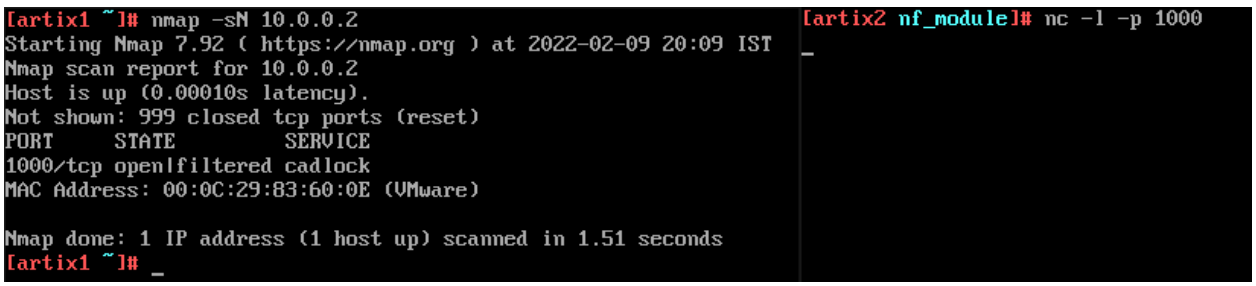
Networks and Systems Security II
Assignment 1

Name: Harsh Kumar **Roll No:** 2019043

Setup

machine:	*hostname*	*IP Address(es)*
VM1:	artix1	10.0.0.1
VM2:	artix2	10.0.0.2, 20.0.0.1

To test the connection, and working *nmap*, I created a socket on *port 1000* on VM2. After this, I ran *nmap* from VM1.



Observation: nmap is able to find that port 1000 is open on VM2.

Netfilter kernel module design

I'm focusing on detecting these scans, by their corresponding TCP header flags. If flags match with any of these given flag values, we drop that packet and log a message in the kernel.

```
Null scan (-sN)

    Does not set any bits (TCP flag header is 0)

FIN scan (-sF)

    Sets just the TCP FIN bit.

Xmas scan (-sX)

    Sets the FIN, PSH, and URG flags, lighting the packet up like a
    Christmas tree.
```

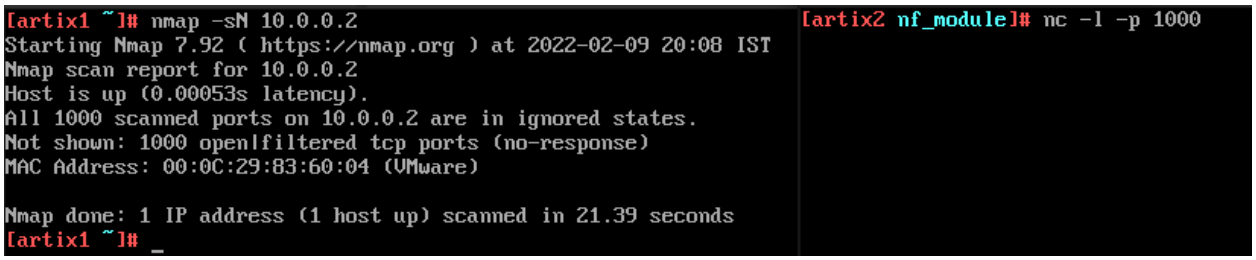
static int __init LKM_init(void) : This function initializes the Netfilter hook. The hook that I am using is the *PRE_ROUTING* stage. This module will run on incoming packets to the machine.

static unsigned int hfunc(void *, struct sk_buff *, const struct nf_hook_state *) : Each time a packet enters the pre-routing stage, this function is called for the sk_buff structure corresponding to that packet in the kernel.

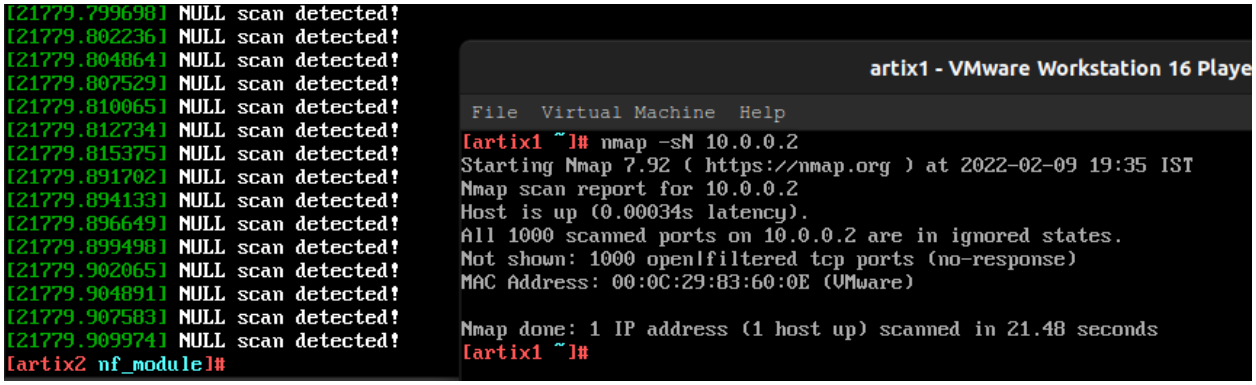
Here, we first extract the IP header from the *sk_buff* structure of the packet. All the reconnaissance scans that we are detecting are TCP-based. Thus, we check if the protocol for the packet is TCP. If yes, we proceed further and extract the TCP headers of the packet. If the header bits match any of the reconnaissance packets headers, we log this event in the kernel and drop the packet by returning *NF_DROP*. For the rest of the packets, we return NF_ACCEPT.

Screenshots

NULL Scan:

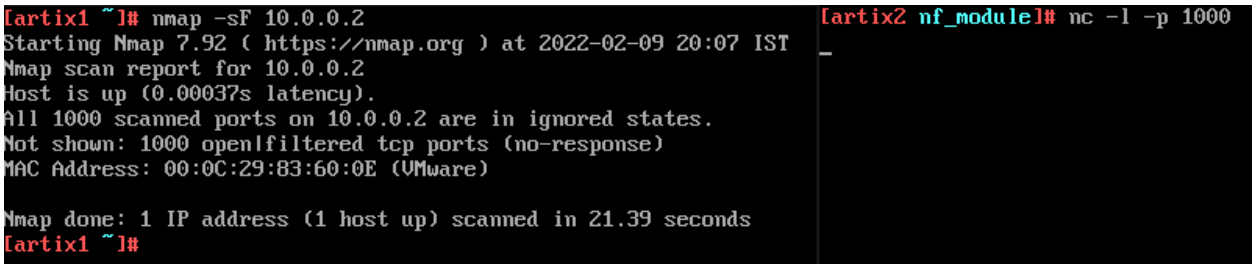


Observation: nmap is not able to detect open port on VM2 in NULL mode



Observation: NULL scan detected is printed on the console for each packet sent by nmap

FIN Scan:



Observation: nmap is not able to detect open port on VM2 in FIN mode

```
[21909.279986] FIN scan detected!
[21909.282623] FIN scan detected!
[21909.285201] FIN scan detected!
[21909.362745] FIN scan detected!
[21909.365590] FIN scan detected!
[21909.368078] FIN scan detected!
[21909.370590] FIN scan detected!
[21909.373183] FIN scan detected!
[21909.375741] FIN scan detected!
[21909.378150] FIN scan detected!
[21909.380793] FIN scan detected!
[21909.383037] FIN scan detected!
[21909.385560] FIN scan detected!
[21909.462705] FIN scan detected!
[artix2 nf_module]# _
```

```
artix1 - VMware Workstation 16 Player (N
File  Virtual Machine  Help
[artix1 ~]# nmap -sF 10.0.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 19:37 IST
Nmap scan report for 10.0.0.2
Host is up (0.00027s latency).
All 1000 scanned ports on 10.0.0.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:83:60:04 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.71 seconds
[artix1 ~]# _
```

Observation: FIN scan detected is printed on the console for each packet sent by nmap

XMAS Scan:

```
[artix1 ~]# nmap -sX 10.0.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 20:04 IST
Nmap scan report for 10.0.0.2
Host is up (0.00037s latency).
All 1000 scanned ports on 10.0.0.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:83:60:04 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
[artix1 ~]#
```

```
[artix2 nf_module]# nc -l -p 1000
_
```

Observation: nmap is not able to detect open port on VM2 in XMAS mode

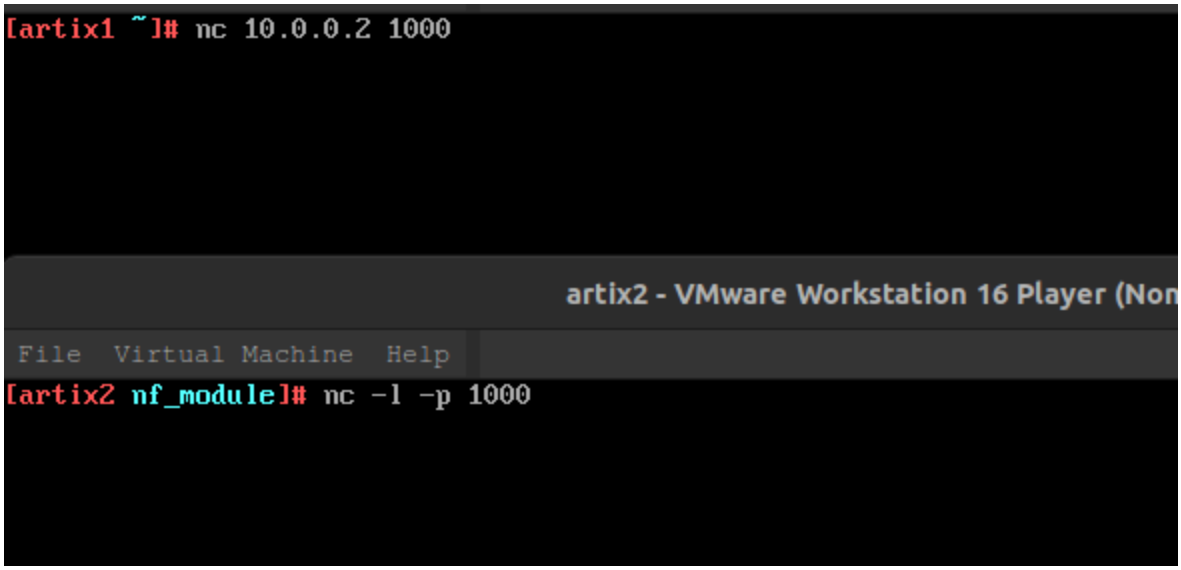
```
[artix1 ~]# nmap -sX 10.0.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 20:04 IST
Nmap scan report for 10.0.0.2
Host is up (0.00037s latency).
All 1000 scanned ports on 10.0.0.2 are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 00:0C:29:83:60:04 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
[artix1 ~]# _
```

```
[23537.839036] XMAS Scan detected!
[23537.841690] XMAS Scan detected!
[23537.844169] XMAS Scan detected!
[23537.846642] XMAS Scan detected!
[23537.849368] XMAS Scan detected!
[23537.851858] XMAS Scan detected!
[23537.854434] XMAS Scan detected!
[23537.856773] XMAS Scan detected!
[23537.934080] XMAS Scan detected!
[23537.936437] XMAS Scan detected!
```

Observation: XMAS scan detected is printed on the console for each packet sent by nmap

As observed above, the *netfilter kernel module* is able to detect these reconnaissance packets sent by *nmap*.

Now, let's make sure that these machine are able to continue their normal communication between themselves. For that, I opened a *netcat* on VM1 and connected to the open port on VM2. After this, I was able to communicate with the the other machine easily, even when the netfilter kernel module was loaded in the kernel.



Test Script

To run:

1. **NULL Scan test** : *./test_script.py NULL 20.0.0.2*
2. **FIN Scan test** : *./test_script.py FIN 20.0.0.2*
3. **XMAS Scan test** : *./test_script.py XMAS 20.0.0.2*