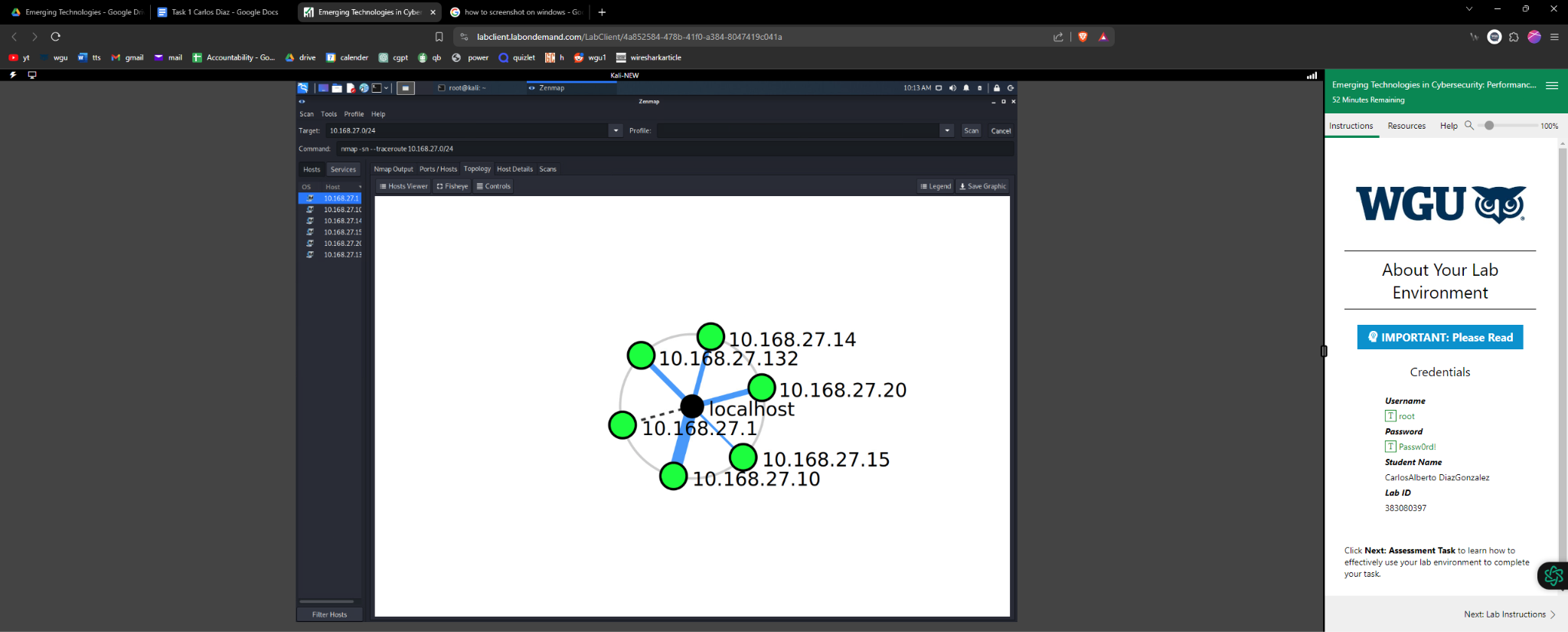
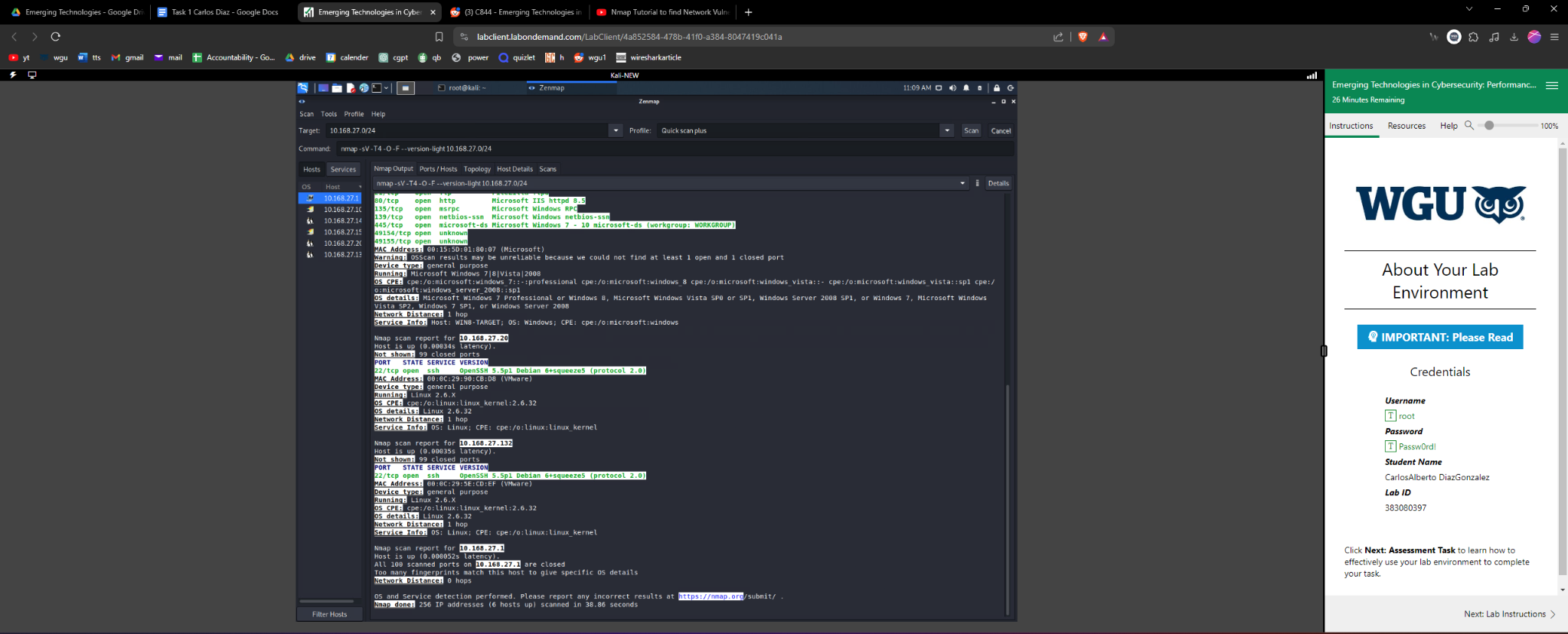
**A.**

I first launched the kali linux root emulator after that I typed Zenmap on the terminal, and then finally I scanned the domain's network 10.168.27.0/24.I selected the Quick scan plus because the intense scan was taking too long and was not sure if my computer was the issue, then continued to scan. The network scan showed a star topology with six devices connected to a local host.

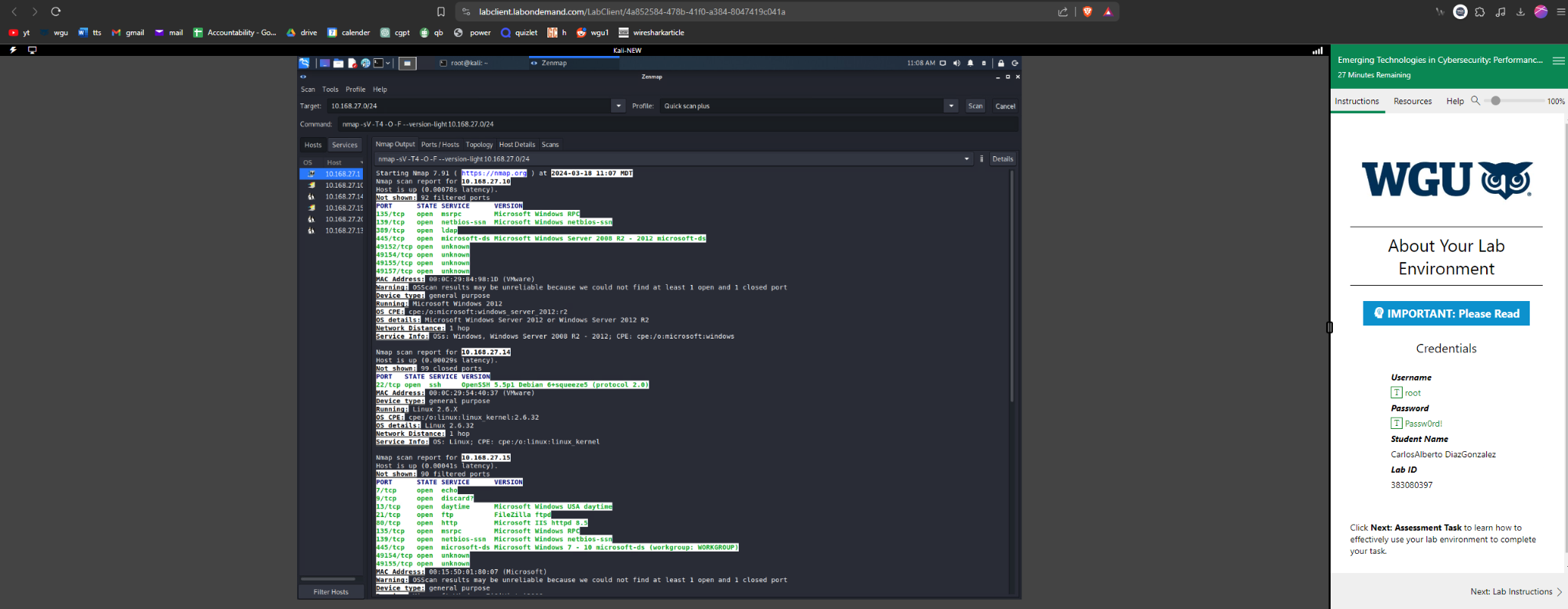
The results were :IP 10.168.27.20 with 1 Open Port, OS Linux 2.6.32 IP 10.168.27.14 1 Open Port, OS Linux 2.6.32IP 10.168.27.132, 1 Open Port, OS Linux 2.6.32IP 10.168.27.10, 8 Open Ports, OS MS Windows Server 2012 R2IP 10.168.27.15, 10 Open Ports, OS MS Windows Server 2008 R2 or Windows 8.1IP 10.168.27.1 0 Open Ports OS Unknown.



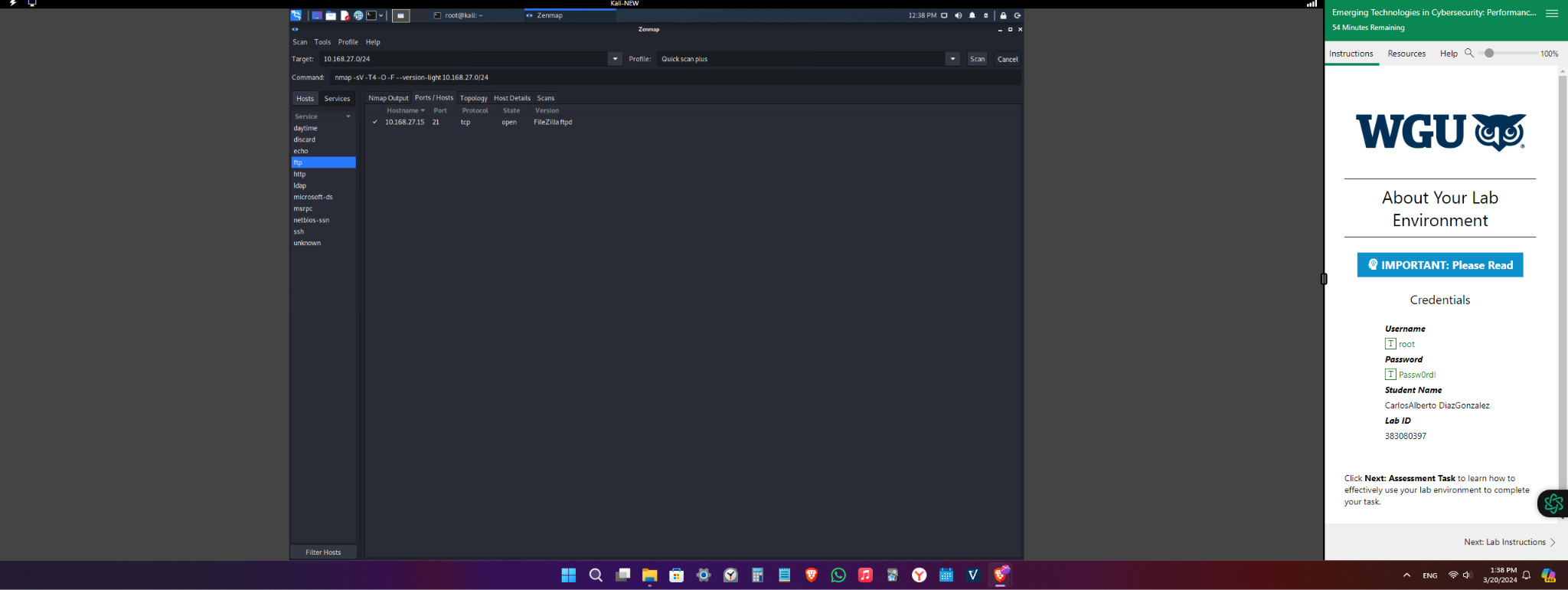
**B.**



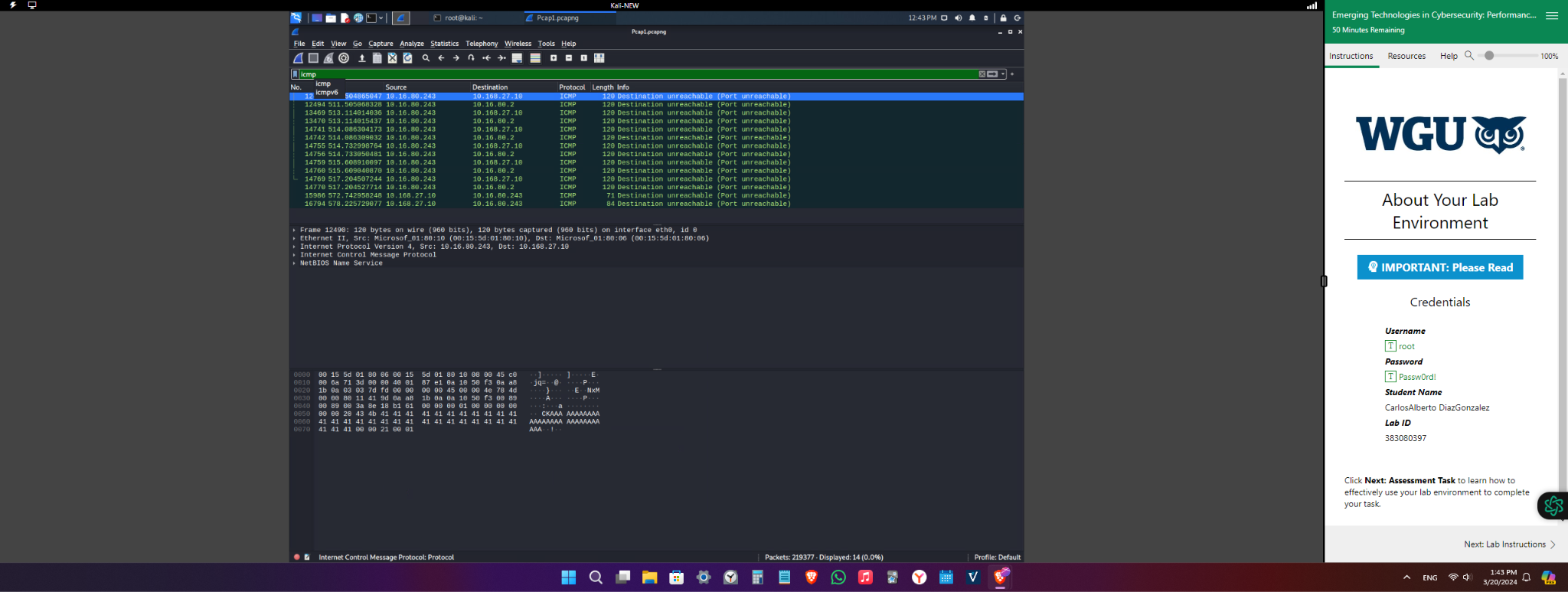
After the Zenmap scan was completed, I discovered a few problems. The scan identifies the following vulnerabilities and their consequences:1. SSH service 10.168.27.14 (Linux 2.6.32) over OpenSSH 5.5p1 (Debian, protocol 2.0). This specific version of OpenSSH enables a remote attacker to access all of the server accounts while the server is processing authentication requests. The result would be that an attacker can send a specifically designed sequence of packets and observe how a server reacts to see if a username is genuine. If a user account has a weak default password or if the system is configured incorrectly, a hacker can weaken the port and get access to the entire system.



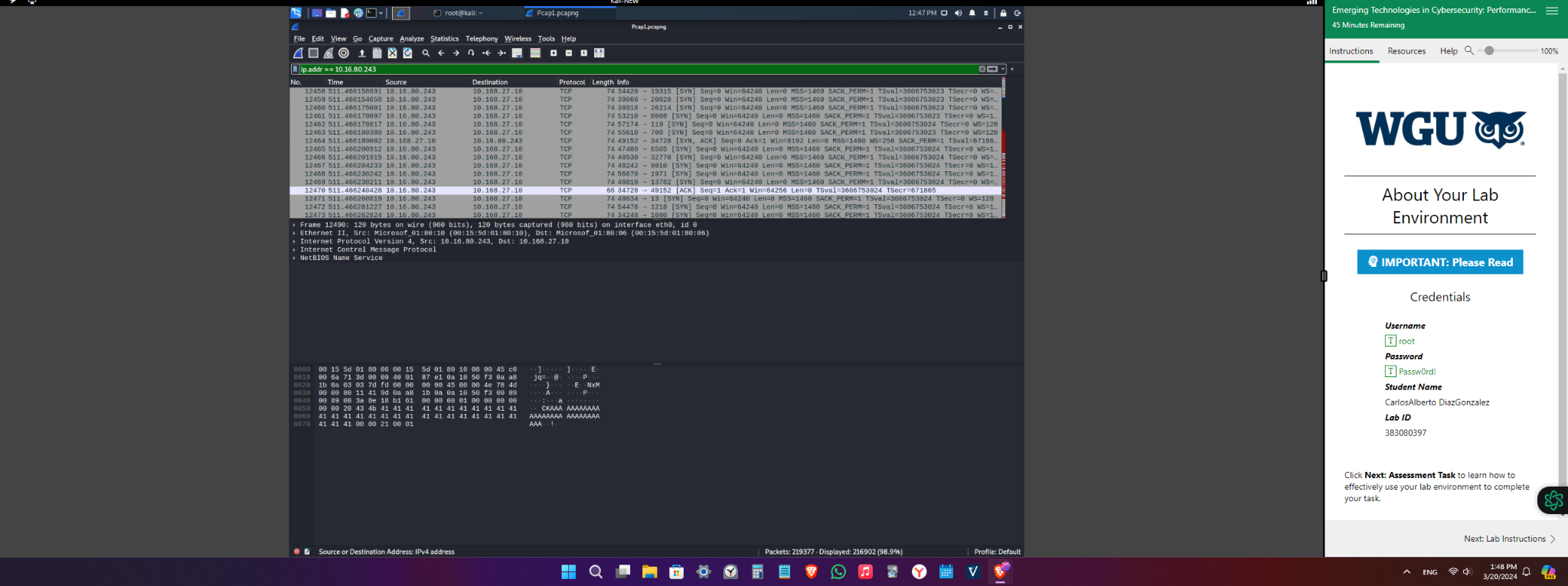
In the device 10.168.27.15 that is a Microsoft Windows Server 2008 R2 or Windows 8.1 Vulnerability: During the scan, ten open ports on this host were discovered. The msrpc port 135 concerning. It is possible for other computers to determine which ports on a server are utilized by services that can be accessed publicaly by using Microsoft Remote Procedure Call (RPC). The risk is that hackers can quickly determine which DCOM-related servers and services are running on a host machine by comparing them to known exploits using a tool like "epdump" (Endpoint Dump).



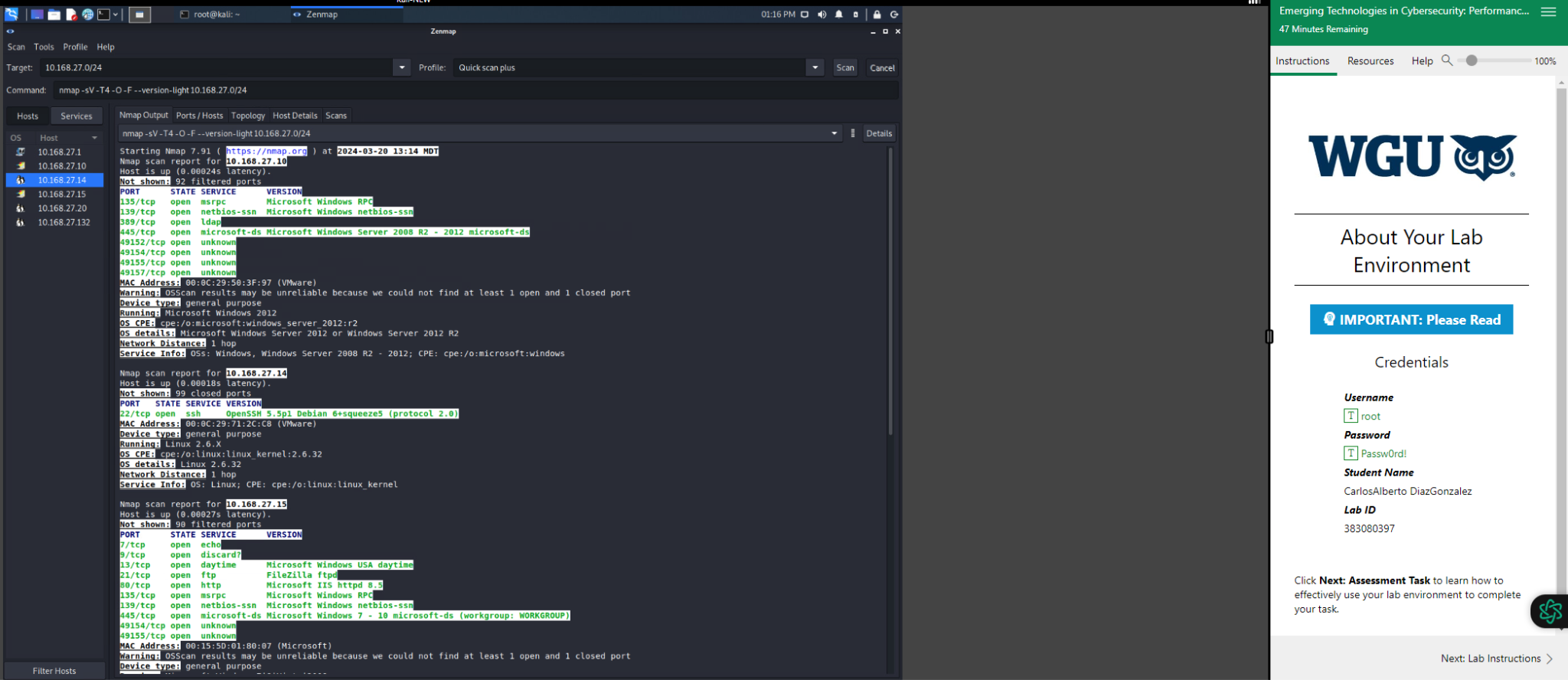
In device 10.168.27.15 which is a Microsoft Windows Server 2008 R2 or Windows 8.1, Port 21 OpenVulnerability FTP servers are connected to the network through port 21. Port 21 is a prime target for these vulnerabilities since these servers are susceptible to anonymous authentication, and cross-site scripting.Implication: Because FTP lacks encryption, anything that travels over it can be read if network traffic is sniffed at any point. This renders FTP considered insecure. This includes the account, password, and any supplied information. The attacker also has the ability to make a target machine crash, execute code, and directly elevate user permissions.



I noticed that 10.16.80.243 which is an external IP address associated with the 10.168.27.0/24 network, was making an effort to investigate devices within the network. You can see which hosts are using which ports and services using a Nmap scan of this type. In order to obtain anonymous verification, it looks like an unidentified device is trying to connect to the. Regular FTP exposures are seen as dangerous practices that don’t have encryption. This protocol can replace simple network access, which an attacker could see in their network scan and take advantage of.

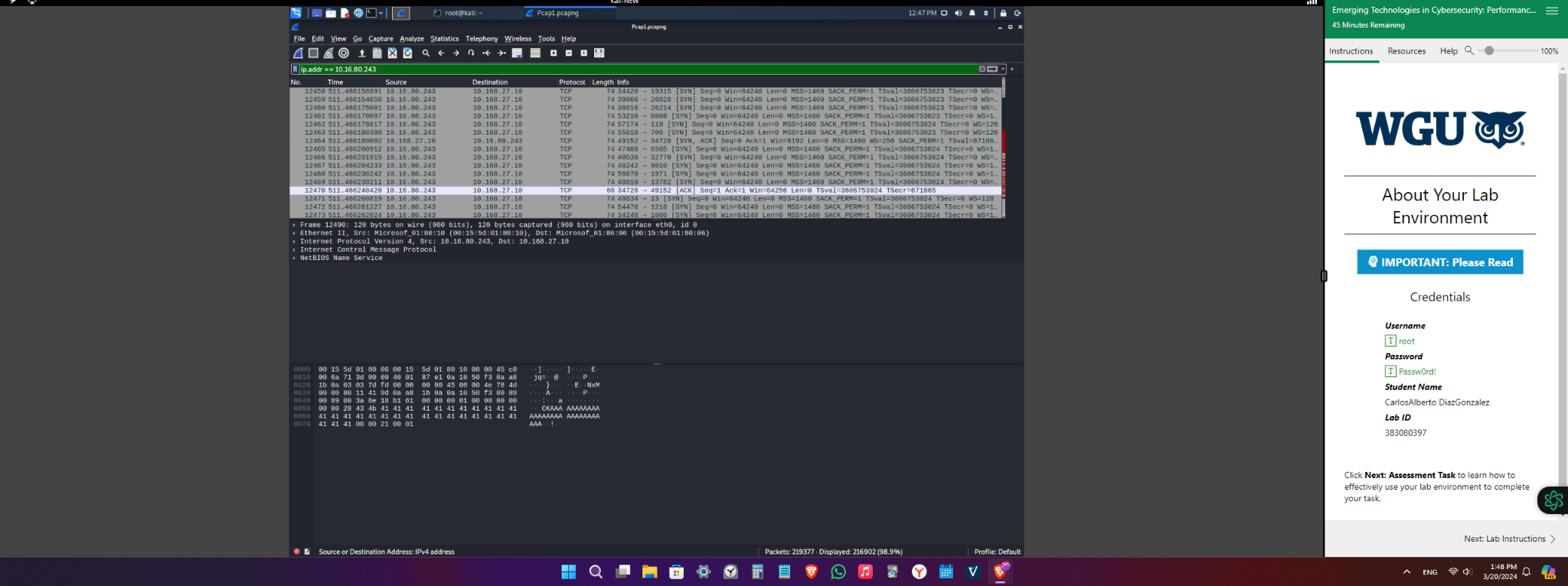


I found that the FileZilla FTP is running at 10.168.27.15 on port 21. FTP is a good target for password and username theft since it is an unsecure protocol that sends data over a network in clear text. Secure FTP should be used instead.



**C.**

The blocking of ICMP traffic was suspicious. ICMP requests were delivered in all in a short period and did not wait for a response from the system in the traffic that Wireshark displays. A reason this traffic could be blocked is a ddos attack.



I found unsafe ports on the network such as Telnet. Unfortunately the lab stopped working because I ran out of time and I could not screenshot in time.

**D.**

For the ICMP traffic this increases the risk of a Ping flood, which is a tactic used to launch a denial-of-service (DoS) attack. In a DoS, an attacker continuously sends ICMP queries without waiting for the targeted system to respond. The goal is to degrade system performance by consuming CPU resources and consuming incoming and outgoing bandwidth. The TCP protocol, which avoids network congestion, is the next odd impact. On the other hand, TCP veto, reset attacks, denial of service, and connection hijacking are a few of the weaknesses. Moreover, TCP cannot shield a segment from attacks that modify messages, obtain unauthorized access, or spy on communications. the primary problem. Man-in-the-middle attacks, in which a hacker poses as a reliable user or device on the network in order to intercept data, can occur with File Transfer Protocol (FTP).If Nmap scanning and SMB brute force are not stopped, the devices and services might be utilized to carry out more attacks or steal sensitive or private information. One example of this is when someone uses their username and password in multiple places inside a network. Inaction will result in losing collected data on the network.

**E.**

To run the ssh service OpenSSH 5.5p1 Debian (protocol 2.0) on the Linux 2.6.32-based device 10.168.27.14 (stretch stable distribution), we would need to update all OpenSSH instances to version 7.8. (Debian, 2018). Concerning the device on 10.168.27.15 - Windows 8.1 Port 135 or Microsoft Windows Server 2008 R2. In general, ports that are identified by the ports database as having known vulnerabilities at the firewall/NAT router edge of your network should be blocked from remote access. Port 135 in particular is open to ransomware and viruses and should instead use a secure port. Certain features (such Windows PCs, sharing, printers not showing up on a network, etc) might disappear if local ports are closed. MicrosoftServer 2008 R2 (Windows 8.1, 10.168.27.15) has a open Port 21 Install Microsoft AlternateTo fix a known problem with the security updates that were released on July 10, 2018, cumulative update packages for Windows 10 Standalone and preview rollup packages for all other supported Windows versions were provided. (MSRC). Ping Flood using ICMP. Completely stopping the ICMP protocol might not be the best idea in order to protect network equipment. Instead, by disabling a subset of ICMP types, network devices can have more exact control over the types of ICMP messages they can send, receive, and respond to. The functionality and kindness of the device should be taken into account while selecting the message types that ought to be permitted to send and receive data across a network. In-depth research should also be done to identify which communication kinds need to be allowed or restricted in order to strike the perfect balance between heightened security and maintaining a high degree of network performance. The 10.168.27.0/24 network's external IP address 10.16.80.243 makes TCP protocol-based attempts to connect to network machines. Adding an IDS would detect the traffic so someone could look over the traffic and an IPS that would reject this type of traffic or configuring a firewall to detect network scans are the two ways to address this problem. A firewall must be configured precisely in order to stop an examination of the network. When an unidentified device is attempting to connect to the network in an attempt to obtain an unidentified confirmation.If you want to keep your network secure, you should block unsafe ports like FTP, SMB, and Telnet. For transactions, switch to the more secure SFTP protocol, or set up a firewall to limit the ports that these protocols can use. It is imperative to utilize secure protocols like SSH, SFTP, and HTTPS. The data being sent is encrypted by these protocols. As a result, it will be harder for an attacker to use a protocol flaw to enter the network because it is not in clear text rather it is encrypted into a hash that needs a key.

**F.**

Falk, B. (2018, July 10). *Windows Firewall Denial of Service Vulnerability*. Security Update Guide - Microsoft Security Response Center. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2018-8206

Helia. (2022, June 24). *Disable TCP port 135 and avoid wannacry ransomware on Windows 10, 8.1, 8, 7, Vista, XP*. Driver Talent. https://www.drivethelife.com/disable-tcp-port-135-avoid-wannacry-ransomware-windows-10-8-7-vista-xp/

*Microsoft Windows 8.1 : Security vulnerabilities, Cves*. Microsoft Windows 8.1 : Security vulnerabilities, CVEs. (2024, January 6). https://www.cvedetails.com/vulnerability-list/vendor\_id-26/product\_id-26434/Microsoft-Windows-8.1.html