

Emerging Technologies in Cybersecurity Task 1

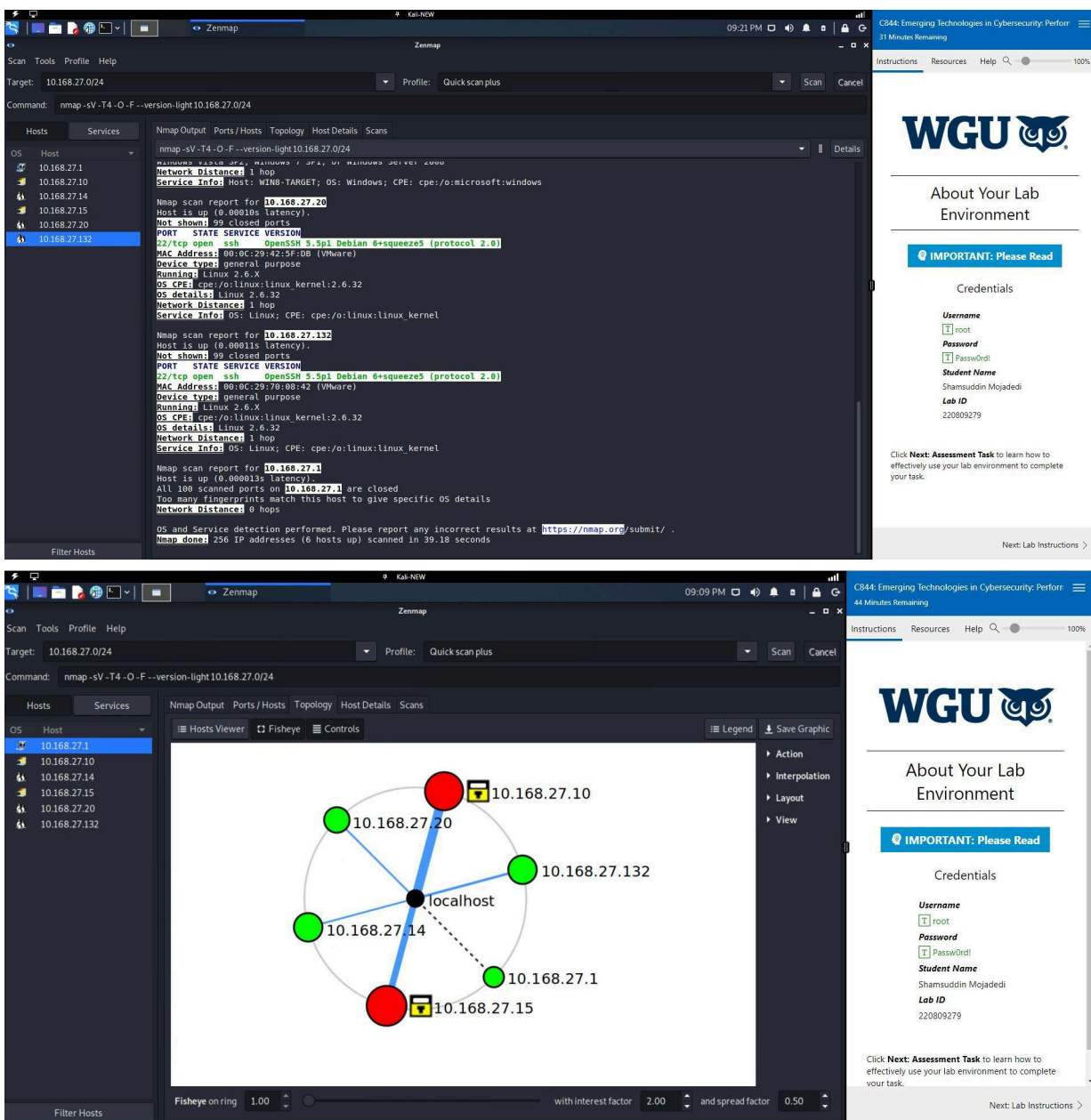
Emerging Technologies in Cyber Security

A. The Network Topology

After opening Zenmap, I ran a network scan of the domain 10.168.27.0/24, selected the Quick scan plus option, then clicked scan. The network scan showed a star topology with six devices connected to a local host.

Results:

- IP 10.168.27.20 – 1 Open Port – OS Linux 2.6.32
- IP 10.168.27.14 – 1 Open Port – OS Linux 2.6.32
- IP 10.168.27.132 – 1 Open Port – OS Linux 2.6.32
- IP 10.168.27.10 – 8 Open Ports – OS MS Windows Server 2012 R2
- IP 10.168.27.15 – 10 Open Ports – OS MS Windows Server 2008 R2 or Windows 8.1
- IP 10.168.27.1 – 0 Open Ports – OS Unknown



B. Summary of nmap/Zenmap Results

After Zenmap scan, The vulnerabilities and their implications based on the scan are as follows:

1. 10.168.27.132 and 10.168.27.20 (Linux 2.6.32) ssh service OpenSSH 5.5p1 Debian, (protocol 2.0).

Vulnerability: This version of OpenSSH grants a remote attacker access to itemize all accounts on the system while processing authentication requests.

Implication: Attackers can send specifically constructed series of packets and observe behavior of a server to detect the presence of a valid username. If this system isn't configured appropriately or a user account is set with a default password, a hacker can weaken the port and control the entire system.

The screenshot shows the Zenmap application interface. The top bar includes the title 'Zenmap' and a status bar with '09:21 PM' and '31 Minutes Remaining'. The main window is divided into several sections:

- Target:** 10.168.27.0/24
- Command:** nmap -sV -T4 -O -F --version-light 10.168.27.0/24
- Hosts List:** A list of IP addresses: 10.168.27.1, 10.168.27.10, 10.168.27.14, 10.168.27.15, 10.168.27.20, and 10.168.27.132. The host 10.168.27.132 is selected.
- Output Pane:** Displays the scan results for the selected host. The output includes:
 - OS: Linux 2.6.32
 - Network Distance: 1 hop
 - Service Info: Host: WIN8-TARGET; OS: Windows; CPE: cpe:/o:microsoft:windows
 - SSH scan report for 10.168.27.20: Host is up (0.000106s 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:29:42:5F:0B (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.
 - SSH scan report for 10.168.27.132: Host is up (0.000115s 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:29:70:03:42 (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.
 - SSH scan report for 10.168.27.1: Host is up (0.0000135s 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 39.18 seconds

The right sidebar contains the WGU logo, 'About Your Lab Environment', an 'IMPORTANT: Please Read' button, and a 'Credentials' section with fields for Username (root), Password (Password!), Student Name (Shamsuddin Mojadedi), and Lab ID (220909279). At the bottom, there is a 'Next: Lab Instructions >' button.

C. Anomalies found when running Wireshark

In this section I analyzed anomalies that are found by executing a scan using Wireshark Pcap1.pcapng.

1. The first thing I noticed was that an external IP address 10.16.80.243 (from the 10.168.27.0/24 network) attempts to browse machines on the network. This is a kind of Nmap scan will reveal what ports and services are running on which host

The image shows a Wireshark packet capture analysis of a scan from 10.16.80.243 to 10.168.27.10. The packet list shows a series of TCP packets from 10.16.80.243 to 10.168.27.10, all with the same source port (5555) and destination port (80). The packet details pane shows the selected packet (No. 391) with the following information:

- Version: 4
- Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 40
- Identification: 0xaa32 (43570)
- Flags: 0x00
- Fragment Offset: 0
- Time to Live: 30
- Protocol: TCP (6)
- Header Checksum: 0x68e9 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 10.16.80.243
- Destination Address: 10.168.27.10

The packet bytes pane shows the raw data of the packet, which is a TCP Reset (RST) packet with the following flags: RST, FIN, PSH, URG. The sequence number is 1024, and the window size is 0. The packet length is 40 bytes.

On the right side of the image, there is a sidebar for WGU (Western Governors University) with the following information:

- About Your Lab Environment
- IMPORTANT: Please Read
- Credentials
- Username: root
- Password: Password
- Student Name: Shamsuddin Mojadedi
- Lab ID: 220609279

At the bottom of the sidebar, there is a link to the Next Lab Instructions.

- It appears that an unknown device is attempting to receive anonymous verification to the network. Typical FTP exposures are considered unsecured and unencrypted protocols. This protocol can take over effortless access into the network, which is what an intruder could observe in their network scan to exploit.

The screenshot displays a Kali Linux desktop environment. The main window is Wireshark, showing a capture of an FTP session. The packet list on the left shows several FTP packets, with packet 21 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP). The packet bytes pane at the bottom shows the raw data of the selected packet.

On the right side of the screen, there is a sidebar for the WGU lab environment. It includes the WGU logo, the text "About Your Lab Environment", an "IMPORTANT: Please Read" button, a "Credentials" section with fields for Username, Password, and Student Name, and a "Lab ID" field. At the bottom of the sidebar, there is a "Next: Lab Instructions" button.

D. Implications of anomalies not getting addressed

1. The next implication of anomaly is the TCP protocol, it employs network congestion avoidance. However, the vulnerabilities include denial of service, connection hijacking, TCP veto and reset attacks. Additionally, TCP cannot guard a segment against message modification attacks, eavesdropping or unauthorized access.
2. The main issue. FTP is vulnerable to spoofing attacks such as man-in-the-middle; the hacker poses as a legitimate user or device on the network and intercepts the data. If Nmap scanning, and SMB brute forcing isn't stopped, the internal devices and services could be exploited to launch other attacks or steal private or critical information. One example of this is utilize usernames and passwords in different places within a network. Failing to act will result in data loss on the network that has been captured.

E. Recommend solutions *all* identified vulnerabilities or anomalies from Wireshark and Nmap.

B1. 10.168.27.14 (Linux 2.6.32) ssh service OpenSSH 5.5p1 Debian, (protocol 2.0).

Upgrade all instances of OpenSSH to version 7.8 for the stable distribution (stretch). (Debian, 2018)

C2. External IP address 10.16.80.243 (from the 10.168.27.0/24 network) attempts to browse machines on the network via TCP protocol.

The solution is to set up a firewall to discover network scans, or to add an IPS that would accordingly fail this kind of traffic. It's important to set up a firewall accurately to stop a network scan. (Shaw, 2019).

C3. Unknown device is trying to receive unidentified verification to the network.

Unsafe ports such as Telnet, SMB, and FTP should be obstructed for trying to maintain a network secure. The ports that those protocols go through should be blocked through the firewall or shift operations to SFTP a more secure version of the protocol. Secure protocols like SSH, SFTP and HTTPS must be used. Those protocols encrypt the data being sent. This step makes more difficult for an intruder to obtain a protocol vulnerability to operate and to access into the network. (US-CERT, 2017)

F. Sources

Debian Security Advisory (2018). DSA-4280-1 openssh -- security update. Retrieved from <https://www.debian.org/security/2018/dsa-4280ICMP>

Shaw, B. (2018). Disable TCP Port 135 and Avoid WannaCry Ransomware on Windows 10, 8.1, 8, 7, Vista, XP. Retrieved from <https://www.drivethelife.com/windows-drivers/disable-tcp-port-135-avoid-wannacry-ransomware-windows-10-8-7-vista-xp.html>

Speedguide (2014). Port 135 known port assignments and vulnerabilities. Retrieved from <https://www.speedguide.net/port.php?port=135>

US-CERT. (2017). SMB Security Best Practices. Retrieved from <https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices>