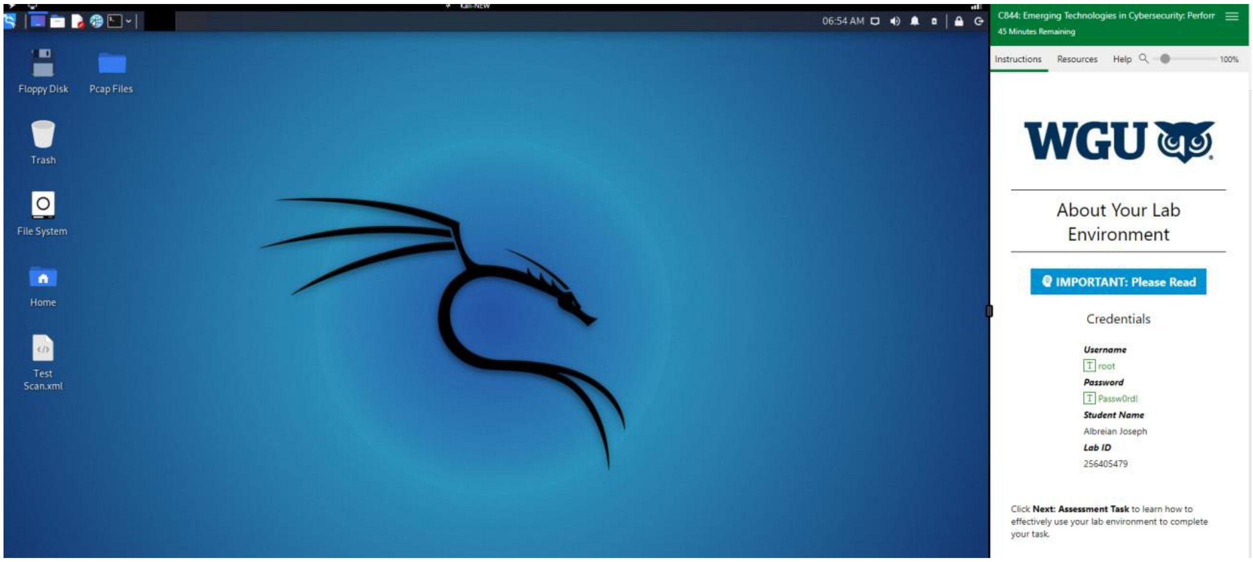
Emerging Technologies in Cybersecurity – C844

Task 1: NMAP and Wireshark

Albreian Joseph – 2589656



C844: Emerging Technologies in Cybersecurity: Perforr

45 Minutes Remaining

About Your Lab Environment

Credentials

Username

root

Password

Passw0rd!

Student Name

Albreian Joseph

Lab ID

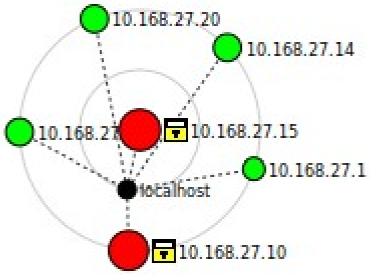
256405479

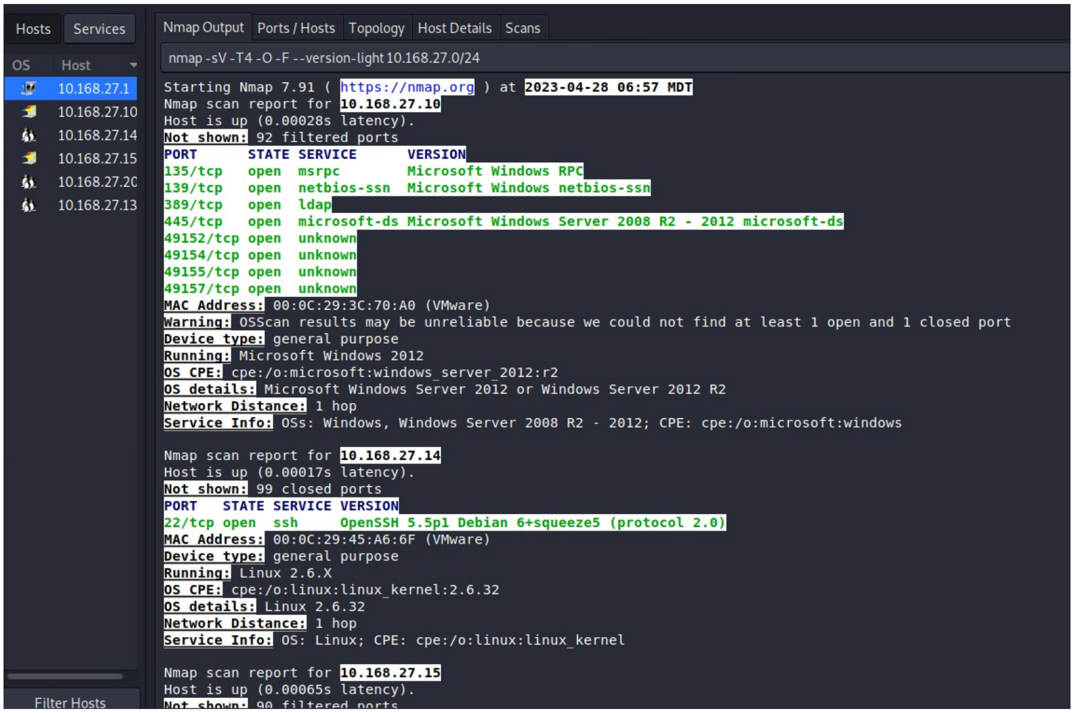
Click **Next: Assessment Task** to learn how to effectively use your lab environment to complete your task.

A. Describe the network topology:

Overview of Host details below:

Host IP	Operating system	Open Ports
10.168.27.1	N/A	0
10.168.27.10	Windows Server 2012	135; 139; 389; 445; 49152; 49154; 49155; 49157
10.168.27.14	Linux 2.6.32	22
10.168.27.15	Windows Server 2008	7; 9; 13; 21; 80; 135; 139; 445; 49154; 49155
10.168.27.20	Linux 2.6.32	22
10.168.27.13	Linux 2.6.32	22





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

```
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-28 06:57 MDT
Nmap scan report for 10.168.27.10
Host is up (0.00028s 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:29:3C:70:A0 (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 (0.00017s 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:29:45:A6:6F (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 10.168.27.15
Host is up (0.00065s latency).
Not shown: 90 filtered ports
```

B. Vulnerabilities on the network and their potential implications:

1st Vulnerability

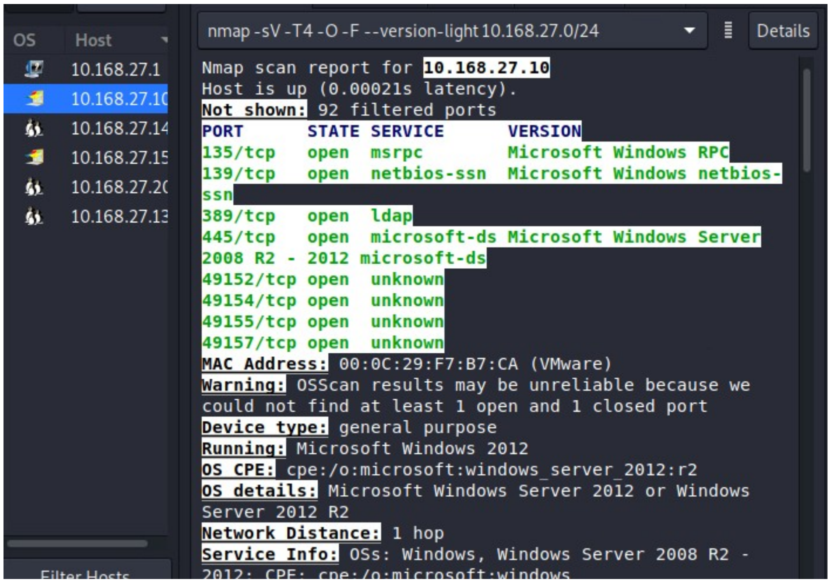
Host: 10.168.27.10

Operating System: Windows Server 2012

Open Ports: 135; 139; 389; 445; 49152; 49154; 49155; 49157

Vulnerable Port: 139 NetBios

Implication: allow a user to read or write remote computer systems; attackers can also launch a DoS.



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

```
Nmap scan report for 10.168.27.10
Host is up (0.00021s 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:F7:B7:CA (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
```

2nd Vulnerability

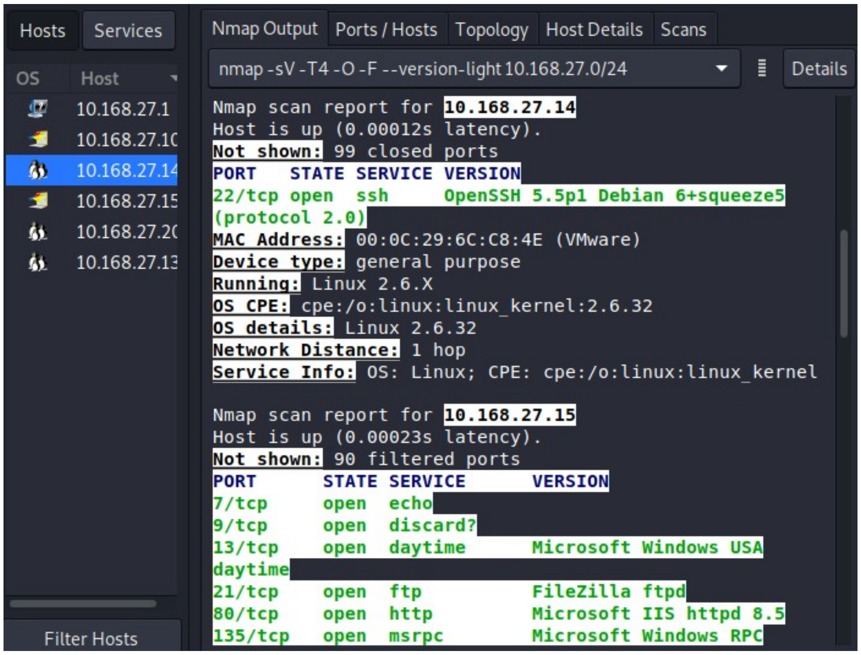
Host: 10.168.27.14

Operating System: Linux 2.6.32

Open Ports: 22

Vulnerable Port: 22 SSH

Implication: An unauthenticated remote attacker can gain unauthorized access and bypass security restrictions through port 22.



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

```
Nmap scan report for 10.168.27.14
Host is up (0.00012s 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:29:6C:C8:4E (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 10.168.27.15
Host is up (0.00023s latency).
Not shown: 90 filtered ports
PORT       STATE SERVICE       VERSION
7/tcp      open  echo
9/tcp      open  discard?
13/tcp     open  daytime       Microsoft Windows USA
daytime
21/tcp     open  ftp           FileZilla ftpd
80/tcp     open  http          Microsoft IIS httpd 8.5
135/tcp    open  msrpc         Microsoft Windows RPC
```

3rd Vulnerability

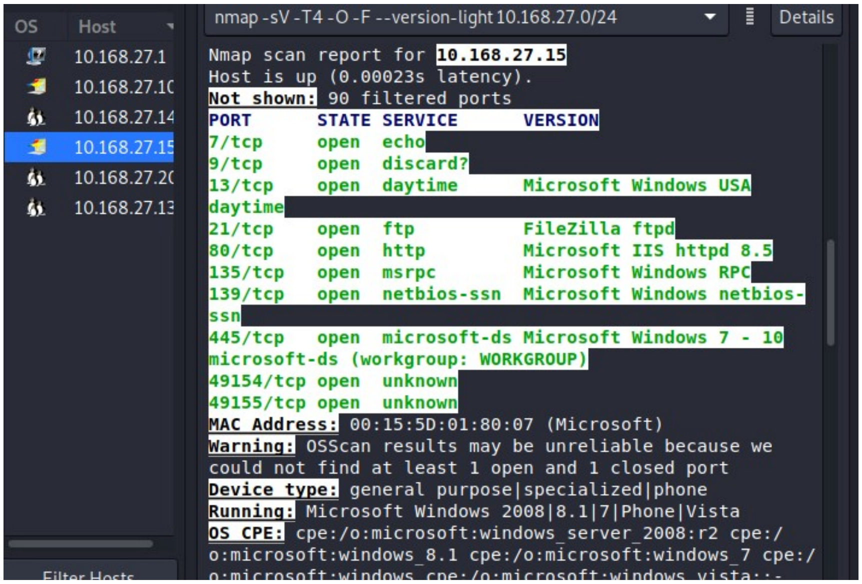
Host: 10.168.27.15

Operating System: Windows Server 2008

Open Ports: 7; 9; 13; 21; 80; 135; 139; 445; 49154; 49155

Vulnerable Port: 80 HTTP

Implication: unencrypted causing attackers to access the user systems and data



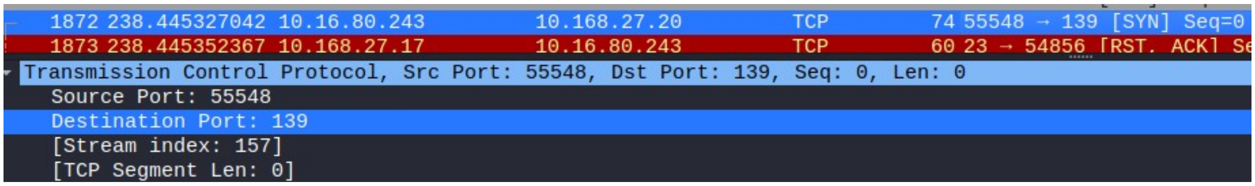
```
nmap -sV -T4 -O -F --version-light 10.168.27.0/24
```

```
Nmap scan report for 10.168.27.15
Host is up (0.00023s latency).
Not shown: 90 filtered ports
PORT      STATE SERVICE      VERSION
7/tcp     open  echo
9/tcp     open  discard?
13/tcp    open  daytime      Microsoft Windows USA
daytime
21/tcp    open  ftp          FileZilla ftpd
80/tcp    open  http         Microsoft IIS httpd 8.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-
ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10
microsoft-ds (workgroup: WORKGROUP)
49154/tcp open  unknown
49155/tcp open  unknown
MAC Address: 00:15:5D:01:80:07 (Microsoft)
Warning: OSScan results may be unreliable because we
could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/
o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/
o:microsoft:windows cpe:/o:microsoft:windows_vista::-
```

C. Anomalies found running Wireshark:

1st Anomaly

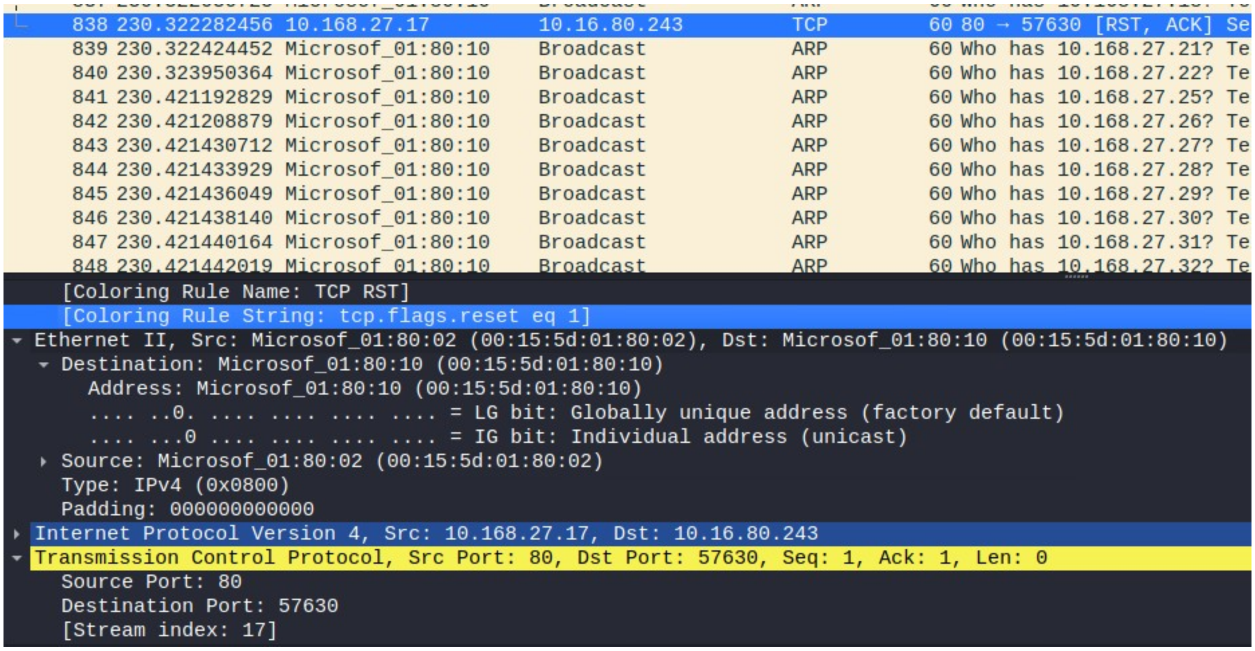
Use of NetBios Port 139. A DoS vulnerability exist when improperly utilizing port 139; also can allow a user to read or write remote computer systems.



```
 1872 238.445327042 10.16.80.243          10.168.27.20          TCP         74 55548 → 139 [SYN] Seq=0
 1873 238.445352367 10.168.27.17          10.16.80.243          TCP         60 23 → 54856 [RST, ACK] Se
Transmission Control Protocol, Src Port: 55548, Dst Port: 139, Seq: 0, Len: 0
   Source Port: 55548
   Destination Port: 139
   [Stream index: 157]
   [TCP Segment Len: 0]
```

2nd Anomaly

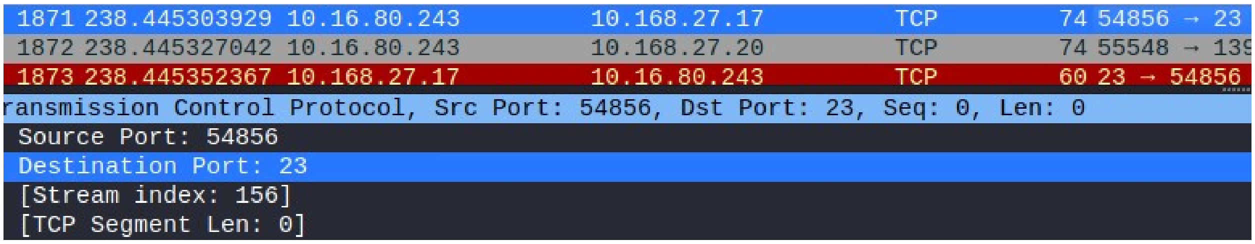
Use of Source HTTP Port 80. HTTP is unencrypted causing attackers to access the user systems and data; leak and tamper with sensitive data.



```
  838 230.322282456 10.168.27.17          10.16.80.243          TCP         60 80 → 57630 [RST, ACK] Se
  839 230.322424452 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.21? Te
  840 230.323950364 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.22? Te
  841 230.421192829 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.25? Te
  842 230.421208879 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.26? Te
  843 230.421430712 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.27? Te
  844 230.421433929 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.28? Te
  845 230.421436049 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.29? Te
  846 230.421438140 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.30? Te
  847 230.421440164 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.31? Te
  848 230.421442019 Microsof_01:80:10     Broadcast             ARP         60 Who has 10.168.27.32? Te
    [Coloring Rule Name: TCP RST]
    [Coloring Rule String: tcp.flags.reset eq 1]
 Ethernet II, Src: Microsof_01:80:02 (00:15:5d:01:80:02), Dst: Microsof_01:80:10 (00:15:5d:01:80:10)
   Destination: Microsof_01:80:10 (00:15:5d:01:80:10)
     Address: Microsof_01:80:10 (00:15:5d:01:80:10)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Source: Microsof_01:80:02 (00:15:5d:01:80:02)
   Type: IPv4 (0x0800)
   Padding: 000000000000
 Internet Protocol Version 4, Src: 10.168.27.17, Dst: 10.16.80.243
 Transmission Control Protocol, Src Port: 80, Dst Port: 57630, Seq: 1, Ack: 1, Len: 0
   Source Port: 80
   Destination Port: 57630
   [Stream index: 17]
```

3rd Anomaly

Use of Telnet Port 23; Port 23 is used to connect to remote users computers. This port is unsecure. Telnet is vulnerable to brute-force and spoofing. Replaced with SSH



```
1871 238.445303929 10.16.80.243          10.168.27.17          TCP          74 54856 → 23
1872 238.445327042 10.16.80.243          10.168.27.20          TCP          74 55548 → 139
1873 238.445352367 10.168.27.17          10.16.80.243          TCP          60 23 → 54856
ransmission Control Protocol, Src Port: 54856, Dst Port: 23, Seq: 0, Len: 0
 Source Port: 54856
 Destination Port: 23
 [Stream index: 156]
 [TCP Segment Len: 0]
```

D. Potential implications of not addressing *each* of the anomalies:

1) Implications of NetBios: **CVE-2017-0174** if improperly configured it allows a DoS vulnerability. (cvedetails)

2) Implication of HTTP: **CVE-2019-6579** and attacker on the webserver could execute system commands with administrative privileges. Security vulnerability could be exploited by and unauthorized attacker with network access to the affected service. (NIST)

3) Implication of Telnet: **CVE-2015-3954** give unauthorized users root privileges. (cvedetails)

E. Recommend solutions:

NetBios Port 139 Recommended resolution for NMAP and Wireshark:

NetBios is a listening port, “TCP Port 139 is one of the highest-risk ports on the network and you may need to disable the port 139 to avoid the WannaCry ransomware attack”, stated Helia.

HTTP port 80 recommended resolution for NMAP and Wireshark:

HTTP port 80 is less secure protocol. The use of HTTPS TLS server on 443 is more secure because it is an encrypted connection. “HTTPS Port 443 was officially pushed in RFC 1700 and solicited by Kipp E.B Hickman.” (RFC)

SSH Port 22 Recommendation resolution for NMAP:

Attackers look for open ports like port 22 to gain access to server. It is good practice to disable unused ports. “Port 22 is a default port for SSH connections and every hacker trying to access your SSH server will attach this port; changing the port adds extra security layer to the SSH connections.” (Rahul)

Telnet Port 23 Recommendation resolution for Wireshark:

SSH replaced Tenet. “SSH serves the same primary function as Telnet but does so in a more secure way.” SSH provides secure access on unsecure networks, reasoning why SSH should be used over Telnet. (Kovacevic, Aleksandar)

Works Cited

"CVE-2015-3954 : Hospira Plum A+ Infusion System Version 13.4 and Prior, Plum A+3 Infusion System Version 13.6 and Prior, and Symbiq Infu." *Www.cvedetails.com*, www.cvedetails.com/cve/CVE-2015-3954/. Accessed 29 Apr. 2023.

Helia. "Disable Port 139 and Avoid WannaCry Ransomware on Windows 10, 8.1, 8, 7, Vista, XP | Driver Talent." *Www.drivethelife.com*, 24 June 2022, www.drivethelife.com/disable-port-139-avoid-wannacry-ransomware-windows-10-8-7-vista-xp/.

Hickman, Kipp . "RFCs 1700 - 1799 Index." *Www.potaroo.net*, www.potaroo.net/ietf/html/rfc1700-1799.html. Accessed 29 Apr. 2023.

"NVD - Cve-2019-6579." *Nvd.nist.gov*, 17 Apr. 2019, nvd.nist.gov/vuln/detail/cve-2019-6579.

Rahul. "How to Secure SSH Server – TecAdmin." *Secure SSH Server*, 24 July 2021, tecadmin.net/how-to-secure-ssh-server. Accessed 29 Apr. 2023.

"Telnet vs. SSH: How Is SSH Different from Telnet?" *Knowledge Base by PhoenixNAP*, 20 May 2021, phoenixnap.com/kb/telnet-vs-ssh.