**Nmap/ZenMap Analysis**

1. There are 6 active host IPV4 private class A addresses in the 10.168.24.0/24 sub mask for the private network. Four hosts have less than 3 ports open (green), while 2 hosts have more than 6 ports open (red). The two red hosts have filtered ports, indicating the respective port status are unknown due to filtered packets (such as with a firewall).

A screenshot of a computer

Description automatically generated with medium confidence

1. Hosts on 10.168.27.10 and 10.168.27.15 both have Windows Server OS (2012/R2 and 2008 respectively) and open RPC ports.

Graphical user interface, text, application, Teams

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generated

Text

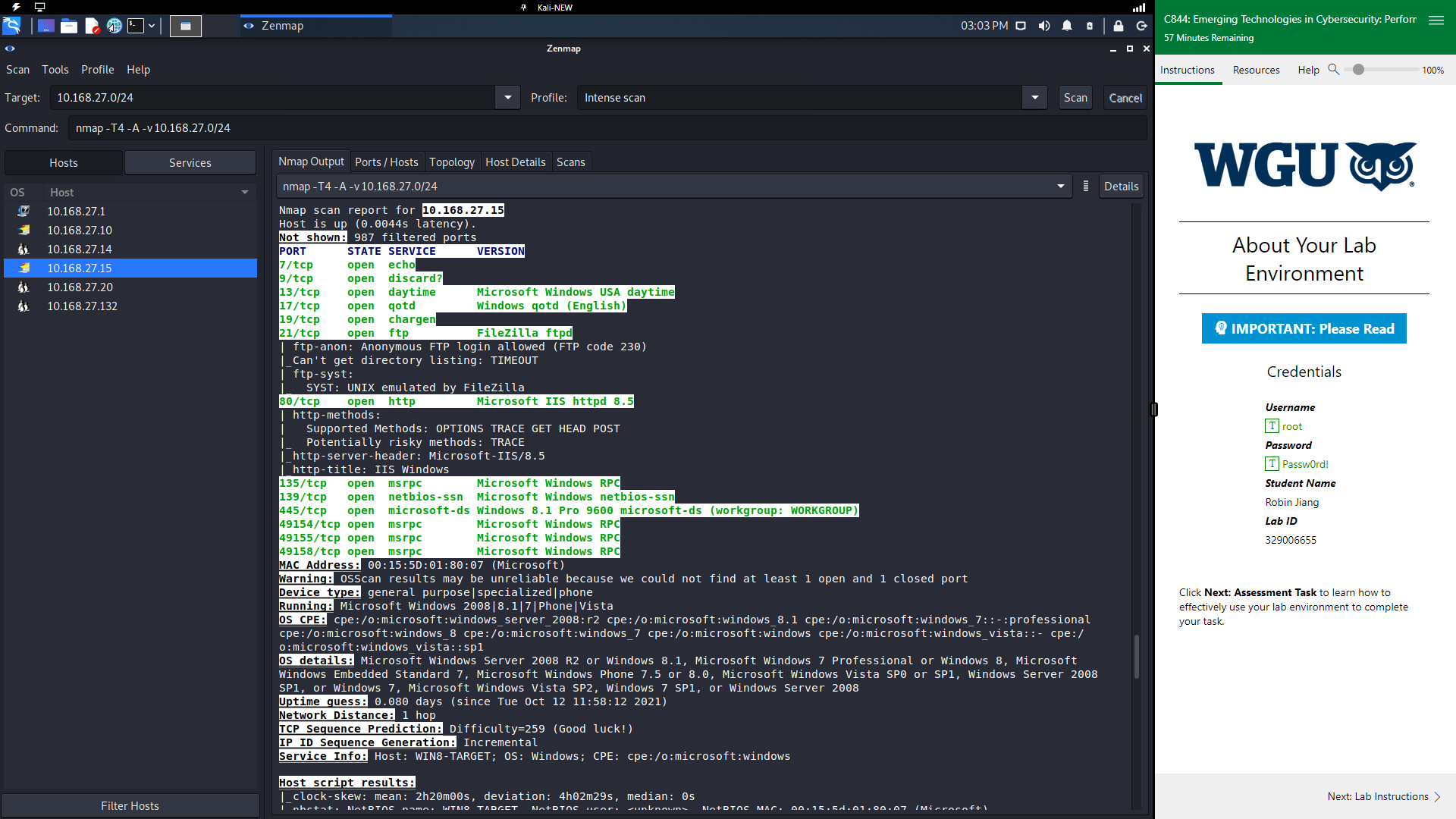
Description automatically generated

These conditions fall within the scope of a common vulnerability and exposure CVE-2020-11131. Task Schedulers on the respective host can fail to authenticate client connections correctly when pinning certificates2. Opportunities for attackers to utilize this vulnerability include when certificates are revoked, or when new hosts are added. Using the network within an enterprise mobility management (EMM) system could expose the network to multiple Bring Your Own Device (BYOD) or Company Owned Business Only/Personal Enabled (COBO/COPE) devices providing a larger attack surface for man in the middle (MITM) attack implementation of this vulnerability. Successful implementation of this vulnerability allows the attacker to run arbitrary code as an administrator, installing programs, view/effect data, and create new user accounts with full privileges3. Another related attack vector would be CVE-2017-11780 on SMBv1/2 ports on the Windows Server Hosts4. Nmap output revealed SMBv1 enabled with message signing disabled on both Windows hosts.

Text

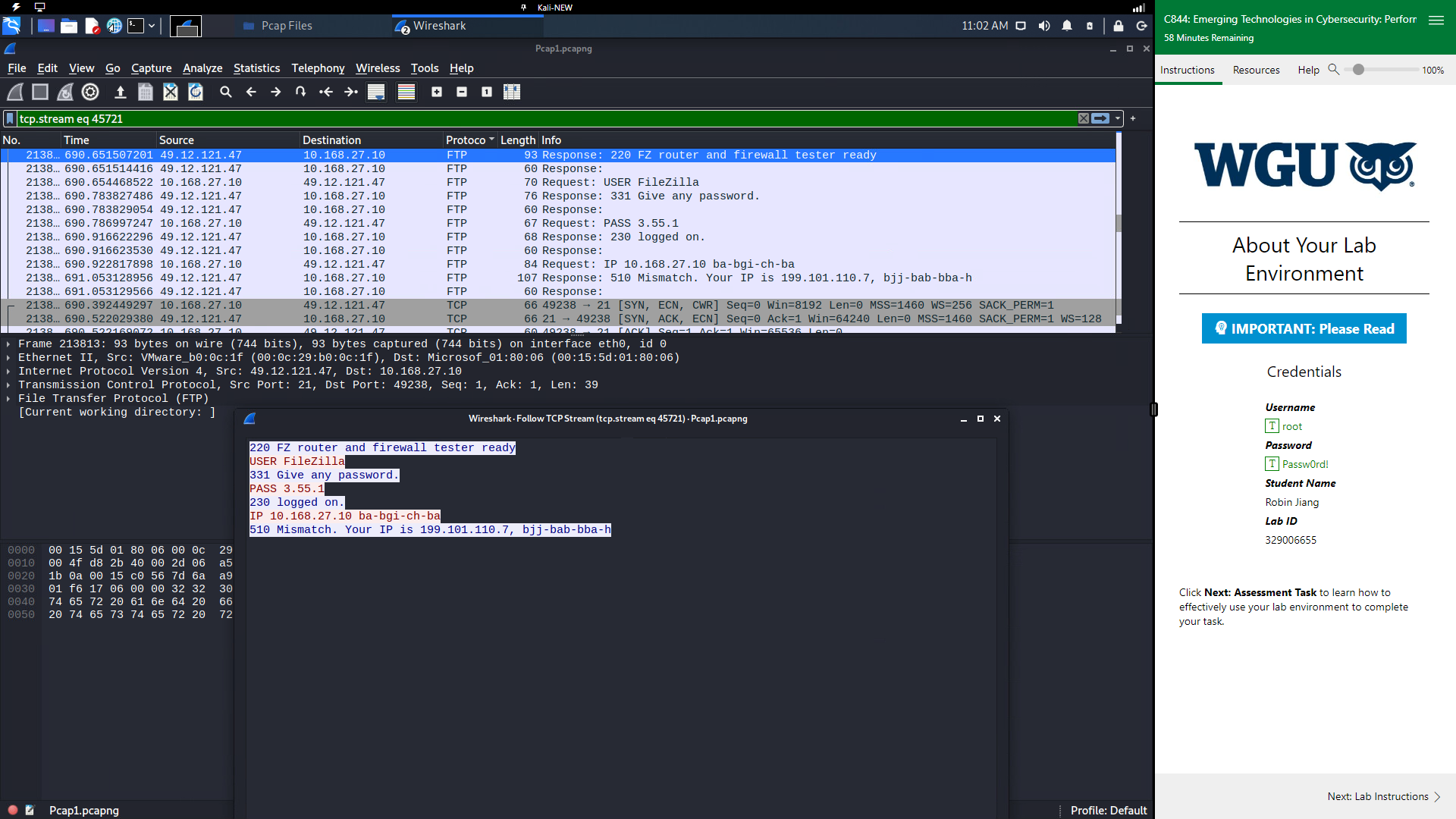
Description automatically generated

This makes the hosts highly susceptible to a MITM attack that may be trying to implement CVE-2020-1113 or any other SMBv1 related vulnerabilities. Host 10.168.27.15 has numerous ports that should be closed or filtered if the services are not needed. Port 7,9,13,17, and 19 use services that are seldom used or for testing purposes only and are open to numerous exploits such as denial of service (DOS) attacks with Metasploit Chargen Probe Utility5.



Port 21 uses FTP which uses cleartext transmissions only. Attackers can easily intercept any communications without encryptions, such as passwords. The same concept applies to port 80, as http is cleartext only and open to similar vulnerabilities.

**Wireshark Analysis**

1. Pcap1.pcapng has a TCP stream showing a FileZilla login attempt from 10.168.27.10 to 49.12.121.47.
2. 

The communications are cleartext, so the user and password are clearly labeled as “FileZilla” and “PASS 3.55.1”. Pcap3.pcapng has a similar HTTP stream showing multiple cleartext login and password attempts from 10.16.80.243 to 10.168.27.10 with username [admin@example.com](mailto:admin@example.com) and various passwords generated by the Wfuzz fuzzer.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Two attempts with passwords “@” and “200” are shown, with many others in subsequent attempts.

1. FTP was not designed to be encrypted, so confidential information can easily be observed by a potential threat sniffing the network for username and password combinations demonstrated in Wireshark. Websites with inadequate input validation are vulnerable to brute force or dictionary password attacks. Without any input controls attackers are free to attempt these exploits until direct intervention is taken.
2. Ensure both Windows servers are properly patched against CVE-2020-1113 while accounting for compatibility issues. Filtering RPC ports by using IPSEC protocol would reduce the foot printing efforts of attackers looking to implement CVE-2020-11136. IPSEC policies will provide encryption security of network traffic to and from the network. Disable SMBv1 on the Windows Server hosts if legacy compatibility is not an issue. Port 139 for NetBIOS SSN should be closed if it is only used for SMBv1 traffic7. Otherwise, message\_signing should be enabled and required for both SMBv1 and 2 to mitigate this attack vector. For the host on 10.168.27.15, unless ports 7,9,13,17, and 19 are needed for the network, these ports should be closed as part of device hardening good practice. Port 21 should be closed and secure alternatives such as FTPS, SFTP, or FTP over SSH should be used with their respective ports depending on the needs of the network. Port 443 for HTTPS should be opened to provide a secure alternative to port 80 HTTP. Websites that require login credentials should have more robust input validation, such as utilizing CAPTCHA or multiple factor authentication (MFA) to mitigate password exploit attempts.
3. *CVE-2020-1113*. CVE. (n.d.). Retrieved January 8, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1113>
4. *Common weakness enumeration*. CWE. (n.d.). Retrieved January 8, 2023, from <https://cwe.mitre.org/data/definitions/295.html>
5. *Security Update Guide - Microsoft Security Response Center*. (n.d.). Retrieved January 8, 2023, from <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1113>
6. *CVE-2017-11780*. CVE. (n.d.). Retrieved January 8, 2023, from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11780
7. *Chargen Probe Utility*. Rapid7. (n.d.). Retrieved January 9, 2023, from https://www.rapid7.com/db/modules/auxiliary/scanner/chargen/chargen\_probe/
8. *Microsoft*. Microsoft Support. (n.d.). Retrieved January 8, 2023, from https://support.microsoft.com/en-us/topic/how-to-configure-rpc-to-use-certain-ports-and-how-to-help-secure-those-ports-by-using-ipsec-2a94b798-063a-479a-8452-9cf07ac613d9
9. Deland-Han. (n.d.). *How to detect, enable and disable smbv1, smbv2, and SMBv3 in windows*. Microsoft Learn. Retrieved January 9, 2023, from https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server