NSSII Assignment 1

Manavjeet Singh, 2018295

Introduction

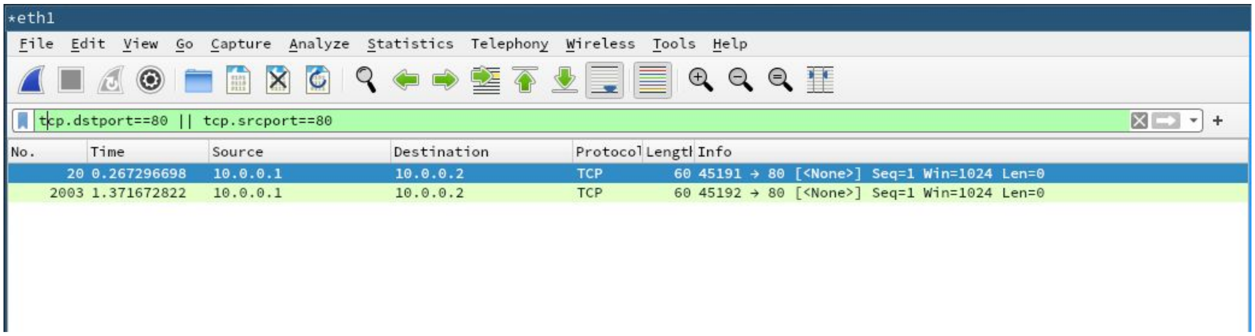
VM1: 10.0.0.1/24 (eth1)
VM2: 10.0.0.2/24 (eth1)

The kernel module is loaded on VM2 and VM1 uses nmap TCP null, Xmas and Fin scans on VM2.
There is a HTTP server running on port 80 of VM2.

Scan Detection

Null scan

In a null scan nmap sends TCP packets to the most popular 1000 ports without any flag being set in it’s header.
This scan can be detected in pre-routing by reading the packet header and making sure that not a single flag is set.
For an open port the packet is simply dropped, thus in this scan nmap is not able to differentiate between an open or filtered port. And for a closed port a RST, ACK packet is returned. Same is visible in the screenshot below.

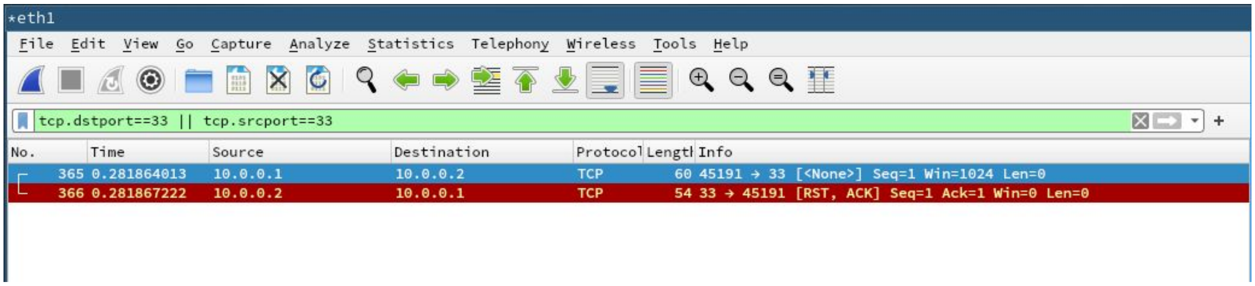


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport==80 || tcp.srcport==80
```

No.	Time	Source	Destination	Protocol	Length	Info
20	0.267296698	10.0.0.1	10.0.0.2	TCP	60	45191 → 80 [<None>] Seq=1 Win=1024 Len=0
2003	1.371672822	10.0.0.1	10.0.0.2	TCP	60	45192 → 80 [<None>] Seq=1 Win=1024 Len=0

For an open port 80

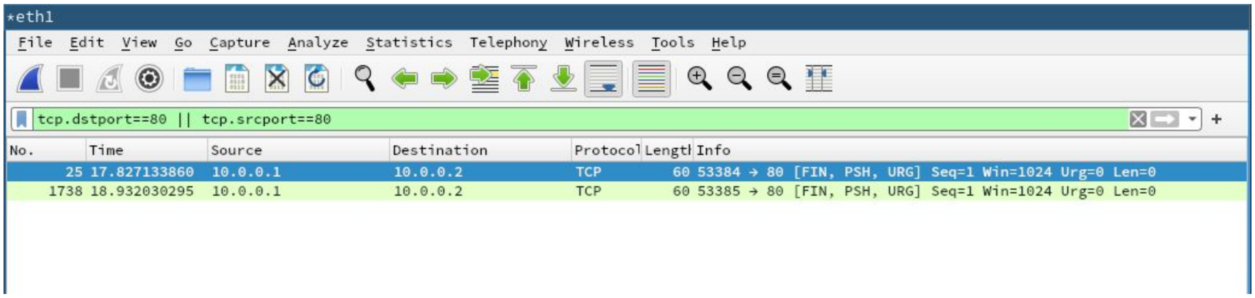

*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport==33 || tcp.srcport==33

No.   Time         Source     Destination  Protocol Length Info
  365 0.281864013  10.0.0.1   10.0.0.2     TCP      60 45191 → 33 [<None>] Seq=1 Win=1024 Len=0
  366 0.281867222  10.0.0.2   10.0.0.1     TCP      54 33 → 45191 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

For a closed port 33

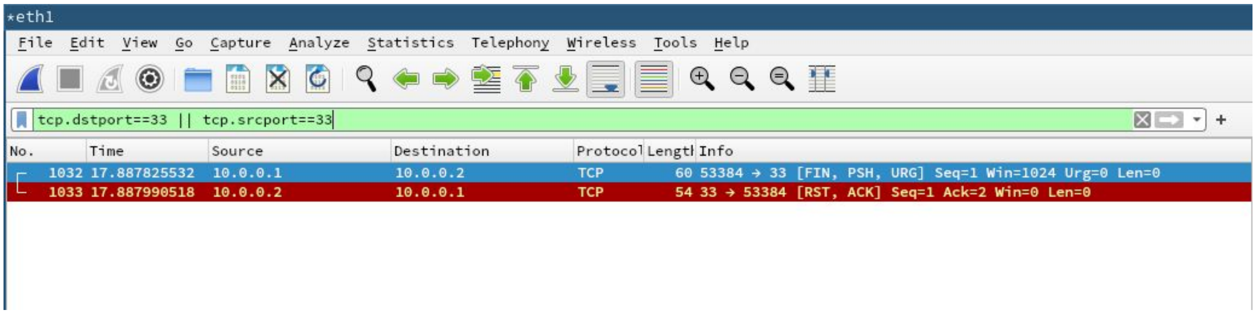
Xmas scan

In Xmas scan, nmap sends TCP packets to the most popular 1000 ports with the FIN, PSH, and URG flags set. According to nmap man page, “lighting the packet up like a Christmas tree”. This scan can be detected in pre-routing by reading the packet header and making sure that FIN, PSH and URG flags are set.
Same as null scan, for an open port the packet is simply dropped, thus in this scan nmap is not able to differentiate between an open or filtered port. And for a closed port a RST, ACK packet is returned. Same is visible in the screenshot below.


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport==80 || tcp.srcport==80

No.   Time          Source     Destination  Protocol Length Info
   25 17.827133860  10.0.0.1   10.0.0.2     TCP      60 53384 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1738 18.932030295  10.0.0.1   10.0.0.2     TCP      60 53385 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
```

For an open port 80


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

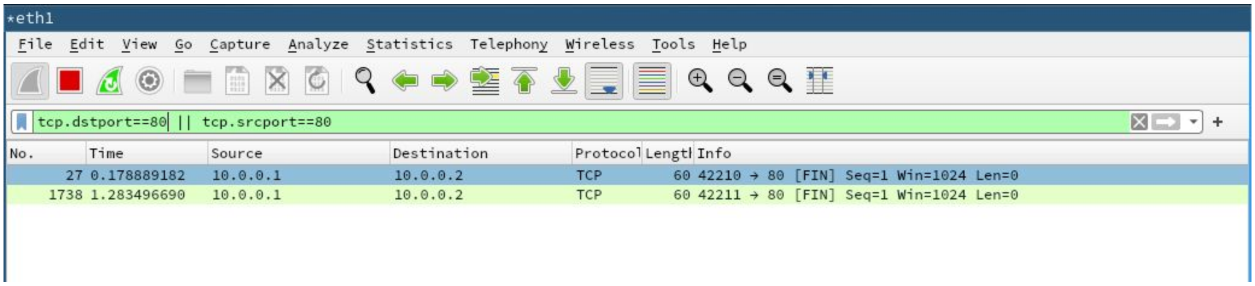
```
tcp.dstport==33 || tcp.srcport==33

No.   Time          Source     Destination  Protocol Length Info
 1032 17.887825532  10.0.0.1   10.0.0.2     TCP      60 53384 → 33 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
 1033 17.887990518  10.0.0.2   10.0.0.1     TCP      54 33 → 53384 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
```

For a closed port 33

Fin Scan

In Fin scan nmap sends TCP packets to the most popular 1000 ports with FIN flag set.
This scan can be detected in pre-routing by reading the packet header and making sure that only the FIN flag is set.

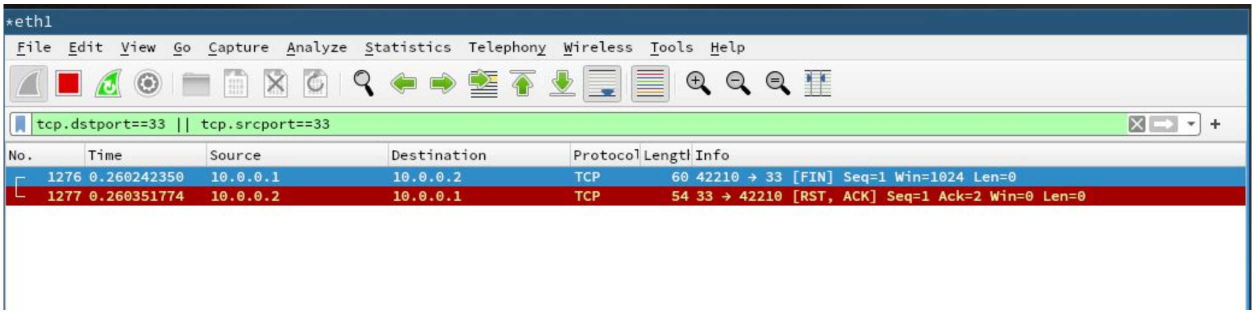
Same as null scan and xmas scan, for an open port the packet is simply dropped, thus in this scan nmap is not able to differentiate between an open or filtered port. And for a closed port a RST, ACK packet is returned. Same is visible in the screenshot below.


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.dstport==80 || tcp.srcport==80
```

No.	Time	Source	Destination	Protocol	Length	Info
27	0.178889182	10.0.0.1	10.0.0.2	TCP	60	42210 → 80 [FIN] Seq=1 Win=1024 Len=0
1738	1.283496690	10.0.0.1	10.0.0.2	TCP	60	42211 → 80 [FIN] Seq=1 Win=1024 Len=0

For an open port 80


*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

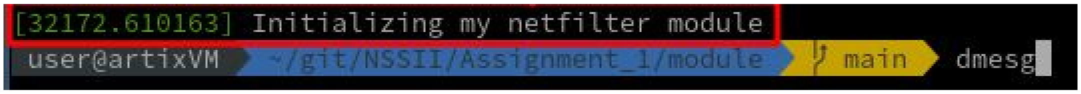
```
tcp.dstport==33 || tcp.srcport==33
```

No.	Time	Source	Destination	Protocol	Length	Info
1276	0.260242350	10.0.0.1	10.0.0.2	TCP	60	42210 → 33 [FIN] Seq=1 Win=1024 Len=0
1277	0.260351774	10.0.0.2	10.0.0.1	TCP	54	33 → 42210 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

For a closed port 33

Running

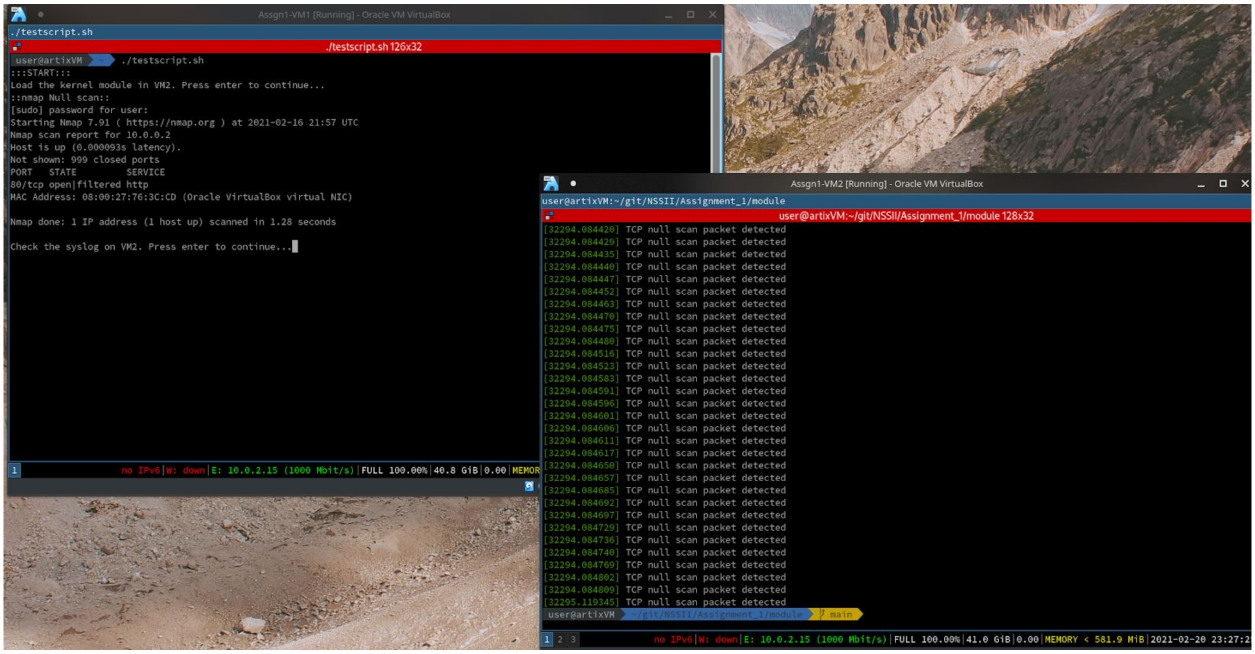
- Run ./testscript.sh on VM1
- Load kernel module on VM2 using command `make insert` in module directory.
- Use command dmesg to check if the module is loaded.



```
[32172.610163] Initializing my netfilter module
 user@artixVM  ~/git/NSSII/Assignment_1/module  main  dmesg
```

- Press enter on VM1 to initiate nmap commands.

- After every nmap scan check dmesg on VM2 and press enter on VM1 for next scan.

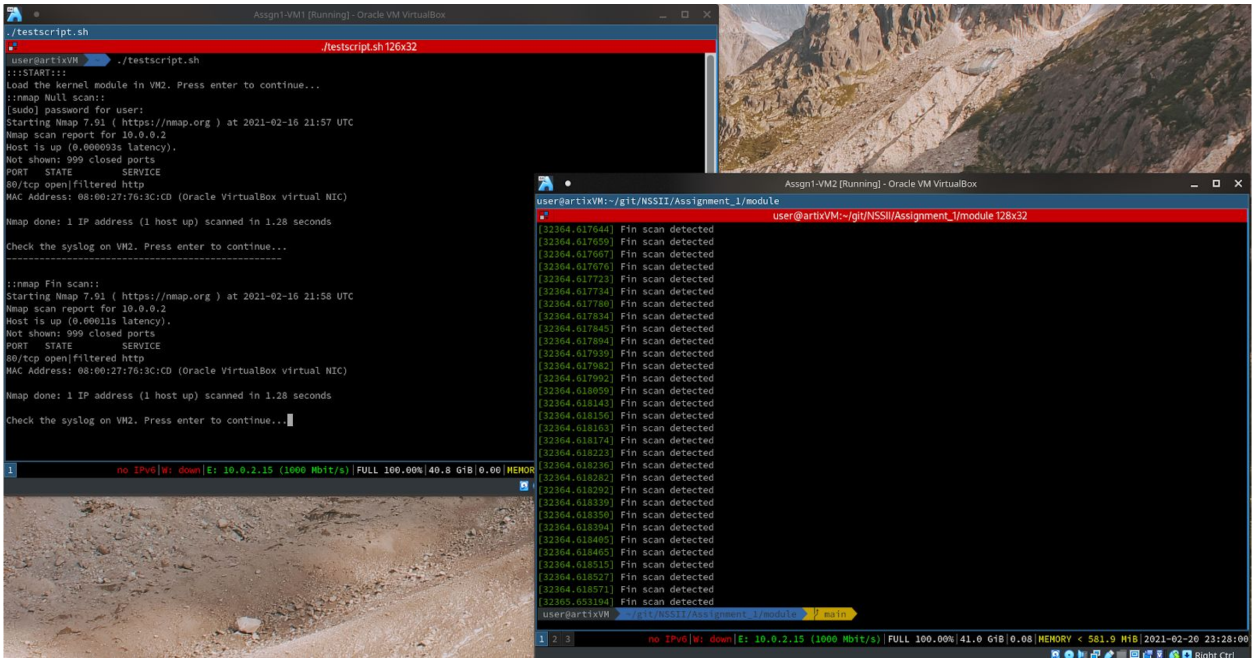

Assgn1-VM1 [Running] - Oracle VM VirtualBox
./testscript.sh
./testscript.sh 126x32
Assgn1-VM2 [Running] - Oracle VM VirtualBox
user@artixVM:~/git/NSSII/Assignment_1/module
user@artixVM:~/git/NSSII/Assignment_1/module 128x32

```
user@artixVM  ~  ./testscript.sh
:::START:::
Load the kernel module in VM2. Press enter to continue...
::nmap Null scan::
[sudo] password for user:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 21:57 UTC
Nmap scan report for 10.0.0.2
Host is up (0.000093s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:76:3C:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

Check the syslog on VM2. Press enter to continue...
```

```
1            no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|40.8 GiB|0.00|MEMOR
```

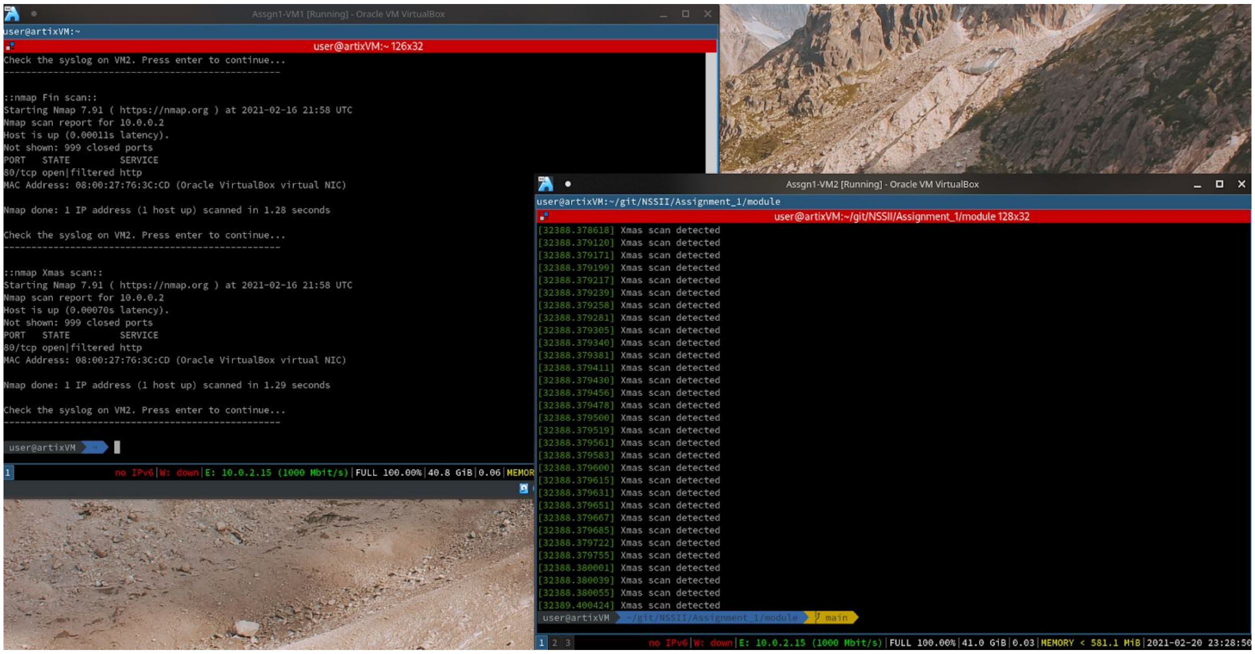
```
[32294.084420] TCP null scan packet detected
[32294.084429] TCP null scan packet detected
[32294.084435] TCP null scan packet detected
[32294.084440] TCP null scan packet detected
[32294.084447] TCP null scan packet detected
[32294.084452] TCP null scan packet detected
[32294.084463] TCP null scan packet detected
[32294.084470] TCP null scan packet detected
[32294.084475] TCP null scan packet detected
[32294.084480] TCP null scan packet detected
[32294.084516] TCP null scan packet detected
[32294.084523] TCP null scan packet detected
[32294.084583] TCP null scan packet detected
[32294.084591] TCP null scan packet detected
[32294.084596] TCP null scan packet detected
[32294.084601] TCP null scan packet detected
[32294.084606] TCP null scan packet detected
[32294.084611] TCP null scan packet detected
[32294.084617] TCP null scan packet detected
[32294.084650] TCP null scan packet detected
[32294.084657] TCP null scan packet detected
[32294.084685] TCP null scan packet detected
[32294.084692] TCP null scan packet detected
[32294.084697] TCP null scan packet detected
[32294.084729] TCP null scan packet detected
[32294.084736] TCP null scan packet detected
[32294.084740] TCP null scan packet detected
[32294.084769] TCP null scan packet detected
[32294.084802] TCP null scan packet detected
[32294.084809] TCP null scan packet detected
[32295.119345] TCP null scan packet detected
user@artixVM  ~/git/NSSII/Assignment_1/module  main
```

```
1 2 3         no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|41.0 GiB|0.00|MEMORY < 581.9 MiB|2021-02-20 23:27:2
```


Assgn1-VM1 [Running] - Oracle VM VirtualBox
./testscript.sh
./testscript.sh 126x32
Assgn1-VM2 [Running] - Oracle VM VirtualBox
user@artixVM:~/git/NSSII/Assignment_1/module
user@artixVM:~/git/NSSII/Assignment_1/module 128x32
Right Ctrl

```
user@artixVM  ./testscript.sh
:::START:::
Load the kernel module in VM2. Press enter to continue...
::nmap Null scan::
[sudo] password for user:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 21:57 UTC
Nmap scan report for 10.0.0.2
Host is up (0.000093s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:76:3C:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

Check the syslog on VM2. Press enter to continue...
--------------------------------------------------

::nmap Fin scan::
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 21:58 UTC
Nmap scan report for 10.0.0.2
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:76:3C:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

Check the syslog on VM2. Press enter to continue...

1          no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|40.8 GiB|0.00|MEMOR
```

```
[32364.617644] Fin scan detected
[32364.617659] Fin scan detected
[32364.617667] Fin scan detected
[32364.617676] Fin scan detected
[32364.617723] Fin scan detected
[32364.617734] Fin scan detected
[32364.617780] Fin scan detected
[32364.617834] Fin scan detected
[32364.617845] Fin scan detected
[32364.617894] Fin scan detected
[32364.617939] Fin scan detected
[32364.617982] Fin scan detected
[32364.617992] Fin scan detected
[32364.618059] Fin scan detected
[32364.618143] Fin scan detected
[32364.618156] Fin scan detected
[32364.618163] Fin scan detected
[32364.618174] Fin scan detected
[32364.618223] Fin scan detected
[32364.618236] Fin scan detected
[32364.618282] Fin scan detected
[32364.618292] Fin scan detected
[32364.618339] Fin scan detected
[32364.618350] Fin scan detected
[32364.618394] Fin scan detected
[32364.618405] Fin scan detected
[32364.618465] Fin scan detected
[32364.618515] Fin scan detected
[32364.618527] Fin scan detected
[32364.618571] Fin scan detected
[32365.653194] Fin scan detected
user@artixVM  ~/git/NSSII/Assignment_1/module  main

1 2 3      no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|41.0 GiB|0.08|MEMORY < 581.9 MiB|2021-02-20 23:28:00
```


Assgn1-VM1 [Running] - Oracle VM VirtualBox
user@artixVM:~
user@artixVM:~ 126x32
Assgn1-VM2 [Running] - Oracle VM VirtualBox
user@artixVM:~/git/NSSII/Assignment_1/module
user@artixVM:~/git/NSSII/Assignment_1/module 128x32

```
Check the syslog on VM2. Press enter to continue...
--------------------------------------------------

::nmap Fin scan::
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 21:58 UTC
Nmap scan report for 10.0.0.2
Host is up (0.00011s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:76:3C:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds

Check the syslog on VM2. Press enter to continue...
--------------------------------------------------

::nmap Xmas scan::
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-16 21:58 UTC
Nmap scan report for 10.0.0.2
Host is up (0.00070s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: 08:00:27:76:3C:CD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds

Check the syslog on VM2. Press enter to continue...
--------------------------------------------------

user@artixVM  ~ 

1          no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|40.8 GiB|0.06|MEMOR
```

```
[32388.378618] Xmas scan detected
[32388.379120] Xmas scan detected
[32388.379171] Xmas scan detected
[32388.379199] Xmas scan detected
[32388.379217] Xmas scan detected
[32388.379239] Xmas scan detected
[32388.379258] Xmas scan detected
[32388.379281] Xmas scan detected
[32388.379305] Xmas scan detected
[32388.379340] Xmas scan detected
[32388.379381] Xmas scan detected
[32388.379411] Xmas scan detected
[32388.379430] Xmas scan detected
[32388.379456] Xmas scan detected
[32388.379478] Xmas scan detected
[32388.379500] Xmas scan detected
[32388.379519] Xmas scan detected
[32388.379561] Xmas scan detected
[32388.379583] Xmas scan detected
[32388.379600] Xmas scan detected
[32388.379615] Xmas scan detected
[32388.379631] Xmas scan detected
[32388.379651] Xmas scan detected
[32388.379667] Xmas scan detected
[32388.379685] Xmas scan detected
[32388.379722] Xmas scan detected
[32388.379755] Xmas scan detected
[32388.380001] Xmas scan detected
[32388.380039] Xmas scan detected
[32388.380055] Xmas scan detected
[32389.400424] Xmas scan detected
user@artixVM  ~/git/NSSII/Assignment_1/module  main

1 2 3      no IPv6|W: down|E: 10.0.2.15 (1000 Mbit/s)|FULL 100.00%|41.0 GiB|0.03|MEMORY < 581.1 MiB|2021-02-20 23:28:50
```

- Remove the module from VM2 using make remove.

References

https://blog.sourcerer.io/writing-a-simple-linux-kernel-module-d9dc3762c234: Writing the hook https://linux.die.net/man/1/nmap: nmap man page

https://github.com/baiwei0427/coding-examples/blob/master/ipip/ipip_tcp.c: Examples

https://elixir.bootlin.com/linux/latest/source/include/linux/tcp.h: TCP opt_len function

https://www.tweaking4all.com/software/linux-software/bash-press-any-key/: Help in test script