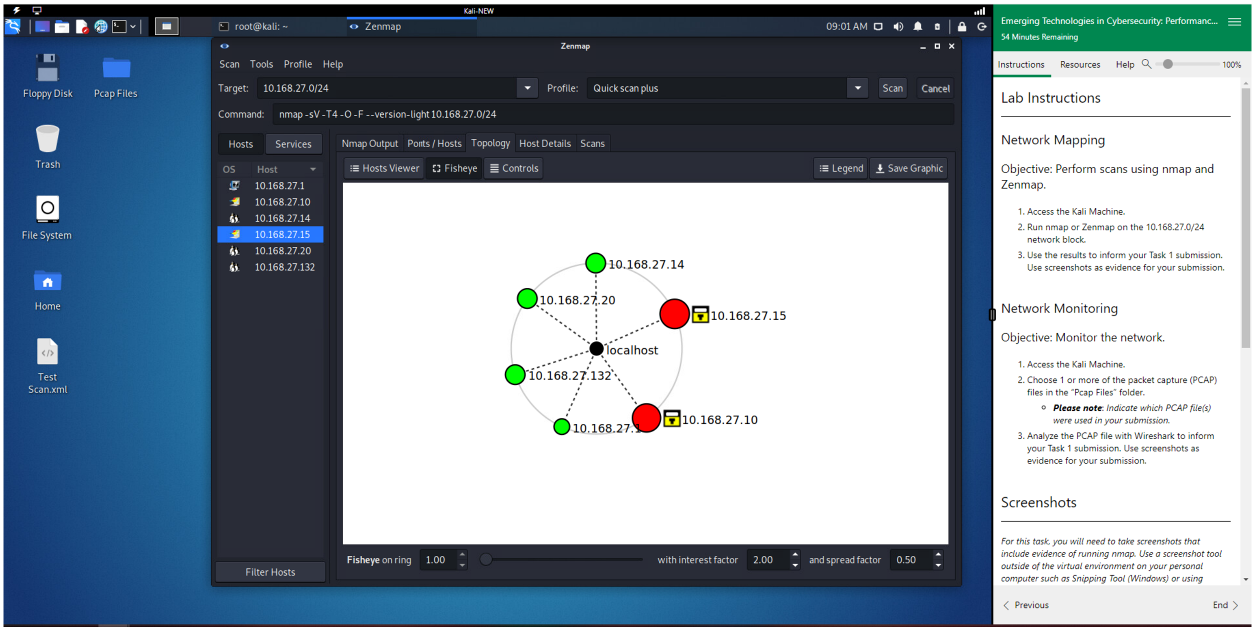
NMAP and Wireshark.

By Griffin Haas

Network Scanning and Topology

In this lab, we started by scanning the subnet 10.168.27.0/24. When the scan was completed, it gave us six machines: two Microsoft Windows server machines, three Linux Machines, and a router.



Target: 10.168.27.0/24

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24

```
10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.132
```

Fisheye on ring 1.00 with interest factor 2.00 and spread factor 0.50

Emerging Technologies in Cybersecurity: Performanc...

54 Minutes Remaining

Lab Instructions

Network Mapping

Objective: Perform scans using nmap and Zenmap.

1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.

Network Monitoring

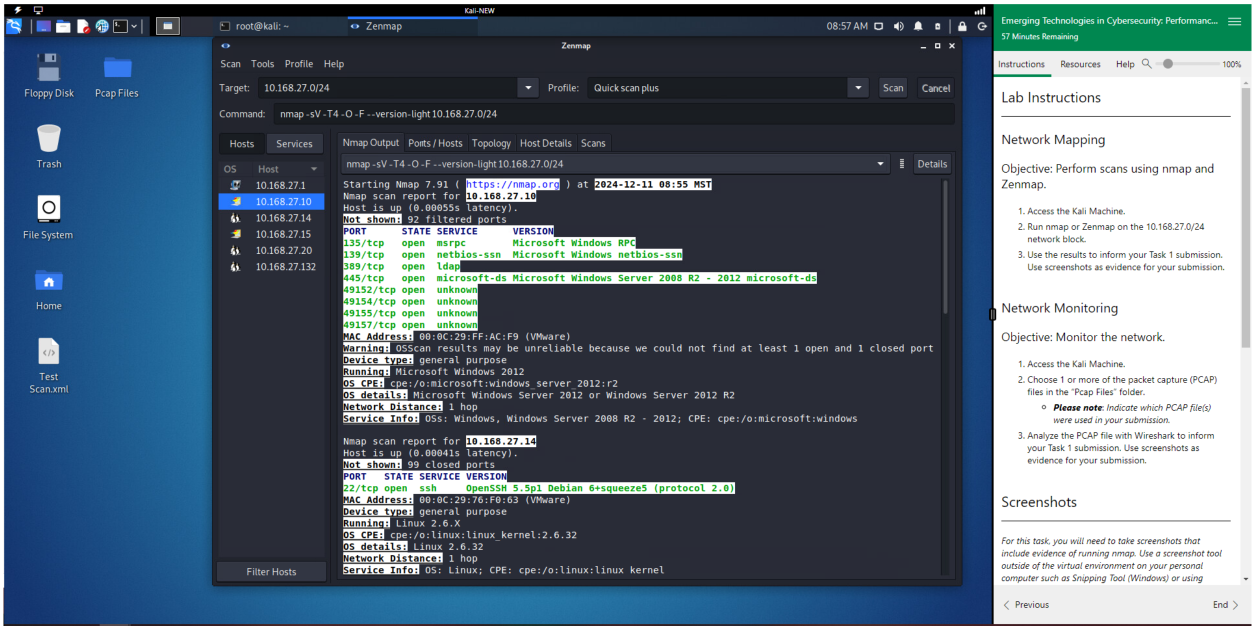
Objective: Monitor the network.

1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the "Pcap Files" folder.
   - ***Please note****: Indicate which PCAP file(s) were used in your submission.*
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.

Screenshots

For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using

This scan shows us that the network is a star. Here is the list of open ports and running services on each machine.



Target: 10.168.27.0/24

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24

10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.132

```
nmap -sV -T4 -O -F --version-light 10.168.27.0/24

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-11 08:55 MST
Nmap scan report for 10.168.27.10
Host is up (0.00055s latency).
Not shown: 92 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:FF:AC:F9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.168.27.14
Host is up (0.00041s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:76:F0:63 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Emerging Technologies in Cybersecurity: Performanc...
57 Minutes Remaining

Lab Instructions

Network Mapping

Objective: Perform scans using nmap and Zenmap.

1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.

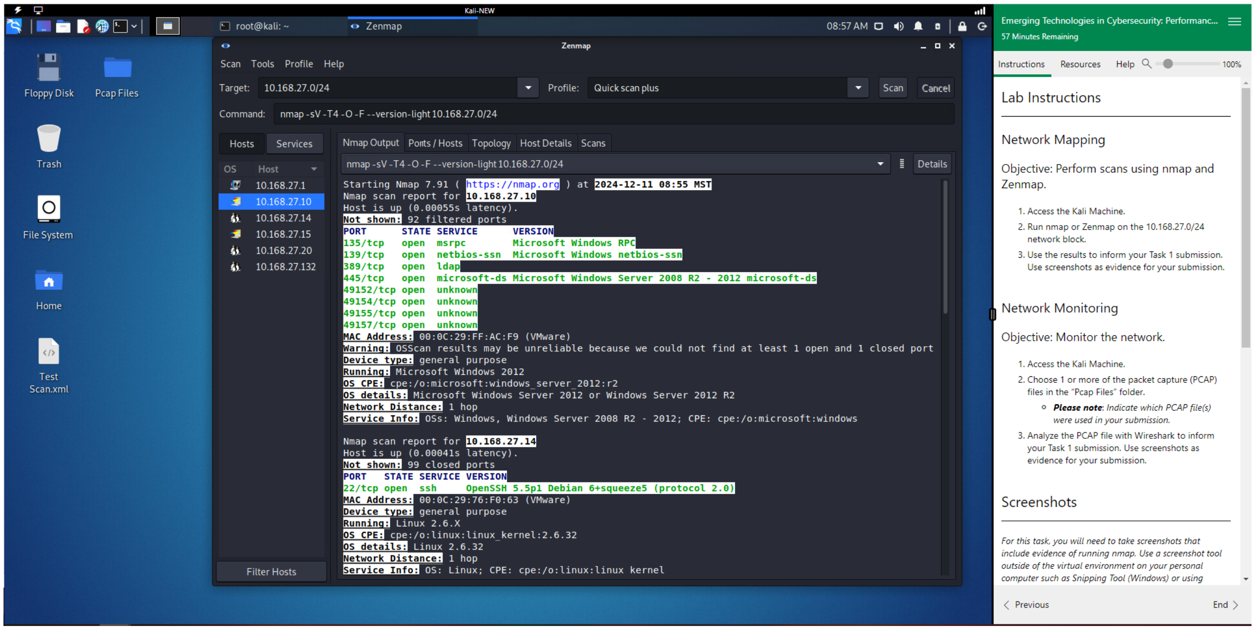
Network Monitoring

Objective: Monitor the network.

1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the "Pcap Files" folder.
   - ***Please note***: *Indicate which PCAP file(s) were used in your submission.*
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.

Screenshots

For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using


Target: 10.168.27.0/24

Profile: Quick scan plus

Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24

10.168.27.1
10.168.27.10
10.168.27.14
10.168.27.15
10.168.27.20
10.168.27.132

```
nmap -sV -T4 -O -F --version-light 10.168.27.0/24

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-11 08:55 MST
Nmap scan report for 10.168.27.10
Host is up (0.00055s latency).
Not shown: 92 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
49152/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
MAC Address: 00:0C:29:FF:AC:F9 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.168.27.14
Host is up (0.00041s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:76:F0:63 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Emerging Technologies in Cybersecurity: Performanc...
57 Minutes Remaining

Lab Instructions

Network Mapping

Objective: Perform scans using nmap and Zenmap.

1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.

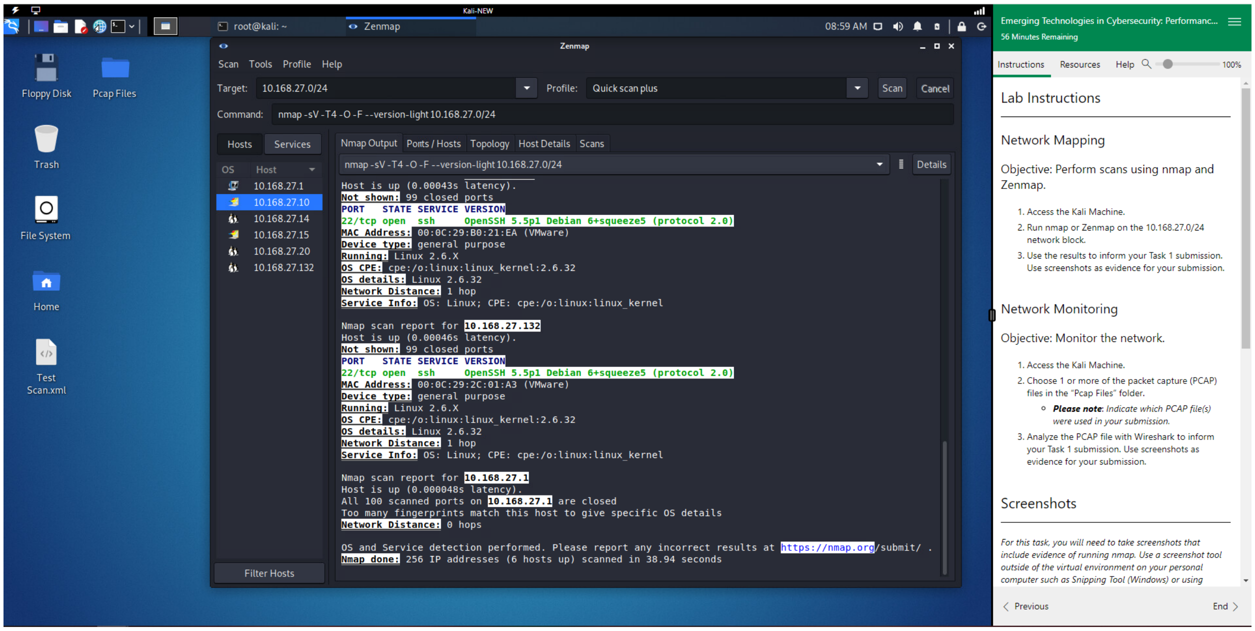
Network Monitoring

Objective: Monitor the network.

1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the "Pcap Files" folder.
   - ***Please note***: *Indicate which PCAP file(s) were used in your submission.*
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.

Screenshots

For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using



Target: 10.168.27.0/24

Profile: Quick scan plus

Scan Cancel

Command: nmap -sV -T4 -O -F --version-light 10.168.27.0/24

```
Host is up (0.00043s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:B0:21:EA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.168.27.132
Host is up (0.00046s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.5p1 Debian 6+squeeze5 (protocol 2.0)
MAC Address: 00:0C:29:2C:01:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.168.27.1
Host is up (0.000048s latency).
All 100 scanned ports on 10.168.27.1 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 38.94 seconds
```

Emerging Technologies in Cybersecurity: Performanc...
56 Minutes Remaining

Lab Instructions

Network Mapping

Objective: Perform scans using nmap and Zenmap.

1. Access the Kali Machine.
2. Run nmap or Zenmap on the 10.168.27.0/24 network block.
3. Use the results to inform your Task 1 submission. Use screenshots as evidence for your submission.

Network Monitoring

Objective: Monitor the network.

1. Access the Kali Machine.
2. Choose 1 or more of the packet capture (PCAP) files in the “Pcap Files” folder.
   - ***Please note***: *Indicate which PCAP file(s) were used in your submission.*
3. Analyze the PCAP file with Wireshark to inform your Task 1 submission. Use screenshots as evidence for your submission.

Screenshots

For this task, you will need to take screenshots that include evidence of running nmap. Use a screenshot tool outside of the virtual environment on your personal computer such as Snipping Tool (Windows) or using

Vulnerabilities, The Implications and Solution.

The first vulnerability we will be looking at will be **CVE-2023-38408**. This vulnerability is shown to be on 10.168.27.15, 10.168.27.14, and 10.168.27.132. This vulnerability occurs in OpenSSH before 9.3p2. In which the service has an untrustworthy search path, allowing attackers to perform remote code execution. Which means an attacker could execute malicious code through this vulnerability.

The next vulnerability will be **CVE-2016-1908** and is found on all machines listed on the previous vulnerability. This vulnerability occurs in versions of OpenSSH before 7.2. This vulnerability mishandles failed cookie generation for untrusted X11 forwarding and relies on local X11 server for access control decisions. Which allows remote X11 clients to obtain trusted X11 forwarding privileges by leveraging configuration issues. X11 forwarding is an SSH protocol that enables users to run graphical applications on a remote server and interact with the system. If attackers are allowed to obtain trusted X11 forwarding privileges, it would allow them to perform actions the machine with no authentication.

The final vulnerability we will be looking at is **CVE-2015-5600** which is found on all machines listed in the first vulnerability. This vulnerability affects OpenSSH versions through 6.9. The kbdint_next_device function in the file auth2-chall.c in sshd does not properly restrict the processing of keyboard-interactive within a single connection, allowing the execution of brute force attacks from remote attackers or causing a DOS (Denial-of-service) attack.

All these vulnerabilities are caused by using a legacy version of OpenSSH. The recommended solution to these vulnerabilities would be to upgrade OpenSSH to a version that is greater than 9.3p2. Preferably the most current version, which is 9.9p2. This allows all listed vulnerabilities to be patched, as well as many others I did not list.

Wireshark Anomalies, Implications, and Solutions.

While looking through the first .pcap file, there are many anomalies we can see throughout the recorded packets. The first anomaly we see is between 14927 and 16821. These packets are shown to be from the MySQL service.