TNE20003 – Internet and Cybersecurity for Engineering Applications

Portfolio Task – Lab 9 Credit Task

Aims:

- To observe and investigate port scanning and intrusion detection.

Preparation:

- View "Introduction to Cybersecurity" & "Cybersecurity"

Due Date:

- All tasks in this lab are to be completed and demonstrated to your Lab instructor preferably during or at the end of the current lab, but if you do not complete the tasks you may demonstrate it at the beginning of your next lab class.

3. Information Gathering: Vulnerability Assessment, Network Mapping, Evasion and Stealth:

5. Define Acceptable Port Scanning:Authorization and Documentation,Scope and Limitations

6. False Positives, False Negatives, Zero-Day Vulnerabilities

4. No

Task 1

Get an understanding of the lab.

The purpose of this lab is to learn about port scanning and intrusion detection systems (IDS). We will use a popular port scanner to scan another machine which has been set up with a popular IDS to detect such intrusions.

This work is to be carried out using the virtual machines used in lab 1.

You will use the **Snort** IDS and nmap port scanning software. You will scan one host from another. The scanned host is to have **Snort** running to detect intrusions. Both **Snort** and **nmap** are already installed on the Virtual Machines you downloaded for lab 1.

You may be asked for a password. All passwords are ***user***.

Task 2 - Host configuration

The two hosts should have been configured with IP addresses in the Pass task.

Take note of the two IP addresses. (Use ifconfig.)

Check connectivity between both hosts with a ping.

Task 3 - Testing Snort

Once connectivity is established validate that Snort is working on VM1.

Open a command prompt window and type:

sudo snort -i 3 -c /etc/snort/snort.conf -T

You should see a series of messages, the last of which are:

Snort successfully validated the configuration!
Snort exiting

This may take quite some time.

2. Intrusion Detection is a security mechanism and a fundamental component of network and computer security. It involves the monitoring of network or system activities for any suspicious or unauthorized behavior that could indicate a security breach.

Task 4 - Add a rule to detect pings

At the moment snort has default rules installed that allow it to detect different attacks. We will add an additional rule that will cause it to detect and report pings.

Edit the Snort config file using gedit (or your favourite Linux editor) to add a local rule.

sudo gedit /etc/snort/rules/local.rules

Add the following line:

alert icmp any any -> any any (msg:"ICMP"; sid:1000001;)

This will detect messages from any network to any network that is an ICMP. The rule number is 1000001.

Now run snort in intrusion detection mode reporting all exceptions to the console

sudo snort -c /etc/snort/snort.conf -A console

From VM2 ping this host. You should see a notification of the pings.

Task 5 - Testing the IDS with some common attacks

Nmap

Port scanning is used to identify vulnerable ports on a host.
From VM2 do a port scan of VM1.

```
nmap -system-dns -v -A  ipaddress
```

What information is shown as a result of the nmap output?

What messages did Snort generate as a result of the port scan? Use wireshark to identify some of them.

Tunnelling Attack

Use the hts and htc commands from the previous lab to see if tunnelling of telnet through http using can be detected by Snort.

Task 6 - Assessment of this lab

Show the instructor that you have got Snort running and have carried out the attacks listed. The instructor will also ask you the following questions. The last two questions are particularly important.

1. What is port scanning?
2. What is Intrusion Detection?
3. Why is port scanning a threat to an organisation?
4. Did Snort detect the tunnelling of telnet through port 80?
5. How should an organisation deal with port scanning in its security policy?
6. What might be some of the limitations of an Intrusion Detection System such as Snort?

1. Port scanning is a network reconnaissance technique used to discover open ports and services on a

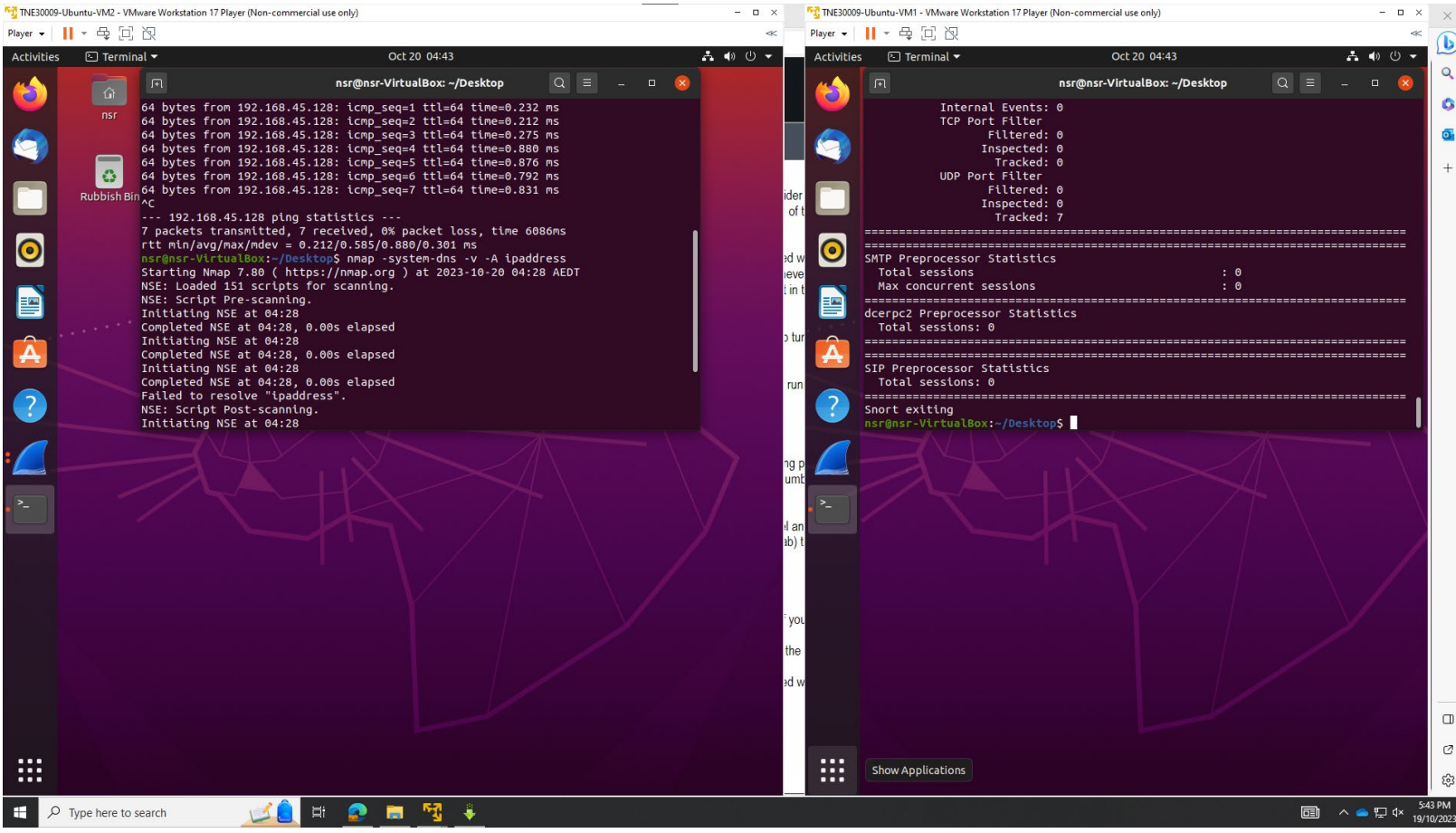
2. Intrusion Detection is a security mechanism and a fundamental

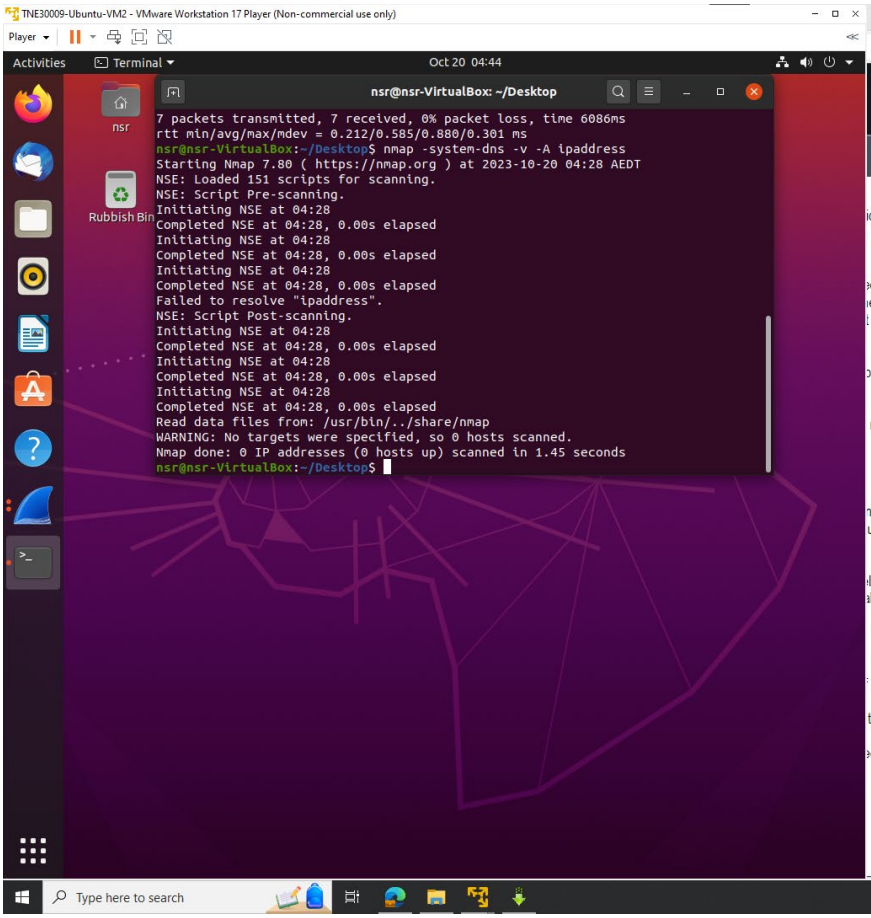
component of network and computer security. It involves the monitoring of network or system activities for any suspicious or unauthorized behavior that could indicate a security breach.

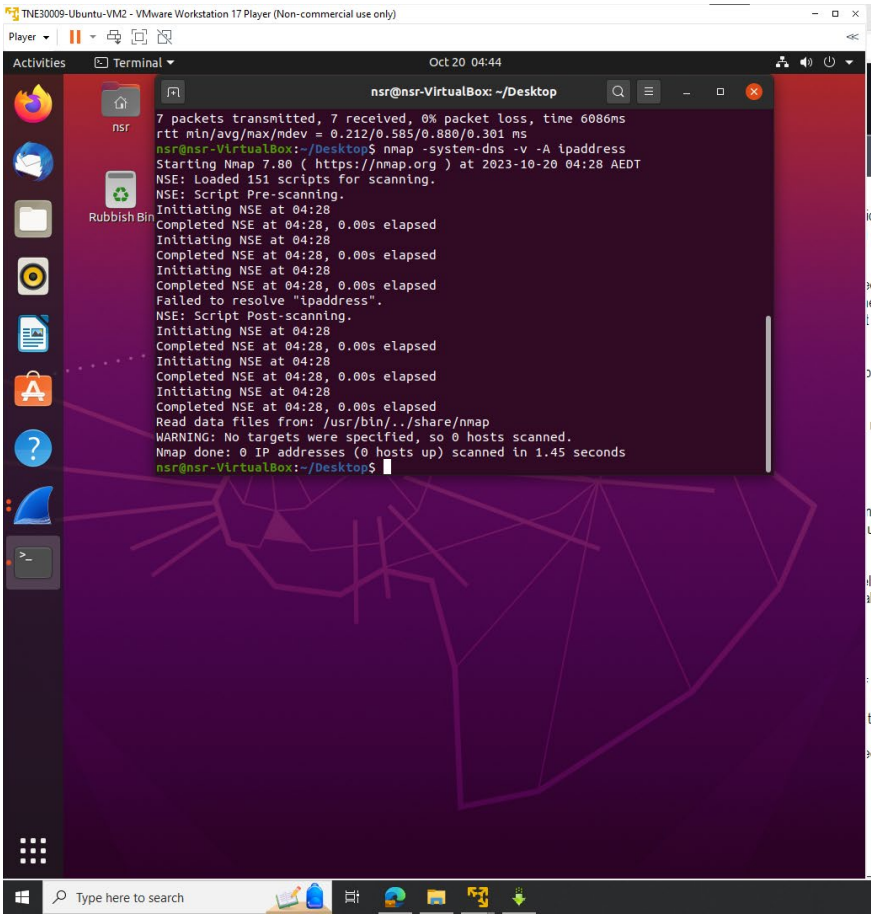
3. Information Gathering: Vulnerability Assessment, Network Mapping, Evasion and Stealth:
4. No

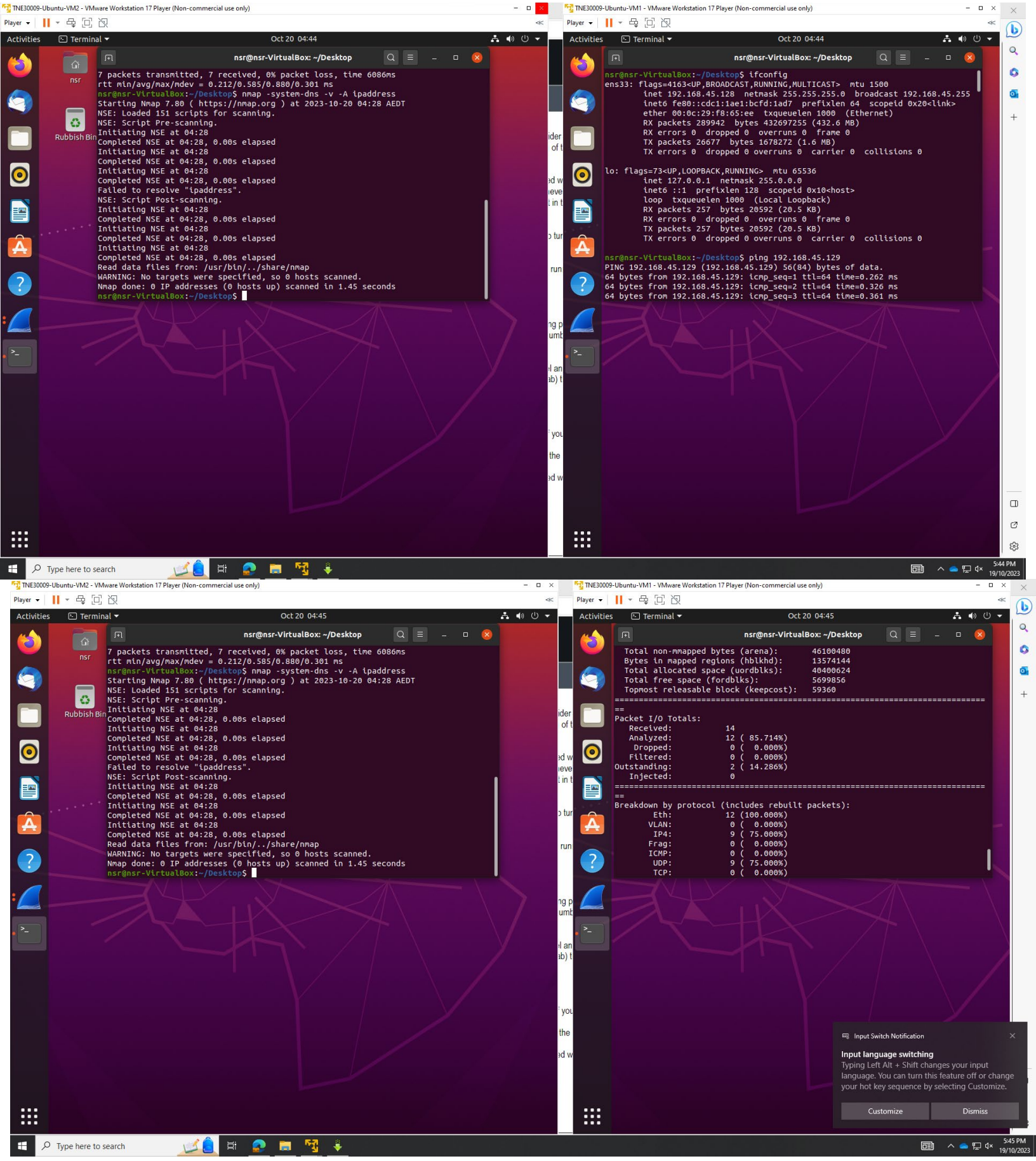
5. Define Acceptable Port Scanning:Authorization and Documentation,Scope and Limitations

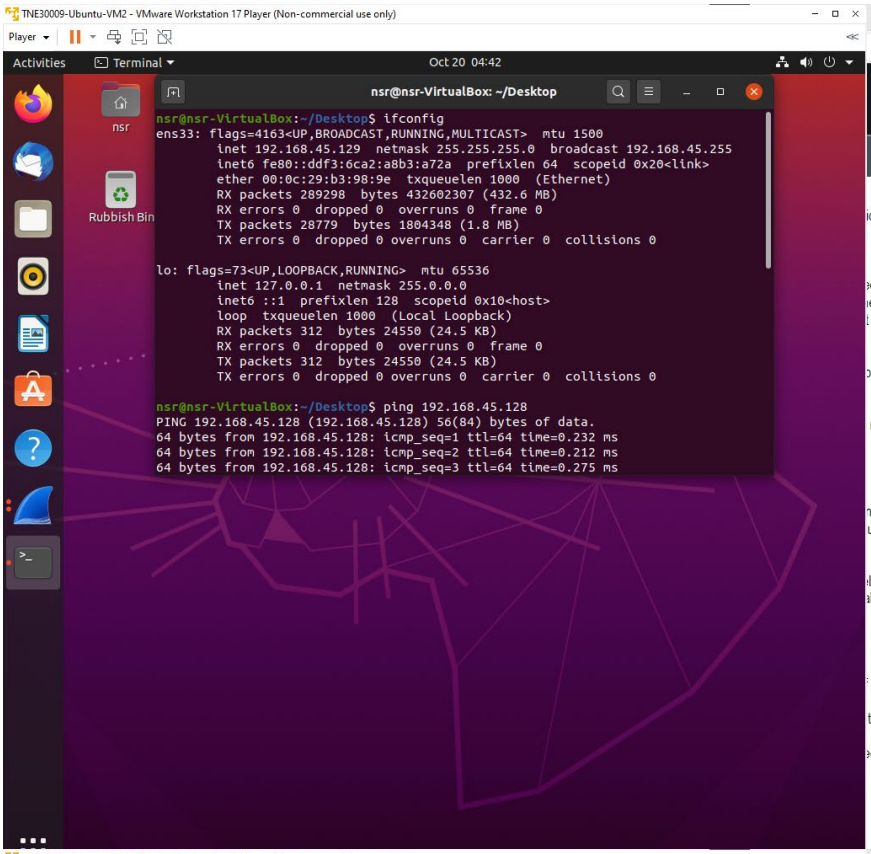
6. False Positives, False Negatives, Zero-Day Vulnerabilities

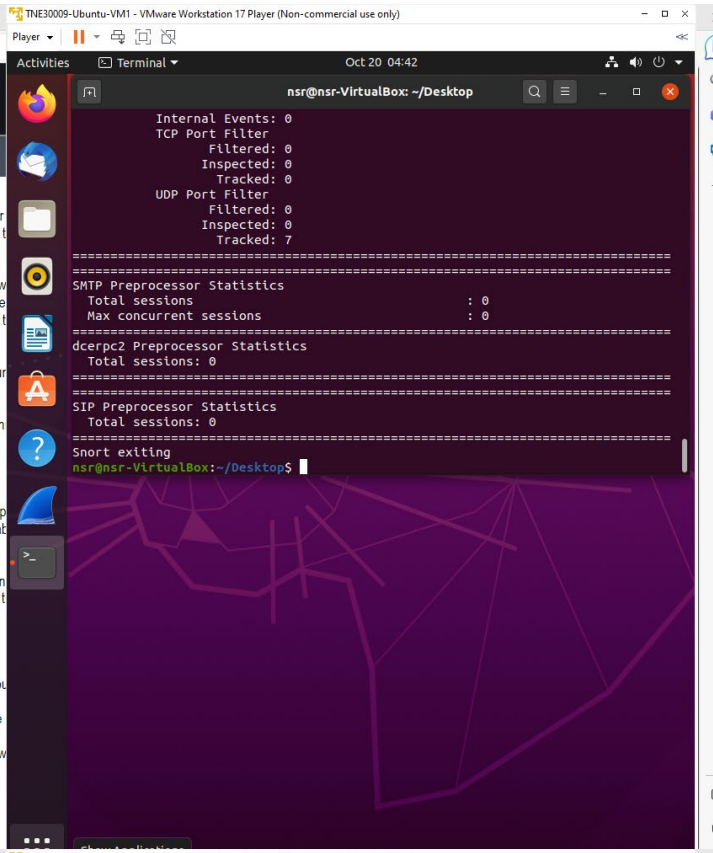


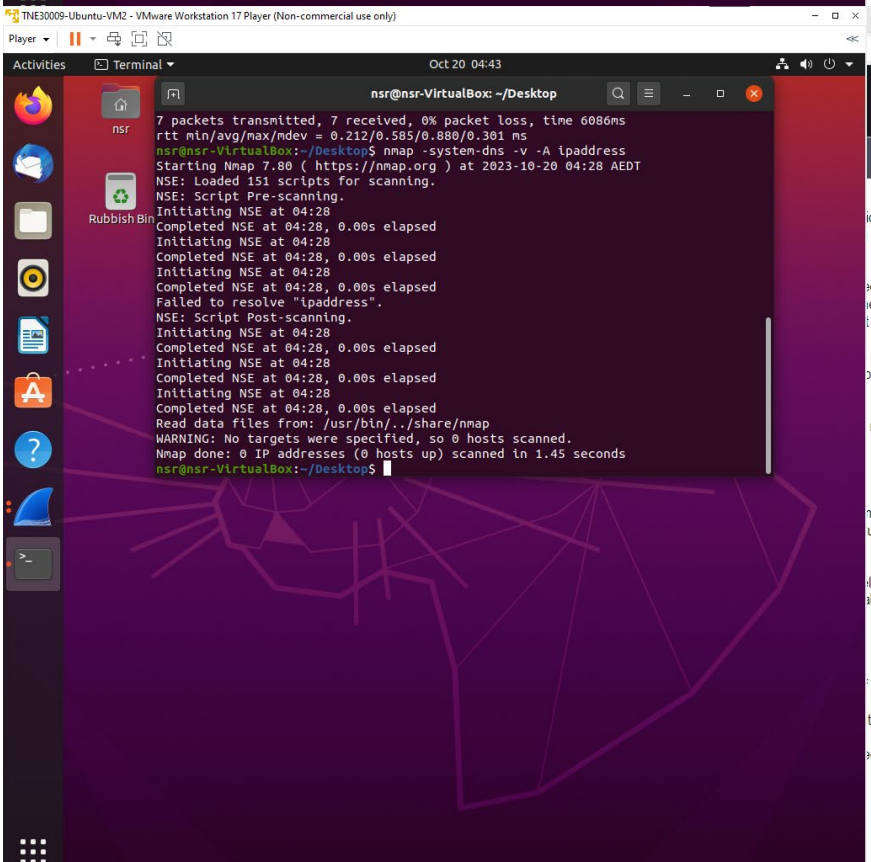

TNE30009-Ubuntu-VM2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:44
nsr@nsr-VirtualBox: ~/Desktop
nsr
Rubbish Bin
7 packets transmitted, 7 received, 0% packet loss, time 6086ms
rtt min/avg/max/mdev = 0.212/0.585/0.880/0.301 ms
nsr@nsr-VirtualBox:~/Desktop$ nmap -system-dns -v -A ipaddress
Starting Nmap 7.80 (https://nmap.org) at 2023-10-20 04:28 AEDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Failed to resolve "ipaddress".
NSE: Script Post-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.45 seconds
nsr@nsr-VirtualBox:~/Desktop$
TNE30009-Ubuntu-VM1 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:44
nsr@nsr-VirtualBox: ~/Desktop
WARNING: /etc/snort/rules/community-web-php.rules(449) GID 1 SID 100000889 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(450) GID 1 SID 100000906 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(451) GID 1 SID 100000907 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(452) GID 1 SID 100000908 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(453) GID 1 SID 100000909 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(454) GID 1 SID 100000910 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(455) GID 1 SID 100000911 in ru
le duplicates previous rule. Ignoring old rule.
WARNING: /etc/snort/rules/community-web-php.rules(456) GID 1 SID 100000912 in ru
le duplicates previous rule. Ignoring old rule.
Type here to search
5:44 PM
19/10/2023

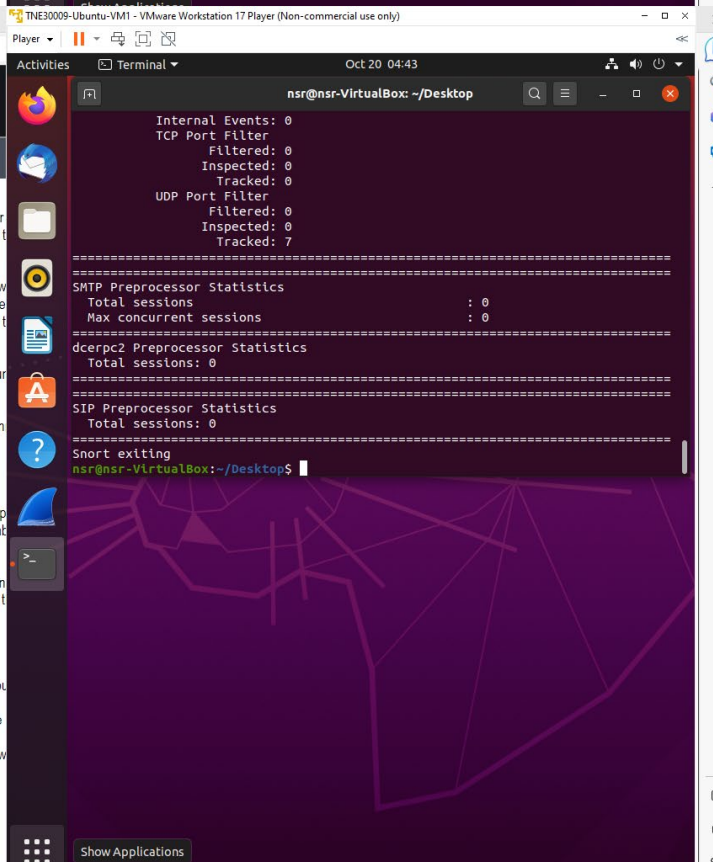

TNE30009-Ubuntu-VM2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:44
nsr@nsr-VirtualBox: ~/Desktop
nsr
Rubbish Bin
7 packets transmitted, 7 received, 0% packet loss, time 6086ms
rtt min/avg/max/mdev = 0.212/0.585/0.880/0.301 ms
nsr@nsr-VirtualBox:~/Desktop$ nmap -system-dns -v -A ipaddress
Starting Nmap 7.80 (https://nmap.org) at 2023-10-20 04:28 AEDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Failed to resolve "ipaddress".
NSE: Script Post-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.45 seconds
nsr@nsr-VirtualBox:~/Desktop$
TNE30009-Ubuntu-VM1 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:44
nsr@nsr-VirtualBox: ~/Desktop
64 bytes from 192.168.45.129: icmp_seq=4 ttl=64 time=0.475 ms
64 bytes from 192.168.45.129: icmp_seq=5 ttl=64 time=0.478 ms
64 bytes from 192.168.45.129: icmp_seq=6 ttl=64 time=0.756 ms
64 bytes from 192.168.45.129: icmp_seq=7 ttl=64 time=0.764 ms
64 bytes from 192.168.45.129: icmp_seq=8 ttl=64 time=0.764 ms
^C
--- 192.168.45.129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7145ms
rtt min/avg/max/mdev = 0.262/0.523/0.764/0.196 ms
nsr@nsr-VirtualBox:~/Desktop$ sudo snort -i 3 -c /etc/snort/snort.conf -T
[sudo] password for nsr:
Running in Test mode
--== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined : [80:81 311 383 591 593 901 1220 1414 1741 18
30 2301 2381 2809 3037 3128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510
7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8
280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444
41080 50002 55555]
PortVar 'SHELLCODE_PORTS' defined : [0:79 81:65535]
Type here to search
5:44 PM
19/10/2023


TNE30009-Ubuntu-VM2 - VMware Workstation 17 Player (Non-commercial use only)
TNE30009-Ubuntu-VM1 - VMware Workstation 17 Player (Non-commercial use only)
Activities
Terminal
Oct 20 04:44
nsr@nsr-VirtualBox: ~/Desktop
nsr
Rubbish Bin
7 packets transmitted, 7 received, 0% packet loss, time 6086ms
rtt min/avg/max/mdev = 0.212/0.585/0.880/0.301 ms
nsr@nsr-VirtualBox:~/Desktop$ nmap -system-dns -v -A ipaddress
Starting Nmap 7.80 (https://nmap.org) at 2023-10-20 04:28 AEDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Failed to resolve "ipaddress".
NSE: Script Post-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.45 seconds
nsr@nsr-VirtualBox:~/Desktop$
nsr@nsr-VirtualBox:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.45.128 netmask 255.255.255.0 broadcast 192.168.45.255
inet6 fe80::cdc1:1ae1:bcfd:1ad7 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:f8:65:ee txqueuelen 1000 (Ethernet)
RX packets 289942 bytes 432697255 (432.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 26677 bytes 1678272 (1.6 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 257 bytes 20592 (20.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 257 bytes 20592 (20.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
nsr@nsr-VirtualBox:~/Desktop$ ping 192.168.45.129
PING 192.168.45.129 (192.168.45.129) 56(84) bytes of data.
64 bytes from 192.168.45.129: icmp_seq=1 ttl=64 time=0.262 ms
64 bytes from 192.168.45.129: icmp_seq=2 ttl=64 time=0.326 ms
64 bytes from 192.168.45.129: icmp_seq=3 ttl=64 time=0.361 ms
Type here to search
5:44 PM
19/10/2023
Oct 20 04:45
Total non-mmapped bytes (arena): 46100480
Bytes in mapped regions (hblkhd): 13574144
Total allocated space (uordblks): 40400624
Total free space (fordblks): 5699856
Topmost releasable block (keepcost): 59360
Packet I/O Totals:
Received: 14
Analyzed: 12 (85.714%)
Dropped: 0 (0.000%)
Filtered: 0 (0.000%)
Outstanding: 2 (14.286%)
Injected: 0
Breakdown by protocol (includes rebuilt packets):
Eth: 12 (100.000%)
VLAN: 0 (0.000%)
IP4: 9 (75.000%)
Frag: 0 (0.000%)
ICMP: 0 (0.000%)
UDP: 9 (75.000%)
TCP: 0 (0.000%)
Input Switch Notification
Input language switching
Typing Left Alt + Shift changes your input language. You can turn this feature off or change your hot key sequence by selecting Customize.
Customize
Dismiss
5:45 PM
19/10/2023


TNE30009-Ubuntu-VM2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:42
nsr@nsr-VirtualBox: ~/Desktop
nsr
Rubbish Bin
nsr@nsr-VirtualBox:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.45.129 netmask 255.255.255.0 broadcast 192.168.45.255
inet6 fe80::ddf3:6ca2:a8b3:a72a prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:b3:98:9e txqueuelen 1000 (Ethernet)
RX packets 289298 bytes 432602307 (432.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 28779 bytes 1804348 (1.8 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 312 bytes 24550 (24.5 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 312 bytes 24550 (24.5 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
nsr@nsr-VirtualBox:~/Desktop$ ping 192.168.45.128
PING 192.168.45.128 (192.168.45.128) 56(84) bytes of data.
64 bytes from 192.168.45.128: icmp_seq=1 ttl=64 time=0.232 ms
64 bytes from 192.168.45.128: icmp_seq=2 ttl=64 time=0.212 ms
64 bytes from 192.168.45.128: icmp_seq=3 ttl=64 time=0.275 ms


TNE30009-Ubuntu-VM1 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:42
nsr@nsr-VirtualBox: ~/Desktop
Internal Events: 0
TCP Port Filter
Filtered: 0
Inspected: 0
Tracked: 0
UDP Port Filter
Filtered: 0
Inspected: 0
Tracked: 7
SMTP Preprocessor Statistics
Total sessions : 0
Max concurrent sessions : 0
dcerpc2 Preprocessor Statistics
Total sessions: 0
SIP Preprocessor Statistics
Total sessions: 0
Snort exiting
nsr@nsr-VirtualBox:~/Desktop$


TNE30009-Ubuntu-VM2 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:43
nsr@nsr-VirtualBox: ~/Desktop
nsr
Rubbish Bin
7 packets transmitted, 7 received, 0% packet loss, time 6086ms
rtt min/avg/max/mdev = 0.212/0.585/0.880/0.301 ms
nsr@nsr-VirtualBox:~/Desktop$ nmap -system-dns -v -A ipaddress
Starting Nmap 7.80 (https://nmap.org) at 2023-10-20 04:28 AEDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Failed to resolve "ipaddress".
NSE: Script Post-scanning.
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Initiating NSE at 04:28
Completed NSE at 04:28, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 1.45 seconds
nsr@nsr-VirtualBox:~/Desktop$


TNE30009-Ubuntu-VM1 - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Oct 20 04:43
nsr@nsr-VirtualBox: ~/Desktop
Internal Events: 0
TCP Port Filter
Filtered: 0
Inspected: 0
Tracked: 0
UDP Port Filter
Filtered: 0
Inspected: 0
Tracked: 7
SMTP Preprocessor Statistics
Total sessions : 0
Max concurrent sessions : 0
dcerpc2 Preprocessor Statistics
Total sessions: 0
SIP Preprocessor Statistics
Total sessions: 0
Snort exiting
nsr@nsr-VirtualBox:~/Desktop$
Show Applications

Type here to search
5:43 PM
19/10/2023