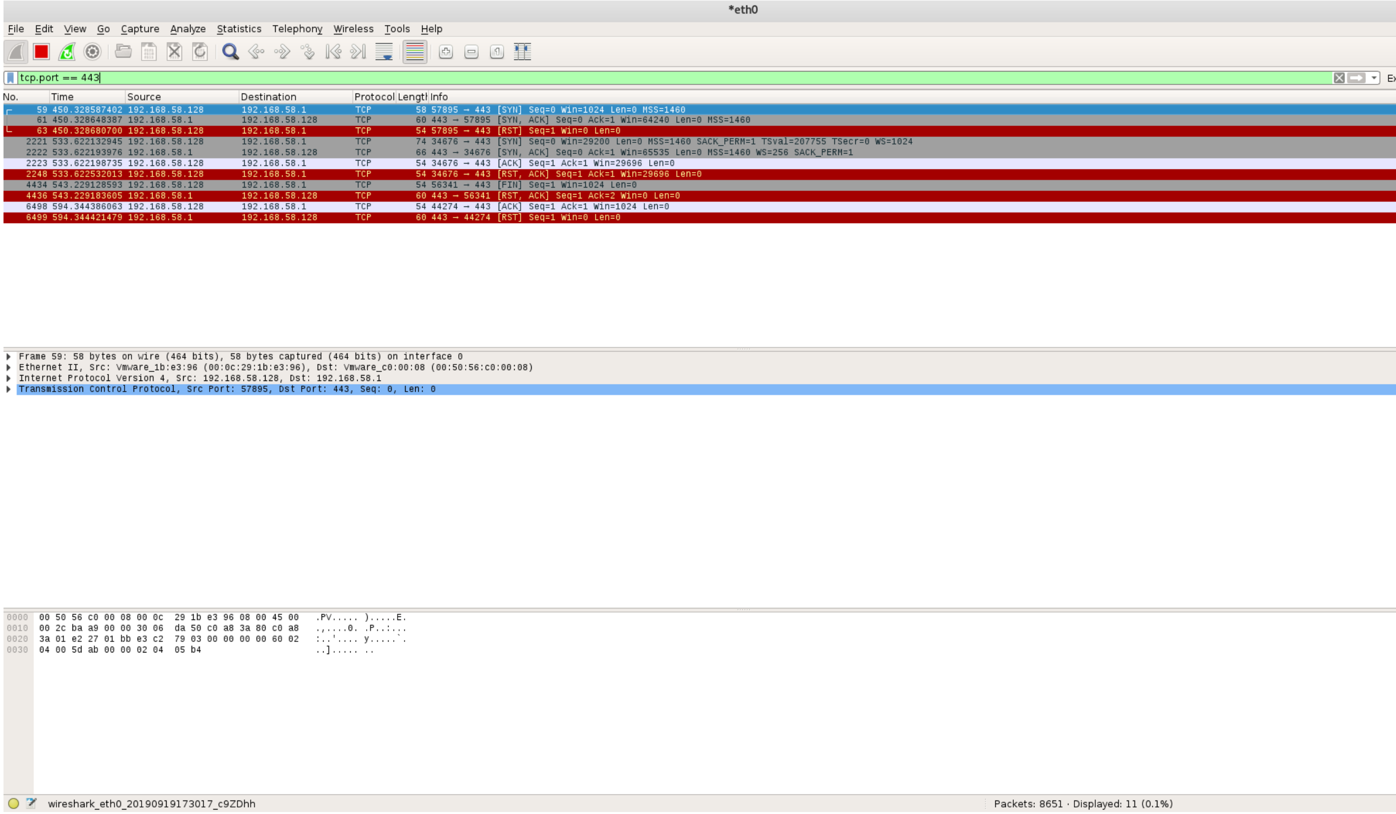


```
Starting Nmap 7.40 ( https://nmap.org ) at 2019-09-19 17:40 EDT
Initiating ARP Ping Scan at 17:40
Scanning 192.168.58.1 [1 port]
Completed ARP Ping Scan at 17:40, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:40
Completed Parallel DNS resolution of 1 host. at 17:40, 0.00s elapsed
Initiating ACK Scan at 17:40
Scanning 192.168.58.1 [1000 ports]
Completed ACK Scan at 17:40, 1.51s elapsed (1000 total ports)
Nmap scan report for 192.168.58.1
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.58.1 are unfiltered
MAC Address: 00:50:56:C0:00:08 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.72 seconds
           Raw packets sent: 1101 (44.028KB) | Rcvd: 1001 (40.028KB)
root@CSEC:~# 
```

(5 p) Identify the ports open and closed, listed in the nmap command output

The list of the ports with their name, state and service is present in the cmd. We can check the status of the port to see if it is open or closed.

(10 p) screenshots of cropped Wireshark captures showing the network traffic of the one of the single ports identified in the previous step for open status and one for closed status



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 443

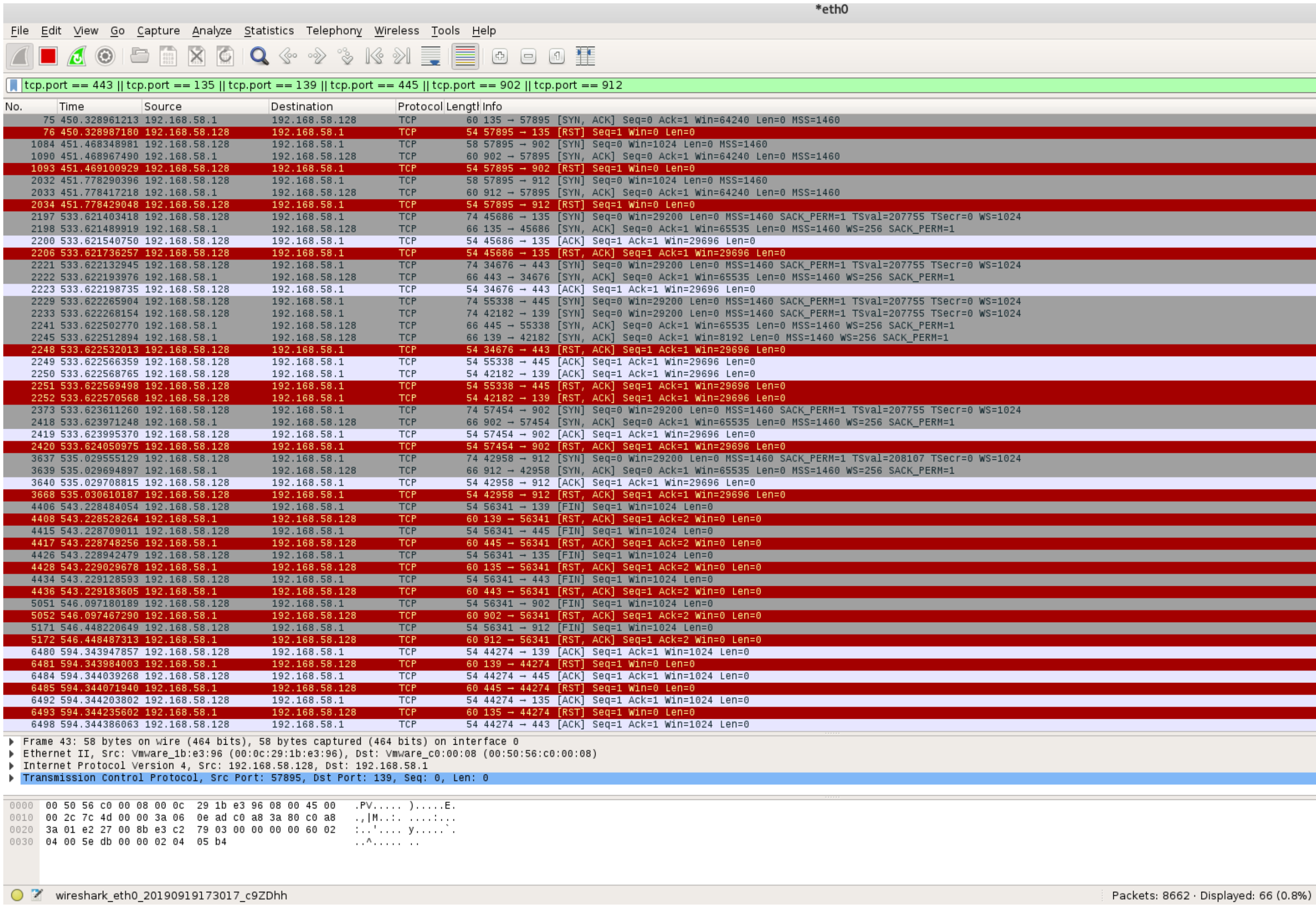
```
No.   Time          Source          Destination     Protocol Lengtl Info
   59 450.328587402 192.168.58.128  192.168.58.1    TCP      58 57895 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
   61 450.328648387 192.168.58.1    192.168.58.128  TCP      60 443 → 57895 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   63 450.328680700 192.168.58.128  192.168.58.1    TCP      54 57895 → 443 [RST] Seq=1 Win=0 Len=0
 2221 533.622132945 192.168.58.128  192.168.58.1    TCP      74 34676 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2222 533.622193976 192.168.58.1    192.168.58.128  TCP      66 443 → 34676 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2223 533.622198735 192.168.58.128  192.168.58.1    TCP      54 34676 → 443 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2248 533.622532013 192.168.58.128  192.168.58.1    TCP      54 34676 → 443 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 4434 543.229128593 192.168.58.128  192.168.58.1    TCP      54 56341 → 443 [FIN] Seq=1 Win=1024 Len=0
 4436 543.229183605 192.168.58.1    192.168.58.128  TCP      60 443 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 6498 594.344386063 192.168.58.128  192.168.58.1    TCP      54 44274 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
 6499 594.344421479 192.168.58.1    192.168.58.128  TCP      60 443 → 44274 [RST] Seq=1 Win=0 Len=0
```

```
▸ Frame 59: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
▸ Ethernet II, Src: Vmware_1b:e3:96 (00:0c:29:1b:e3:96), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
▸ Internet Protocol Version 4, Src: 192.168.58.128, Dst: 192.168.58.1
▸ Transmission Control Protocol, Src Port: 57895, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  00 50 56 c0 00 08 00 0c  29 1b e3 96 08 00 45 00   .PV..... ).....E.
0010  00 2c ba a9 00 00 30 06  da 50 c0 a8 3a 80 c0 a8   .,....0. .P..:...
0020  3a 01 e2 27 01 bb e3 c2  79 03 00 00 00 00 60 02   :..'.... y.....`.
0030  04 00 5d ab 00 00 02 04  05 b4                     ..]..... ..
```

wireshark_eth0_20190919173017_c9ZDhh

Packets: 8651 · Displayed: 11 (0.1%)


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port == 443 || tcp.port == 135 || tcp.port == 139 || tcp.port == 445 || tcp.port == 902 || tcp.port == 912

No.   Time           Source         Destination    Protocol Lengtl Info
   75 450.328961213 192.168.58.1   192.168.58.128  TCP      60 135 → 57895 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
   76 450.328987180 192.168.58.128 192.168.58.1    TCP      54 57895 → 135 [RST] Seq=1 Win=0 Len=0
 1084 451.468348981 192.168.58.128 192.168.58.1    TCP      58 57895 → 902 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 1090 451.468967490 192.168.58.1   192.168.58.128  TCP      60 902 → 57895 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 1093 451.469100929 192.168.58.128 192.168.58.1    TCP      54 57895 → 902 [RST] Seq=1 Win=0 Len=0
 2032 451.778290396 192.168.58.128 192.168.58.1    TCP      58 57895 → 912 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2033 451.778417218 192.168.58.1   192.168.58.128  TCP      60 912 → 57895 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 2034 451.778429048 192.168.58.128 192.168.58.1    TCP      54 57895 → 912 [RST] Seq=1 Win=0 Len=0
 2197 533.621403418 192.168.58.128 192.168.58.1    TCP      74 45686 → 135 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2198 533.621489919 192.168.58.1   192.168.58.128  TCP      66 135 → 45686 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2200 533.621540750 192.168.58.128 192.168.58.1    TCP      54 45686 → 135 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2206 533.621736257 192.168.58.128 192.168.58.1    TCP      54 45686 → 135 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 2221 533.622132945 192.168.58.128 192.168.58.1    TCP      74 34676 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2222 533.622193976 192.168.58.1   192.168.58.128  TCP      66 443 → 34676 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2223 533.622198735 192.168.58.128 192.168.58.1    TCP      54 34676 → 443 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2229 533.622265904 192.168.58.128 192.168.58.1    TCP      74 55338 → 445 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2233 533.622268154 192.168.58.128 192.168.58.1    TCP      74 42182 → 139 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2241 533.622502770 192.168.58.1   192.168.58.128  TCP      66 445 → 55338 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2245 533.622512894 192.168.58.1   192.168.58.128  TCP      66 139 → 42182 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2248 533.622532013 192.168.58.128 192.168.58.1    TCP      54 34676 → 443 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 2249 533.622566359 192.168.58.128 192.168.58.1    TCP      54 55338 → 445 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2250 533.622568765 192.168.58.128 192.168.58.1    TCP      54 42182 → 139 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2251 533.622569498 192.168.58.128 192.168.58.1    TCP      54 55338 → 445 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 2252 533.622570568 192.168.58.128 192.168.58.1    TCP      54 42182 → 139 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 2373 533.623611260 192.168.58.128 192.168.58.1    TCP      74 57454 → 902 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=207755 TSecr=0 WS=1024
 2418 533.623971248 192.168.58.1   192.168.58.128  TCP      66 902 → 57454 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2419 533.623995370 192.168.58.128 192.168.58.1    TCP      54 57454 → 902 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 2420 533.624050975 192.168.58.128 192.168.58.1    TCP      54 57454 → 902 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 3637 535.029555129 192.168.58.128 192.168.58.1    TCP      74 42958 → 912 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=208107 TSecr=0 WS=1024
 3639 535.029694897 192.168.58.1   192.168.58.128  TCP      66 912 → 42958 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3640 535.029708815 192.168.58.128 192.168.58.1    TCP      54 42958 → 912 [ACK] Seq=1 Ack=1 Win=29696 Len=0
 3668 535.030610187 192.168.58.128 192.168.58.1    TCP      54 42958 → 912 [RST, ACK] Seq=1 Ack=1 Win=29696 Len=0
 4406 543.228484054 192.168.58.128 192.168.58.1    TCP      54 56341 → 139 [FIN] Seq=1 Win=1024 Len=0
 4408 543.228528264 192.168.58.1   192.168.58.128  TCP      60 139 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 4415 543.228709011 192.168.58.128 192.168.58.1    TCP      54 56341 → 445 [FIN] Seq=1 Win=1024 Len=0
 4417 543.228748256 192.168.58.1   192.168.58.128  TCP      60 445 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 4426 543.228942479 192.168.58.128 192.168.58.1    TCP      54 56341 → 135 [FIN] Seq=1 Win=1024 Len=0
 4428 543.229029678 192.168.58.1   192.168.58.128  TCP      60 135 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 4434 543.229128593 192.168.58.128 192.168.58.1    TCP      54 56341 → 443 [FIN] Seq=1 Win=1024 Len=0
 4436 543.229183605 192.168.58.1   192.168.58.128  TCP      60 443 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 5051 546.097180189 192.168.58.128 192.168.58.1    TCP      54 56341 → 902 [FIN] Seq=1 Win=1024 Len=0
 5052 546.097467290 192.168.58.1   192.168.58.128  TCP      60 902 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 5171 546.448220649 192.168.58.128 192.168.58.1    TCP      54 56341 → 912 [FIN] Seq=1 Win=1024 Len=0
 5172 546.448487313 192.168.58.1   192.168.58.128  TCP      60 912 → 56341 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
 6480 594.343947857 192.168.58.128 192.168.58.1    TCP      54 44274 → 139 [ACK] Seq=1 Ack=1 Win=1024 Len=0
 6481 594.343984003 192.168.58.1   192.168.58.128  TCP      60 139 → 44274 [RST] Seq=1 Win=0 Len=0
 6484 594.344039268 192.168.58.128 192.168.58.1    TCP      54 44274 → 445 [ACK] Seq=1 Ack=1 Win=1024 Len=0
 6485 594.344071940 192.168.58.1   192.168.58.128  TCP      60 445 → 44274 [RST] Seq=1 Win=0 Len=0
 6492 594.344203802 192.168.58.128 192.168.58.1    TCP      54 44274 → 135 [ACK] Seq=1 Ack=1 Win=1024 Len=0
 6493 594.344235602 192.168.58.1   192.168.58.128  TCP      60 135 → 44274 [RST] Seq=1 Win=0 Len=0
 6498 594.344386063 192.168.58.128 192.168.58.1    TCP      54 44274 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0

▶ Frame 43: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
▶ Ethernet II, Src: Vmware_1b:e3:96 (00:0c:29:1b:e3:96), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
▶ Internet Protocol Version 4, Src: 192.168.58.128, Dst: 192.168.58.1
▶ Transmission Control Protocol, Src Port: 57895, Dst Port: 139, Seq: 0, Len: 0

0000  00 50 56 c0 00 08 00 0c  29 1b e3 96 08 00 45 00   .PV..... ).....E.
0010  00 2c 7c 4d 00 00 3a 06  0e ad c0 a8 3a 80 c0 a8   .,|M..:. ....:...
0020  3a 01 e2 27 00 8b e3 c2  79 03 00 00 00 00 60 02   :..'.... y.....`.
0030  04 00 5e db 00 00 02 04  05 b4                     ..^..... ..

wireshark_eth0_20190919173017_c9ZDhh                     Packets: 8662 · Displayed: 66 (0.8%)
```

Activity 4 – Port scanning method analysis

(20p) In your lab report you must include an explanation describing how each port scanning works, for each of the nmap command listed and used in the previous step (a.) of Activity 2.

TCP SYN Scan: TCP SYN scan sends a SYN packet to initiate a 3way handshake to every port of the server. TCP SYN scan is used when malicious hacker needs to determine the state of the port without establishing a full connection.

TCP connect Scan: TCP Connect Scan works like TCP SYN scan but instead of RST it sends ACK to establish a connection and then sends resets packet. It used when privileged access isn't available.

TCP FIN scan: TCP FIN scan sends a FIN packet without establishing a TCP connection. This scan is quiet and does not appears in any system logs.

FIN SCAN: A windows device will always send a RST frame for all the queries regardless of the status of port, whereas Linux device will not send anything if the port is open and send RST packet if port is closed.

IF open| filtered is appeared during FIN scan this means that the machine is not a windows machine.

(10p) In your lab report you must include an explanation describing how SYN and Connect port scanning methods differ, and when you would use each.

SYN and CONNECT Scans are two very different scans, SYN is a more stealthy and quieter method, where it leaves no logs and doesn't complete a full 3 way handshake of TCP whereas CONNECT is a louder method where it completes a TCP handshake to gather information, leaving logs. The SYN scan requires privileged access whereas the CONNECT scan can be performed without privileged access by any user. You would use a SYN scan as the primary scan to gather information about ports when you have privileged access and because it works across all operating systems whereas the CONNECT scan should be used as a last resort if privileged access isn't available

(10p) In your lab report you must include an explanation describing how FIN and ACK port scanning methods can be used in combination with each other.

FIN and ACK scans can be used in conjunction as the ACK scan tells us whether a port is filtered or unfiltered and the FIN scan tells us if the port is Closed or Open/Filtered. That way we can identify exactly which port is closed, which is open and which port has a firewall that is blocking the scans. This information can be very valuable for future scans that can specifically investigate those certain ports.

(10p) In your lab report you must include an explanation describing the differences between an open port, a closed port, and a filtered port, referencing your Nmap commands used in the previous step (a.) of Activity 2.

An open port is a vulnerable port. This port actively replies to every SYN and ACK request sent its way and tells the source everything it need to know about that port. If an important port is left open, then it can be used to attack the system. A closed port also gives information to the user, but not complete information, it just sends an RST when a SYN is sent towards it. This helps the scanner identify which ports have been closed. A filtered port is one which might be open or close, but the scanner cannot know the condition of that port because the filter drops any replies sent by the system to the scanner.