Emerging Technologies in Cybersecurity Task 1

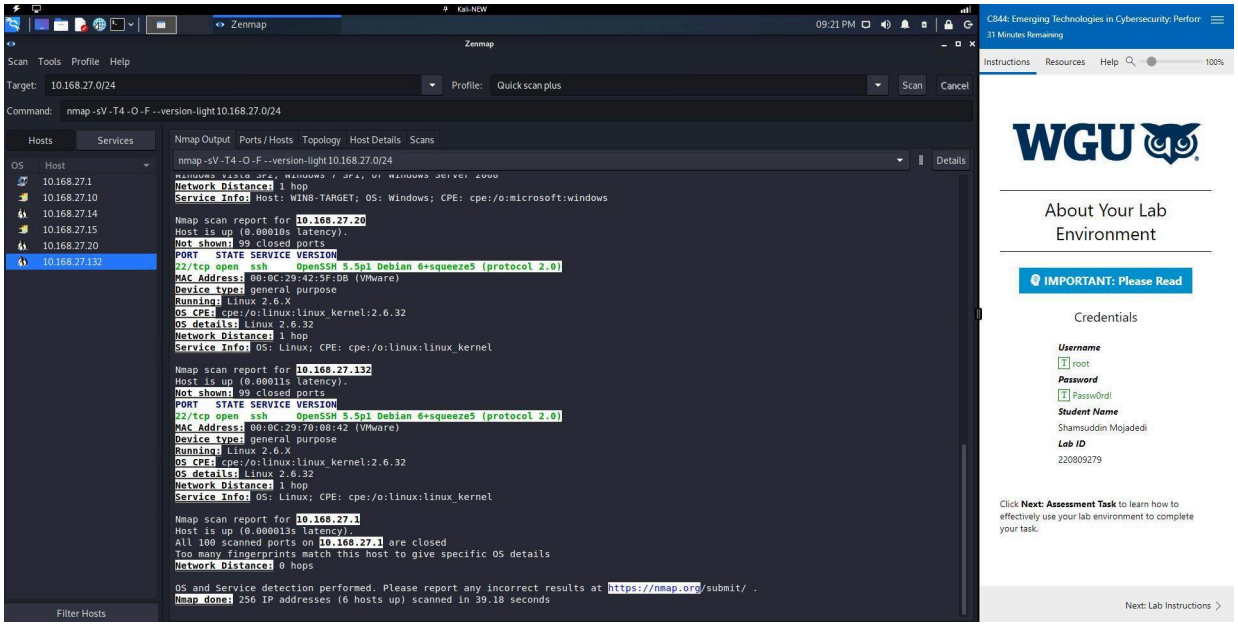
Emerging Technologies in Cyber Security

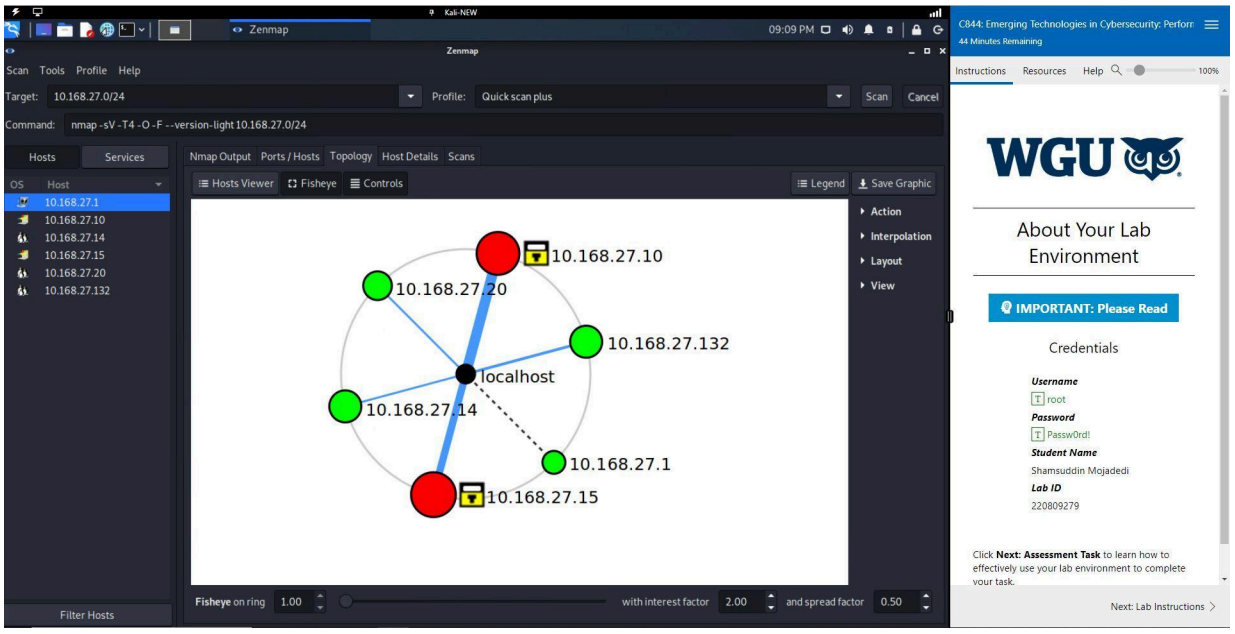
A. The Network Topology

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.

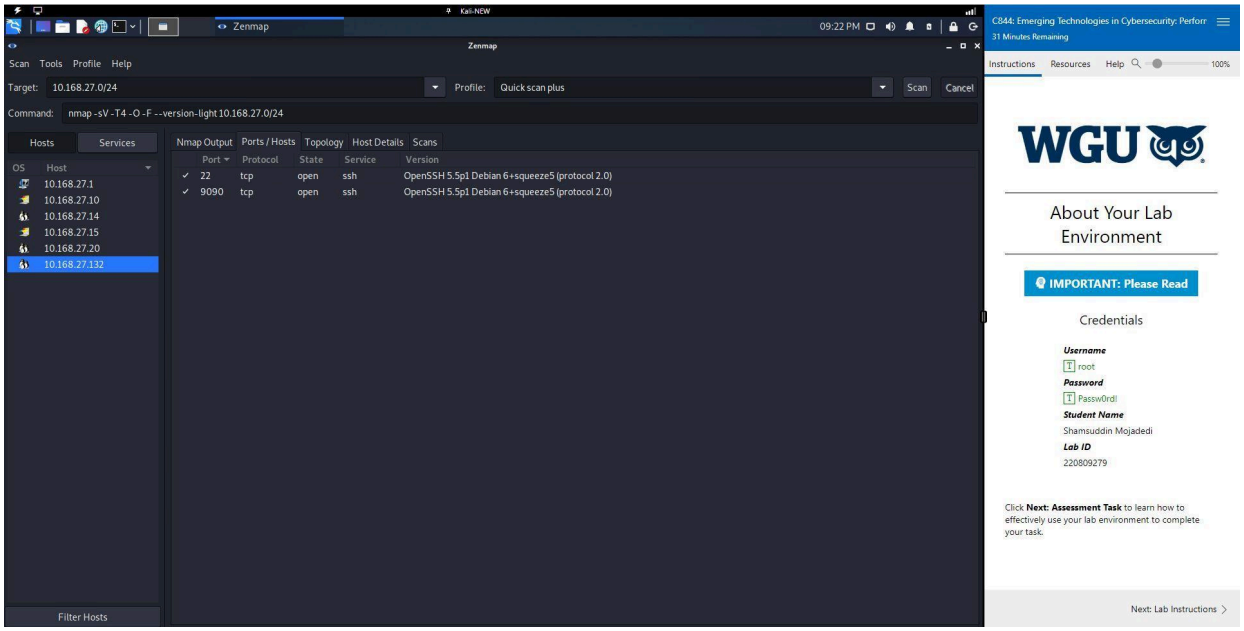
Results:

- 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





IOMoARcPSD|11292896



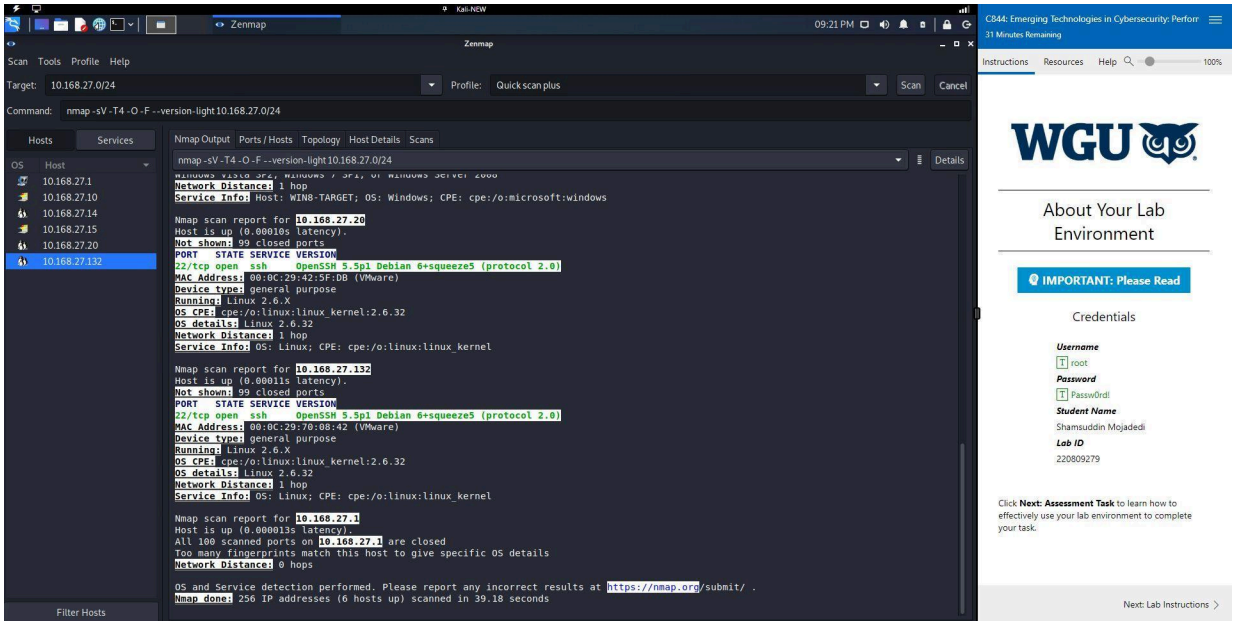
B. Summary of nmap/Zenmap Results

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.

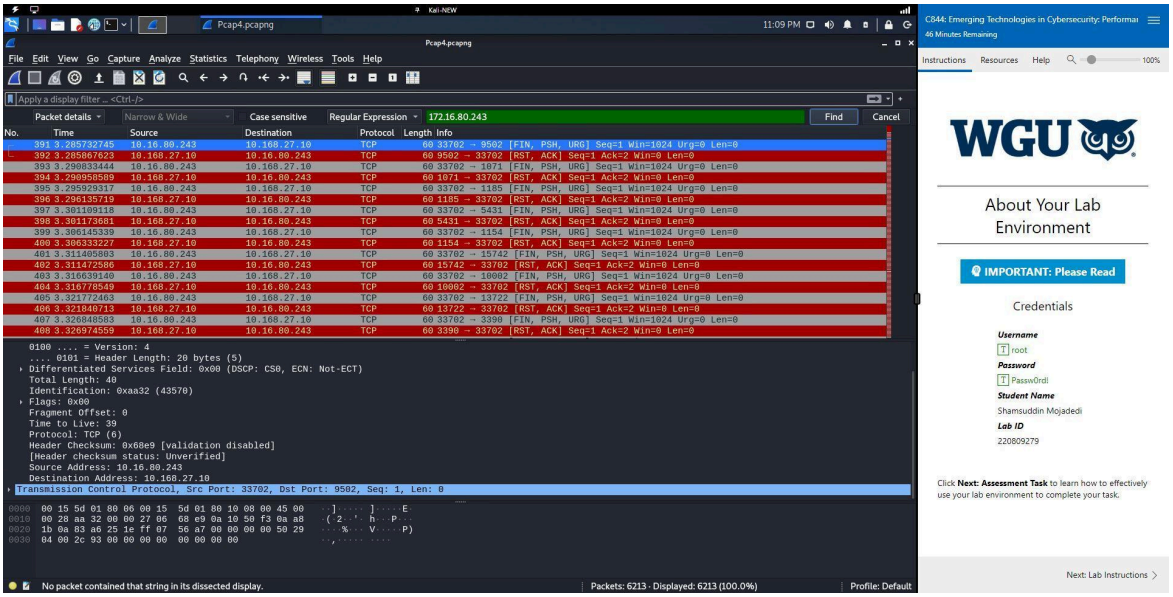
Implication: Attackers can send specifically constructed series of packets and observe behavior of a server to detect the presence of a valid username. If this system isn't configured appropriately or a user account is set with a default password, a hacker can weaken the port and control the entire system.



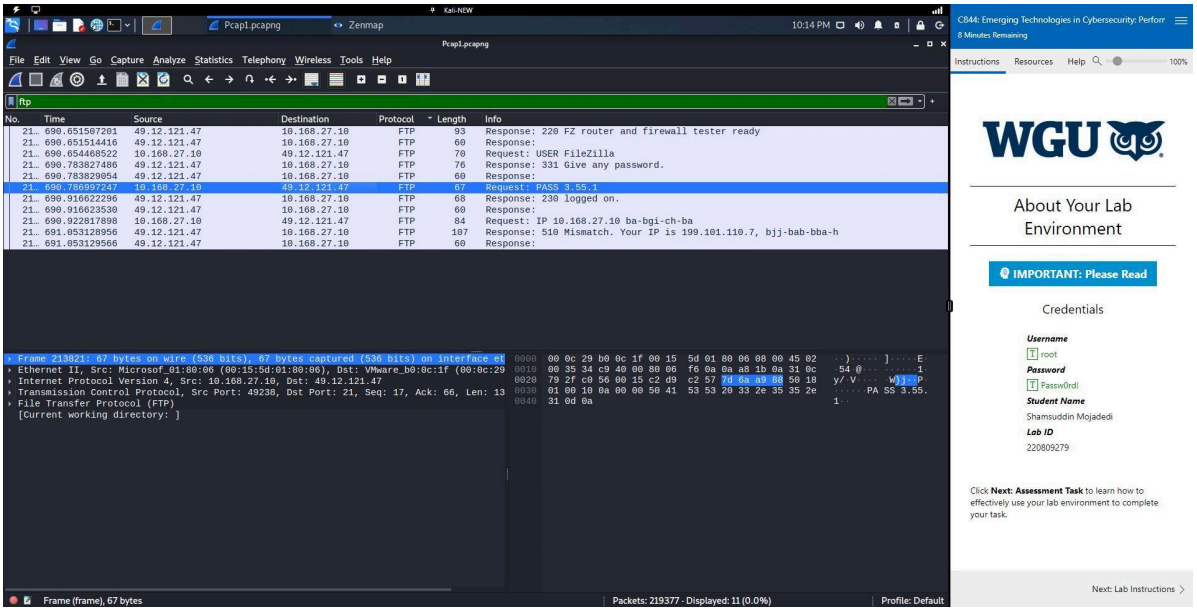
C. Anomalies found when running Wireshark

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



2. 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.



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). (Debain, 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

Debain 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