AskCyPert

Port Scanning Lab

CAC
Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Purpose

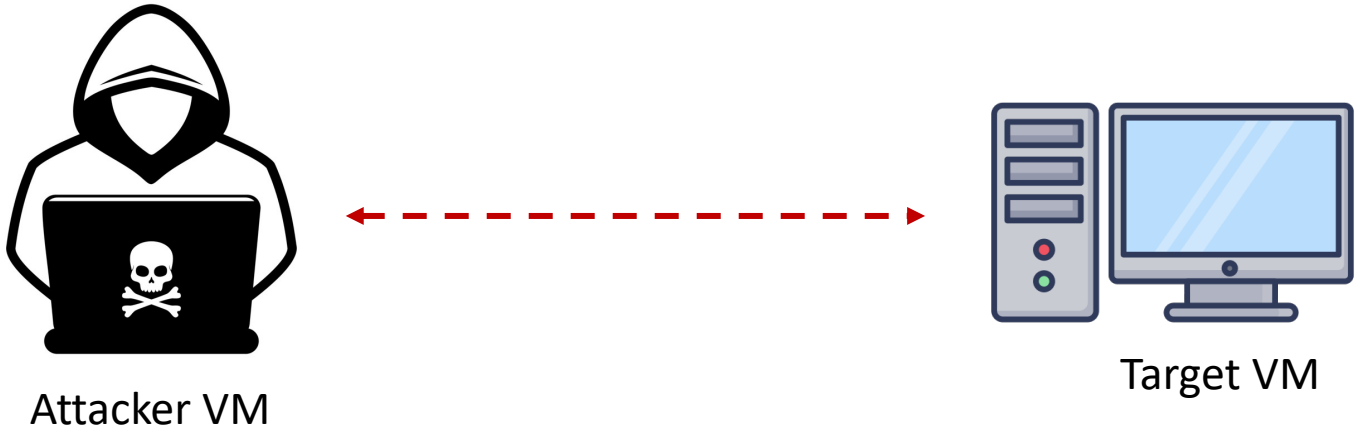
- The purpose of this lab is to familiarize the student with the basics of port scanning
- In this lab, the student will perform port scanning attacks using NMAP
- The students will also use NMAP to identify the different services running on the target system

What is port scanning?

- Attackers use port scanning to perform reconnaissance on the target system
- A successful port scanning attack, informs the attackers of the open ports and services running on the target system
- The attacker uses this information to perform an attack by exploiting an existing vulnerability on one or more services running on the target system

Virtual Lab Setup

- This lab is composed of 2 VMs



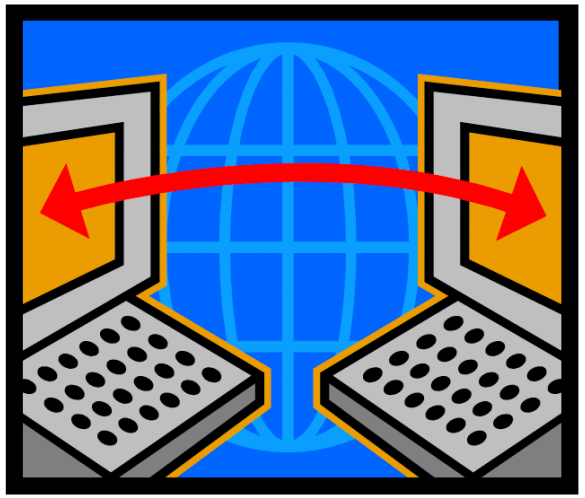
Lab Structure

- The *Port scanning* lab consists of 3 experiments
  1. Port scanning
  2. TCP SYN scan
  3. Detect OS and running services

Lab Software Tools

For this lab, we will be using the following tools:

- **Nmap:** Open-source tool for network discovery. It is used to discover hosts and services on a computer network, creating a map of the network's structure.



AskCyPert

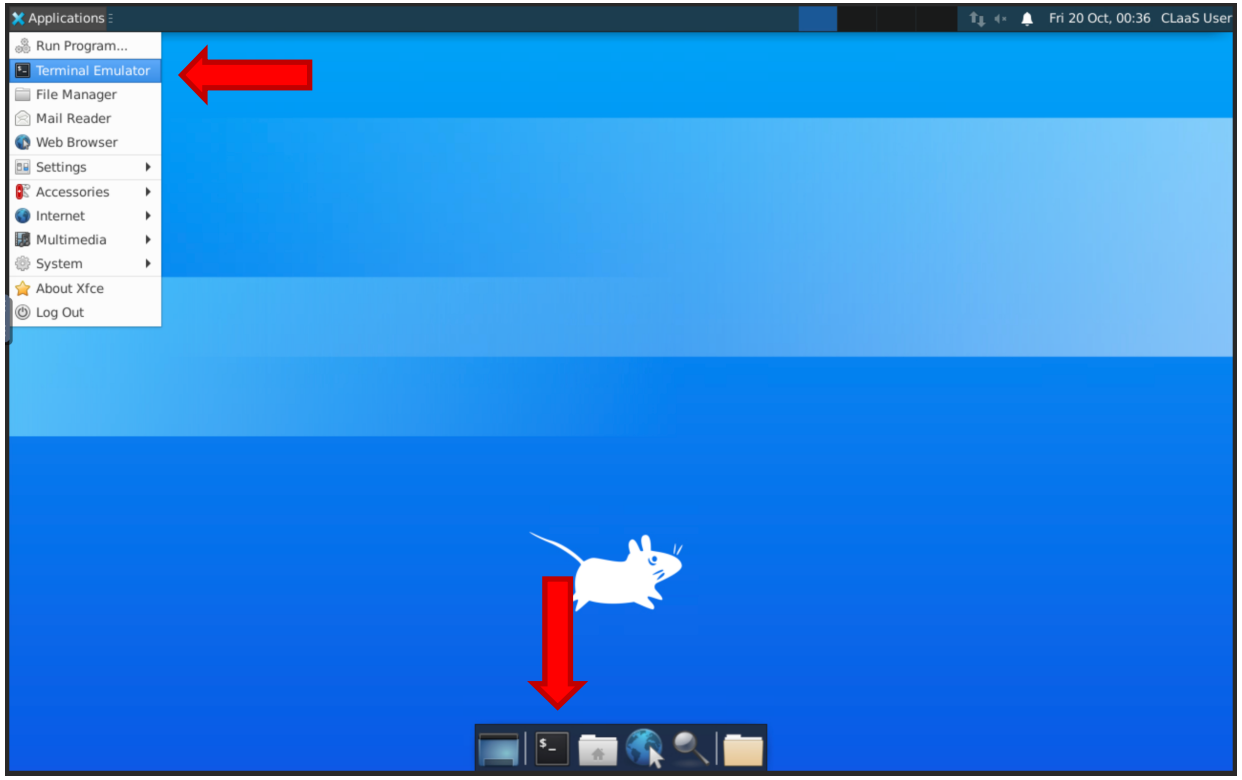
Experiment 0:
Getting ready to start

CAC Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Open a terminal
  - For this lab we will be using the terminal.
  - There are two ways to open it.
    - From the menu
    - Or by clicking the icon on the dock:

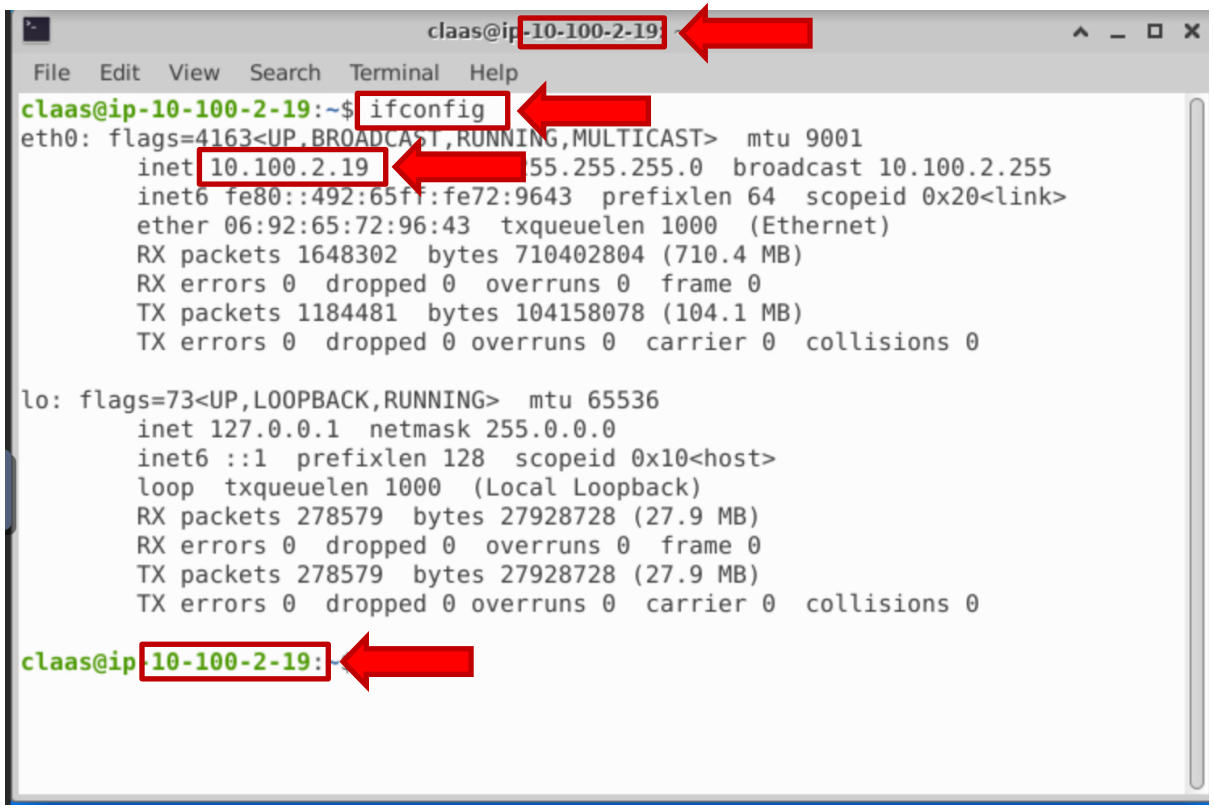


Experiment Instructions

- Step 2: Get the IP addresses
  - We can see the IP address as soon as we open the terminal
  - Or by typing

    `ifconfig`

  - *You will need the IPs of all the VMs, for the rest of the lab.*



AskCyPert

Experiment 1: Port Scanning

CAC
Center for Cloud and Autonomic Computing

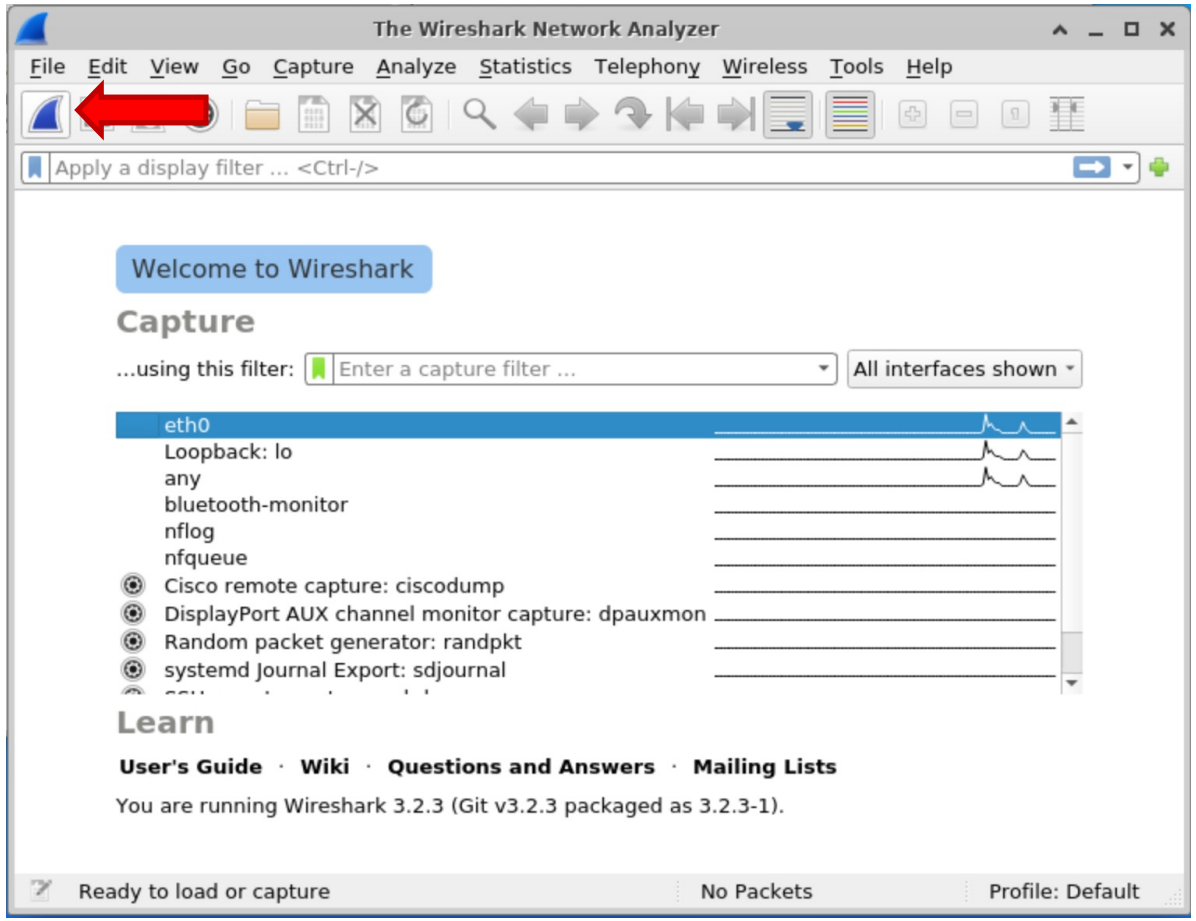
NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Open Wireshark
  - On the Target VM
  - Open a terminal and type

    `wireshark`

- Step 2: Prepare Wireshark
  - Once Wireshark is open select the *eth0* interface
  - Click the blue button to *Start capturing packets*



Experiment Instructions

- Step 3: Scan a single IP
  - On the Attacker VM
  - Open a terminal and type

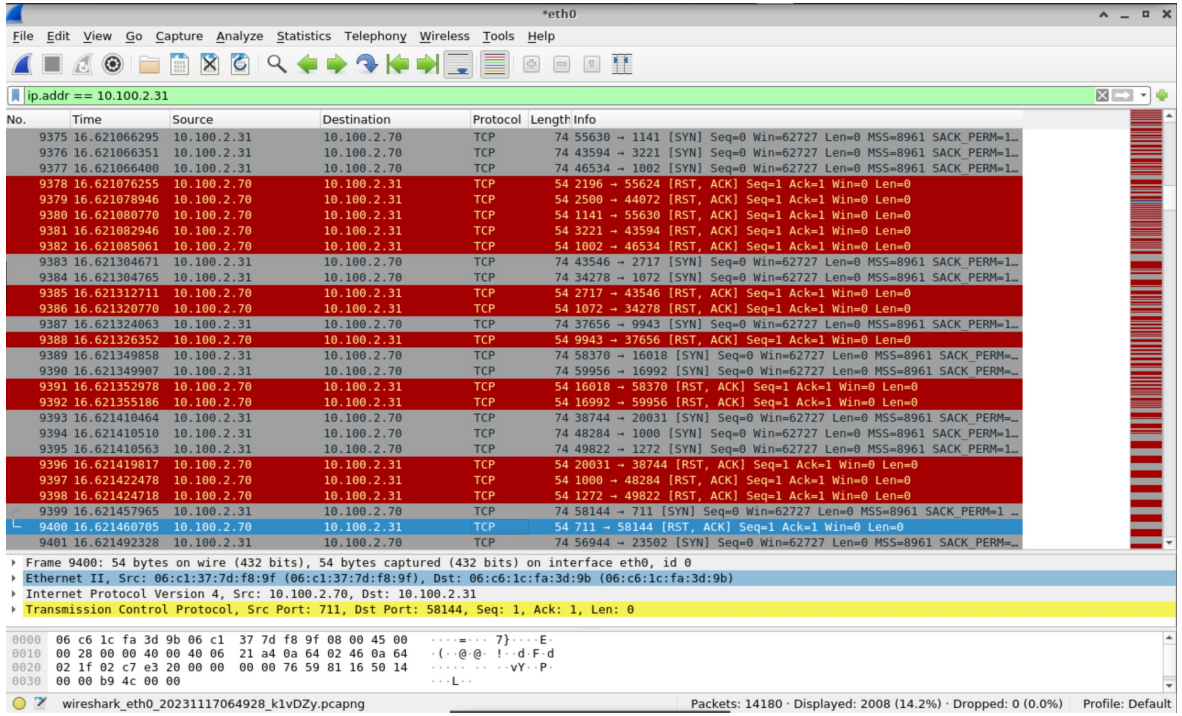
```
nmap <IP of target>
```

```
claas@ip-10-100-2-31:~$ nmap 10.100.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 06:48 UTC
Nmap scan report for ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)
Host is up (0.0070s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5901/tcp open  vnc-1

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

Experiment Instructions

- Step 4: Observe the traffic on the target VM
  - Go back to the target VM
  - On Wireshark select *Stop capturing packets*
  - Filter the traffic using the following display filter

```
ip.addr == <IP of attacker>
```



Experiment Instructions

- Step 5: Scan a range of ports
  - On the Attacker VM
  - Open a terminal and type

```
nmap –p 1-100 <IP of target>
```

```
claas@ip-10-100-2-31:~$ nmap -p 1-100 10.100.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 06:59 UTC
Nmap scan report for ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)
Host is up (0.0012s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

AskCyPert

Experiment 2: TCP SYN Scan

CAC
Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Scan using TCP SYN scan
  - On the Attacker VM
  - Open a terminal and type

```
sudo nmap -sS <IP of target>
```

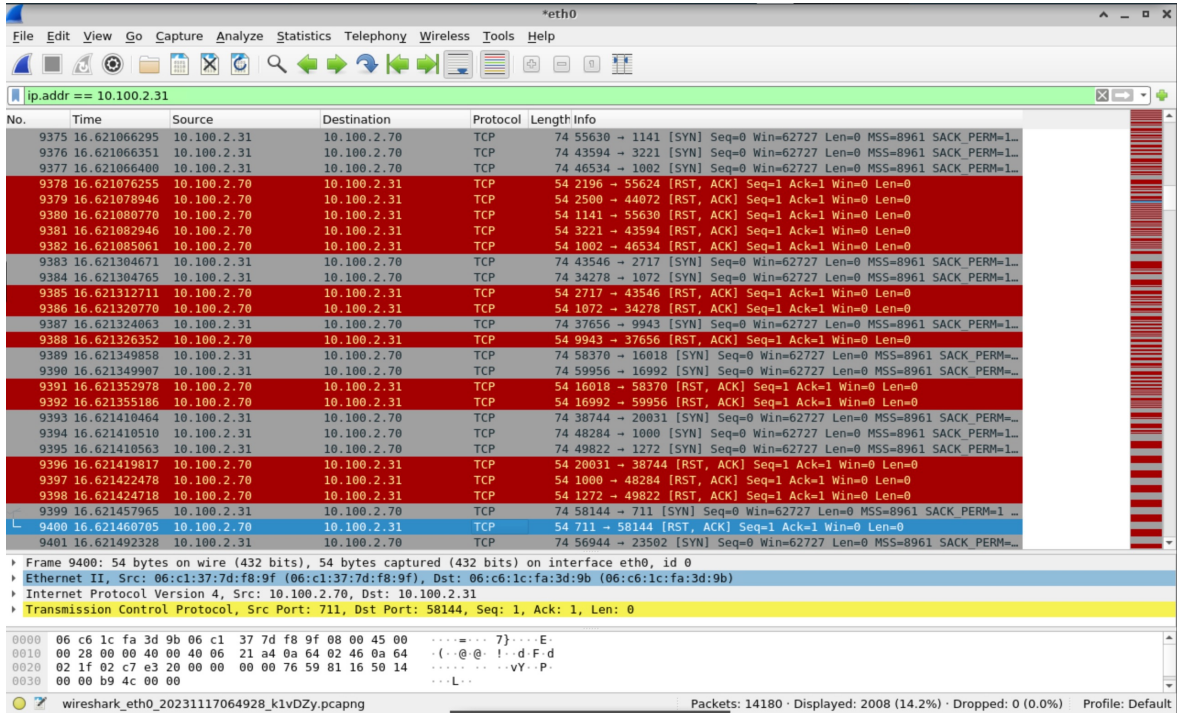
```
claas@ip-10-100-2-31:~$ sudo nmap -sS 10.100.2.70
[sudo] password for claas:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 07:03 UTC
Nmap scan report for ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)
Host is up (0.0052s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
5901/tcp open  vnc-1
MAC Address: 06:C1:37:7D:F8:9F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

  - *Sudo password: Claas2022*

Experiment Instructions

- Step 2: Observe the traffic on the target VM
  - Go back to the target VM
  - On Wireshark select *Stop capturing packets*
  - Filter the traffic using the following display filter

```
ip.addr == <IP of attacker>
```



AskCyPert

Experiment 3: Detect OS and running services

CAC Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION

Experiment Instructions

- Step 1: Scan OS and running services
  - On the Attacker VM
  - Open a terminal and type

    `nmap -A <IP of target>`

  - Then, type

    `sudo nmap -A <IP of target>`

  - Observe the differences
  - *Sudo password: Claas2022*

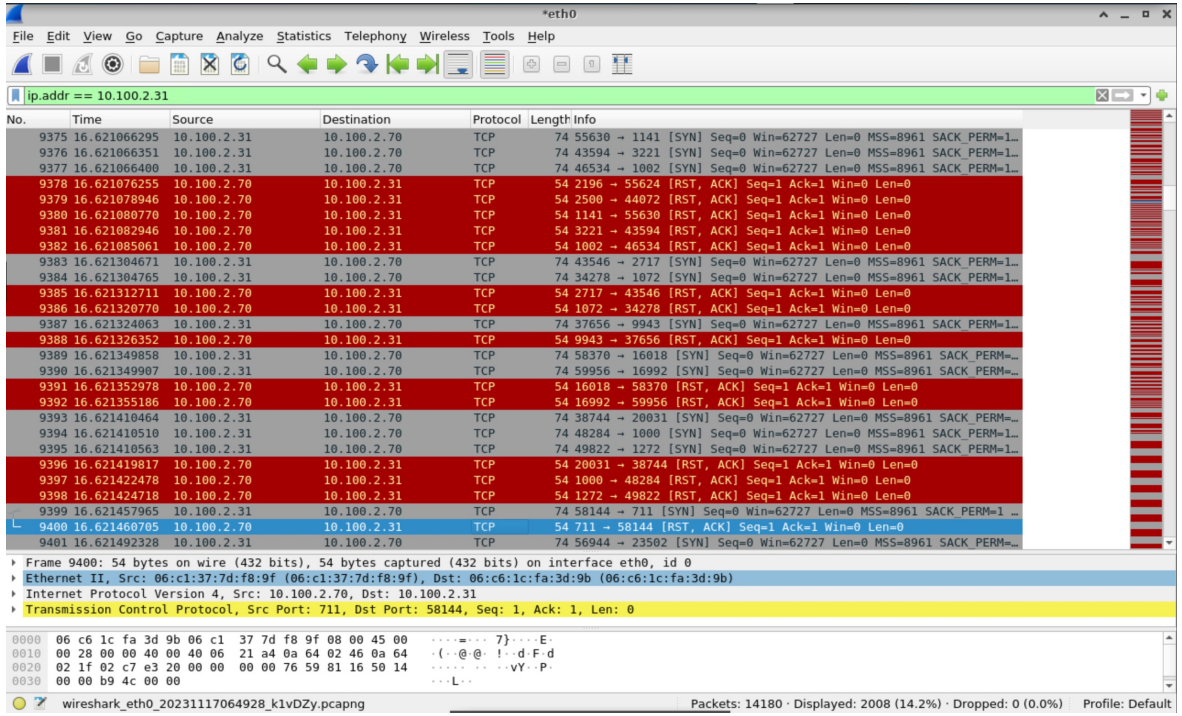
```
claas@ip-10-100-2-31:~$ nmap -A 10.100.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 07:17 UTC
Nmap scan report for ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)
Host is up (0.0076s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2
.0)
5901/tcp open  vnc     VNC (protocol 3.8)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_vnc-info: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

```
claas@ip-10-100-2-31:~$ sudo nmap -A 10.100.2.70
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 07:17 UTC
Nmap scan report for ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)
Host is up (0.00041s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2
.0)
5901/tcp open  vnc     VNC (protocol 3.8)
MAC Address: 06:C1:37:7D:F8:9F (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=11/17%OT=22%CT=1%CU=33744%PV=Y%DS=1%DC=D%G=Y%M=06C137%
OS:TM=65571394%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10D%TI=Z%CI=Z%II=
OS:I%TS=A)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11
OS:NW7%O5=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=
OS:F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%
OS:T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS:=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=
OS:0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(
OS:R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.41 ms ip-10-100-2-70.us-west-2.compute.internal (10.100.2.70)

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.38 seconds
```

Experiment Instructions

- Step 2: Observe the traffic on the target VM
  - Go back to the target VM
  - On Wireshark select *Stop capturing packets*
  - Filter the traffic using the following display filter

```
ip.addr == <IP of attacker>
```



Lab Report

- From *Experiment 1 Step 4*: Observe the traffic and describe how nmap knows which ports are open and which are closed.
- Investigate the command used in *Experiment 2 Step 1,* what is half-port scanning, and how it works.
- Observe the differences in Experiment 3 Step 1. Investigate why one command provides more information than the other.
- Based on the traffic observed in Experiment 3 Step 2, how does nmap find the OS and running services?

Conclusion

- In this lab, we used Nmap to perform a comprehensive scan of a target host, identifying a variety of open ports and services.

- We also used Nmap to perform a version scan, which revealed the specific versions of some of the running services. This information can be used to identify potential vulnerabilities that could be exploited by attackers.

AskCyPert

End of Lab

CAC
Center for Cloud and Autonomic Computing

NATIONAL SCIENCE FOUNDATION