Milestone Final

Network & Vulnerability Report

ABC Manufacturing

Guysell Dixson

December 12, 2021

IT 320 Network Security

Instructor Anderson

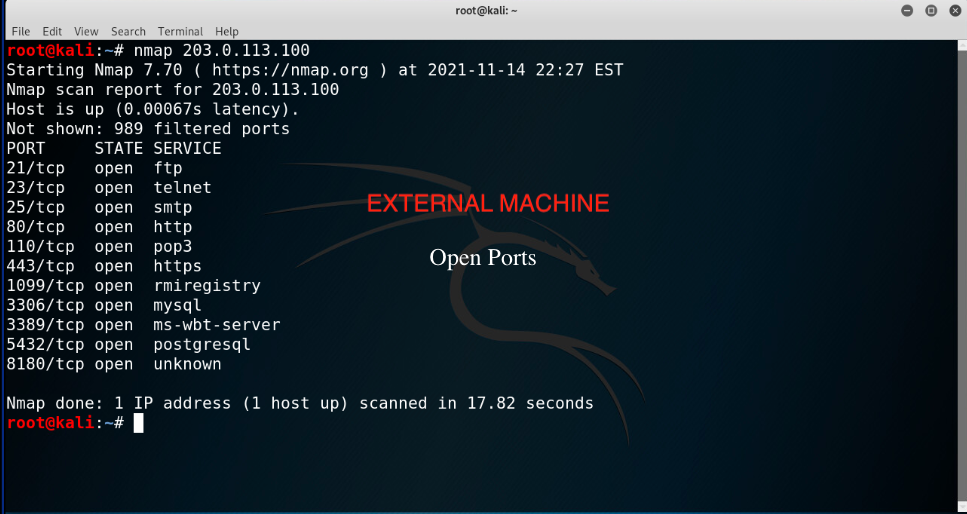
Southern New Hampshire University

**Introduction**

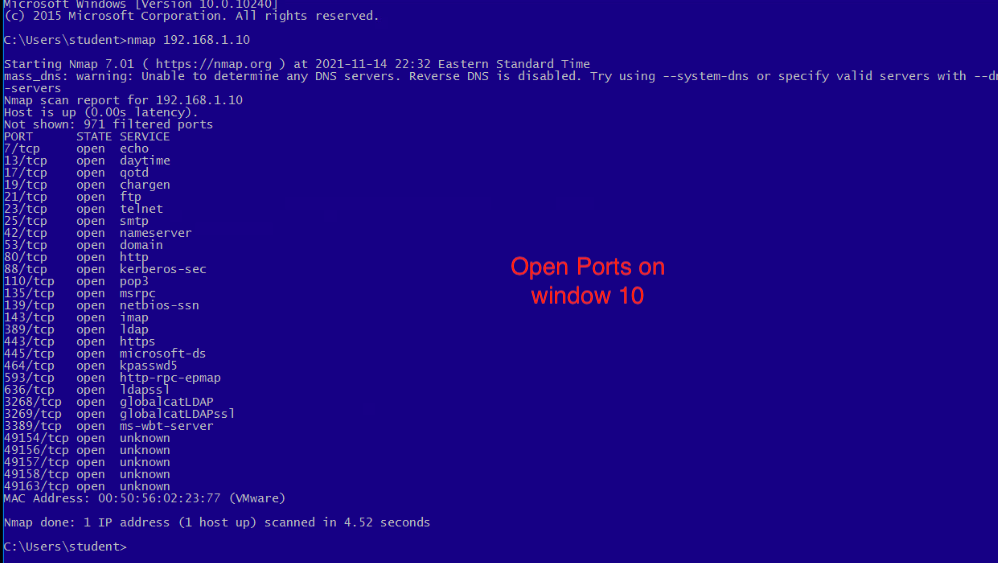
After doing a vulnerability and network assessment for ABC Manufacturing, the following sections will give feedback to the findings related to the firewall and open ports as it pertains to network security. The findings are just what has been discovered with the current settings and protocols that are in place. After scans have been ran and analysis have been done, recommendation to harden your network infrastructure will be recommended.

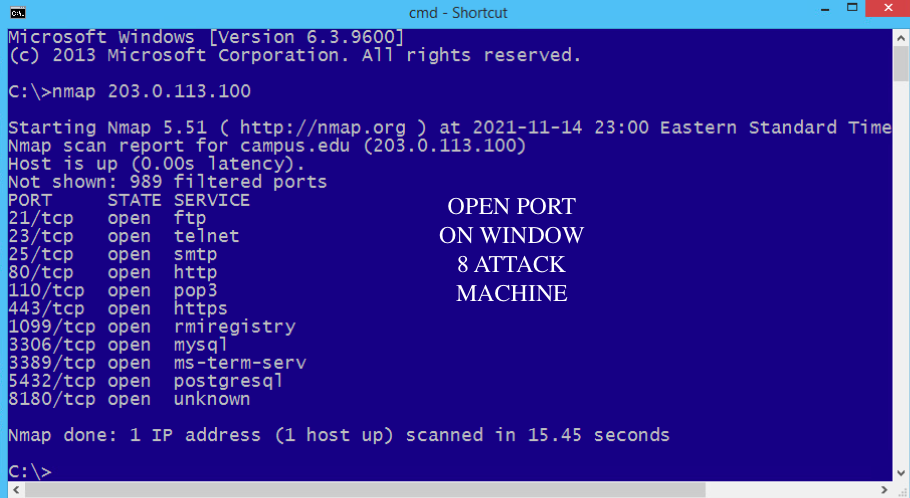
**Network Assessment**

After running a nmap on the Kali2 attack machine it was noticed that ports tcp/21 ftp, tcp/23 telnet, tcp/25 smtp, tcp/80 http, tcp/110 pop3, 1099/tcp rmiregistry, 2206/tcp mysql, 3389/tcp ms-wbt-server, 5432/tcp postgresql, 8188/tcp unknown ports are all open. With these ports open it allows for the proper incoming and outgoing packets. The threat to the attack machine is that without the proper configurations, these open ports will not block the need malicious packets that will come through. The position on the network also compromises the security of the network. The attack machines are in front of the firewall meaning that traffic comes through the attack machine before the firewall.



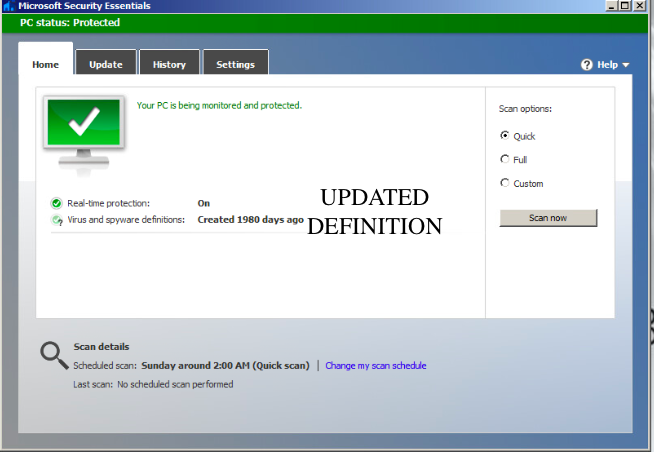
Upon scanning the windows 10, it is noticed that the several unnecessary ports are open. The following ports that are posing threats are 7/tcp echo, 13/tcp daytime, 17/tcp qotd, 19/tcp chargen and several unknown services. Again, if theses ports are not configured and closed these ports will lend to an open backdoor for hackers. This server has too many open ports and without a constant watch on the flow of traffic this poses a threat and to ABC manufacturing’s network security. Please reference the figure below to see more open and unused ports.

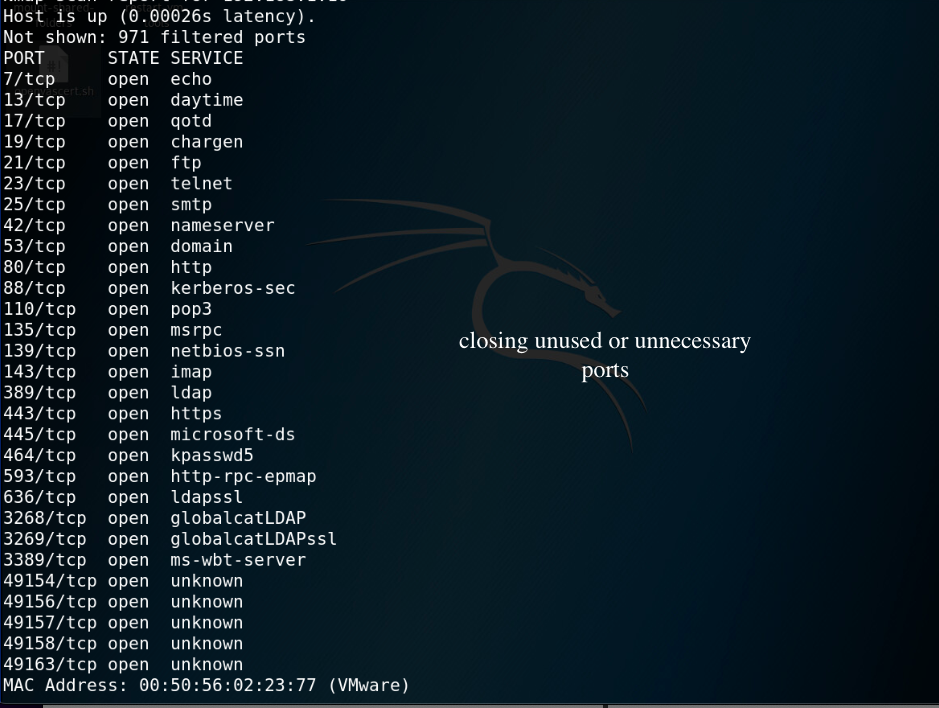
  
 A nmap scan was performed on the window 8.1 attack machine. The findings are below. The concerning port is the 8180/tcp unknown. The threat to this server will be configuration and making sure that the firewall is up to date.



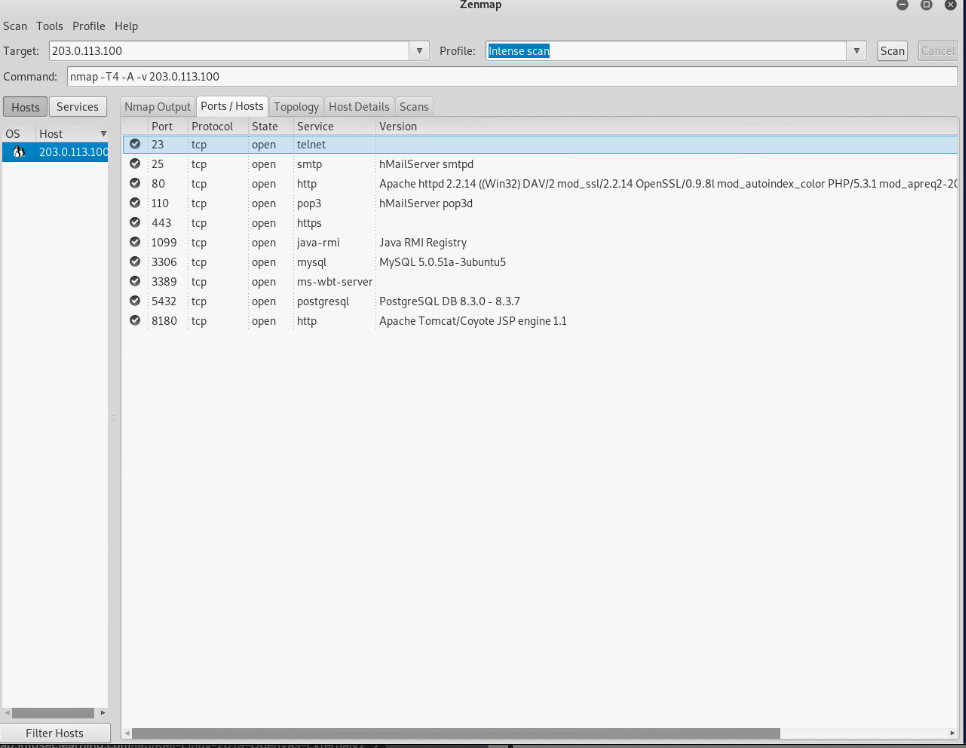
**Network Assessment: Malicious Software Protection**

After running a virus scan using the Microsoft Security Essential, it was found that the network was running on an outdated software. The definitions were not up to date. This could lead to newly developed malware and viruses to be able to pass through the firewall uncontested and wreak havoc upon the network. Making sure that this is consistently update will prevent the intrusion of unknown malware and viruses from gaining access within the infrastructure.

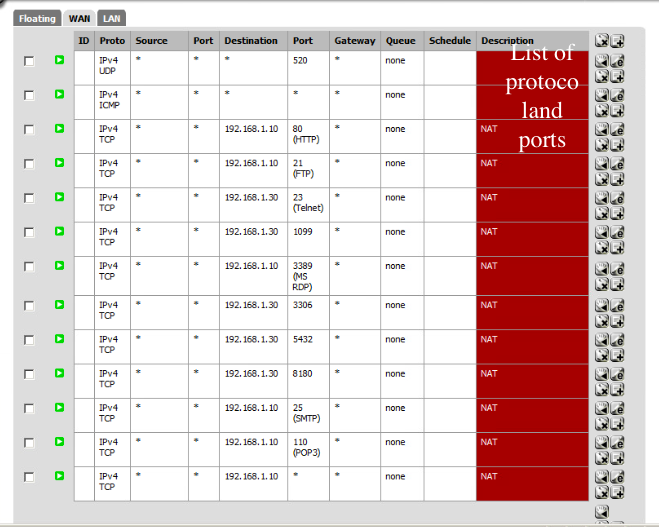


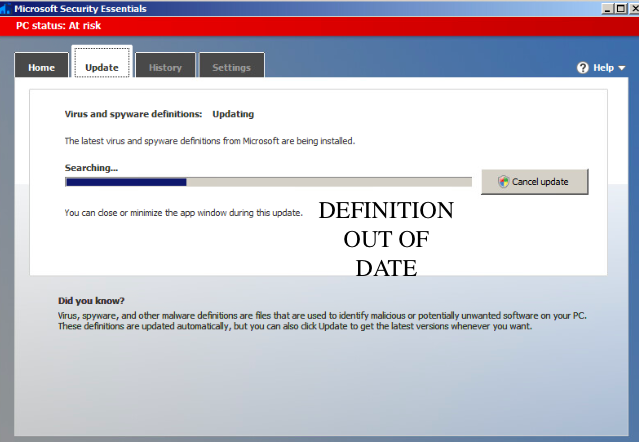
**Vulnerability Assessment** 

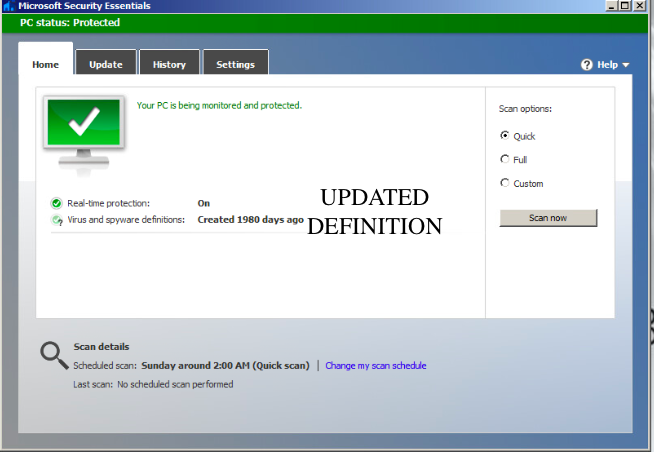
The above figure is a list of open ports that are being used. The threat of these port is that it gives multiple access points for a hacker to gain access into ABC’s network. These open ports are also running on IPv4 backed by NAT. This gives the traffic on certain ports a secure transit. The figure below shows what ports and protocols are using NAT to help with transport on the network. By using zenmap scan the I was able to see what host and ports are being used and what protocol are being ran.



Within the network configuration the protocol, ports and description are available. The advantage of this view point is that ABC manufacturing can view the current protocol on the given ports and pentesting these port to see if the firewall is configured properly on the network.



An anti-virus scan was done to check the vulnerability of the system. Upon discovery the anti-virus definitions were not up to date. The risk of this being outdated is that new viruses and malware are introduced at a high rate. If a firewall can to define what is a virus or malware, it cannot filter out the malicious traffic and this puts ABC’s network at risk. 



The vulnerability to the operating system if the firewall is not configured properly can be a lose of production. With configuration set to allow all this causes more of a risk. This violated the least privilege rule. Allowing for a fluid transports of packages. The firewall needs to be configured to allow only requests out from the network and limit the incoming request. This vulnerability can allow attackers to brute force into the network and escalate privileges and gain control of the network. Making sure proper configuration is done on the firewall will help ensure a secure network.

**Network Security Posture Recommendations:**

ABC Manufacturing was not fully aware of the need security measures needed to setup a properly secure network. While doing a nmap and zenmap it was discovered that multiple unneeded ports were open. From my meeting with ABC Manufacturing it was expressed that only certain port be open and this is not the case. This leaves an opening to be exploited. See image 1 to see open ports.

Viewing the OpenVAS, there are several vulnerabilities that needs to be addressed. One issue is use of weak passwords. Another issue is that the Java RMI server insecure default configuration remote code execution vulnerability. Please refer to image 2 below.

On the external attack machine there are unnecessary open ports. Again, using nmap and zenmap, it shows these open ports. Unused ports can give an opening for attackers to exploit. Even more if these ports are improperly configured it will allow for intrusion to happen and go unchallenged.

**Network Security Posture Recommendation: Impact**

Open ports can be dangerous when the service listening on the port is misconfigured, unpatched, vulnerable to exploits, or has poor network security rules (Tunggal, 2021). These open ports are seen as the doorway into ABC Manufacturing infrastructure and goes against industry best practice.

When it comes to the use of weak passwords, it can lead to an attacker using a brute force attack and decoding the user’s password and gaining access to the client machine. This also allows for attackers to bypass the firewall and get direct access to the network. A weak password used on a firewall or system admin device can lead to a breach of data and more importantly the loss of control over the network due to a ransomware. (Chauhan and Panda, 2015).

The Java RMI Server insecure default configuration remote code execution vulnerability can allow unauthenticated, remote attacker to exploit the system by transmitting malicious packets into the software. Once these packets are translated it could give the attacker elevated privileges (2016)

**Network Security Posture Recommendation: Likelihood**

With the open ports and the weak passwords, the likelihood of ABC Manufacturing being a victim is likely. On average the global cost of data breaches is 3.86 million This come from a weak password. From data breaches 15 million occurs across 17 different industries (Whitney, 2021) As seen in image 3, password is the most commonly used password. As mentioned earlier a weak password can cost a lot of money, bad reputation and loss of confidence in the company. With the open ports such as Telnet which leads to unencrypted remote access, this could easily be picked up by an eavesdropping device and piggyback into the network through a remote computer. This makes it a high possibility that if targeted that ABC Manufacturing will be in a very unfavorable security position.

**Network Security Posture Recommendation: Mitigation Strategies**

To mitigate the above issues, ABC Manufacturing should do the following. One they need to make sure that all passwords are more complexed. Meaning not to use guessable passwords or phrases. Next, they should implement a multi factor authentication. This will make it harder for attackers to brute force attack the system. A password manager that monitors and suggest a more secure password, would help users to create a better password. Lastly, they should educate their team on password protocol and the importance of a strong password and how not to leave those credentials written down in visible sight. To mitigate Java RMI server insecure default configuration remote code execution vulnerability, it is suggested to follow secure coding guidelines for Java. Always run a security manager when using RMI and establish a reasonable security policy. Use it for local communication only with specific socket permissions in the security policy. Lastly, run RMI over SSL/TLS ad require authentication for both server and client (RMI Security Recommendations, 2021).

**Network Security Posture Recommendation: Prioritization**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Description of Vulnerability** | **impact** | **Likelihood** | **Priority** | **Recommendation** |
| **Unused Unnecessary open ports** | **3** | **3** | **4** | **Close all unused ports. Keep HTTP, HTTPS and SMTP ports open.** |
| **Weak Passwords** | **2** | **4** | **3** | **Incorporate a password manager, train staff to create stronger passwords.** |
| **Unsecure protocol Telnet** | **3** | **3** | **2** | **Switch to SSH to replace telnet. It’s a more secure connection and is more up to date with the newest protocols.** |

**Network Security Posture Recommendation: Rationale**

A priority rating of 4 for open ports was given because with open ports this leaves an open door into the network.Open ports can affect the CIA. Confidence in the fact that a listening device can reveal network information. Integrity because open ports can talk without proper port control. Lastly, availability because open ports still process incoming traffic which can result in denial of service attack (Tunggal, 2021)

A level 3 was given for weak passwords because even though it is important to have a stronger password, a simple email stating that all passwords will be required to be more complex and that staff will change within a given time frame will provide a smaller window for attackers to brute force the old passwords. The change of passwords could also be the way to teach the importance of having a multi factor authentication put in place. Also, all password protocol should implement a time tables on how often a user should change their password. This will ensure that even if an attacker happens to brute force a password that they have a small window of opportunity to use it or that it will stay active.

Level 2 was given because telnet is an unsecure remote host through command line interface. This unsecure communication is in plain text and can be seen in real time. By switching to SSH it will provide a cryptic file transmission over an unsecure network. If remote client access is not greatly used this priority is low and the company has time to upgrade to this cryptographic network protocol.

**Network Security Posture Recommendation: Execute**

Upon hiring ABC Manufacturing demanded that certain ports were open. After doing a nmap and a zenmap, shown in figure 1 and 2. By going through the pfsense firewall it also shown that multiple ports were open. See figure 4 and 5. To mitigate these issues and to provide the service ask for by ABC Manufacturing. Within the pfsense firewall outbound and forwarding port within the NAT tab, unwanted ports were deleted and SSH port for 443 HTTPS, HTTP and SMTP was left open and a secure protocol was put in place. See image 5

**Network Security Posture Recommendation: Hardening the Server**

To harden the server, I took away the ability of unneeded protocol by unselecting them. Protocols that were unsecure and transmitted plain text packets were disabled. Within the firewall setting telnet, SNMP trap routing and remote access where disabled and only the needed ports were left open. See image 6 below.

Backup Images

Image 1

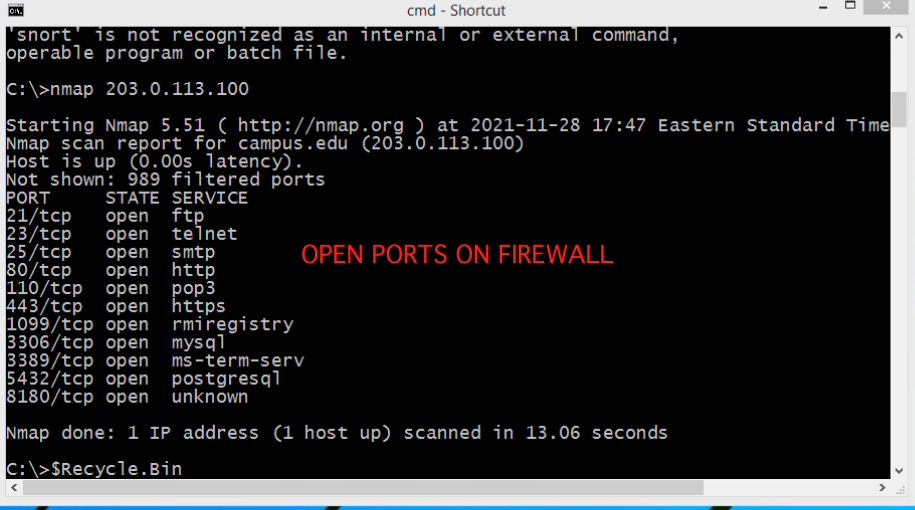


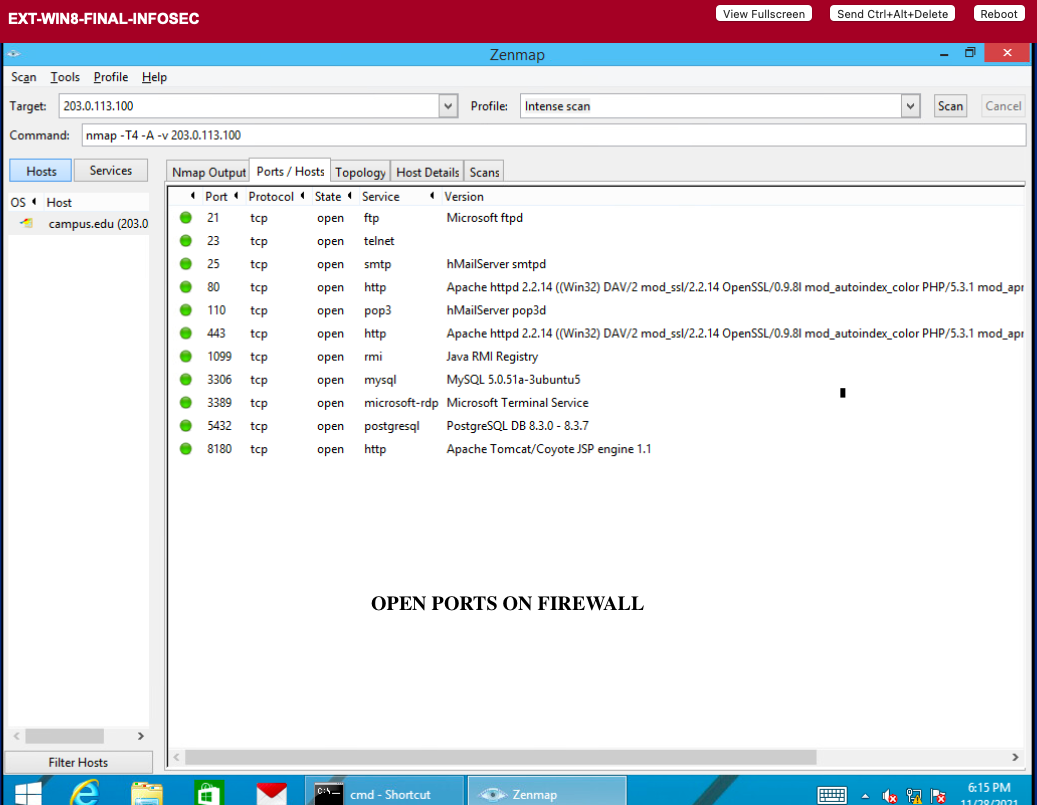
Image 2 

Image 3

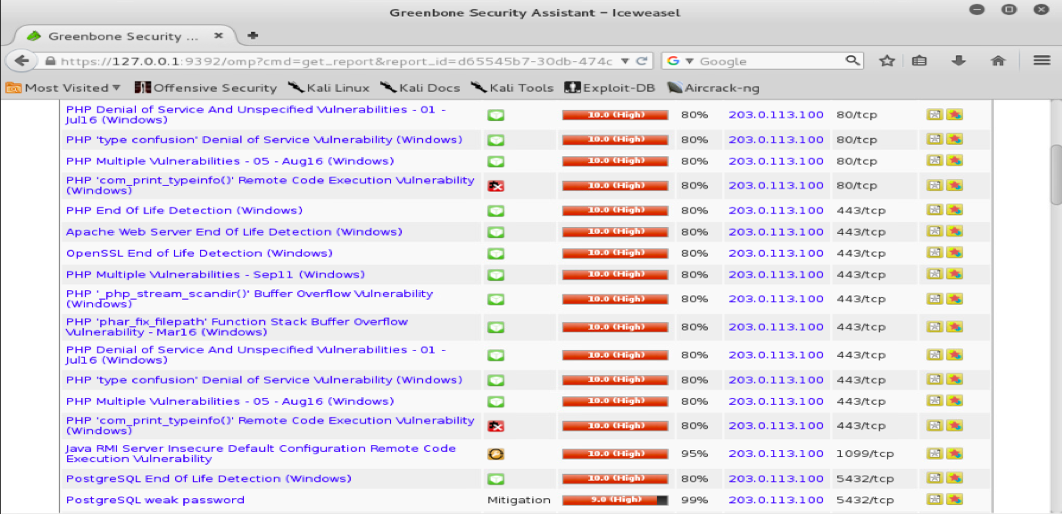


Image 4

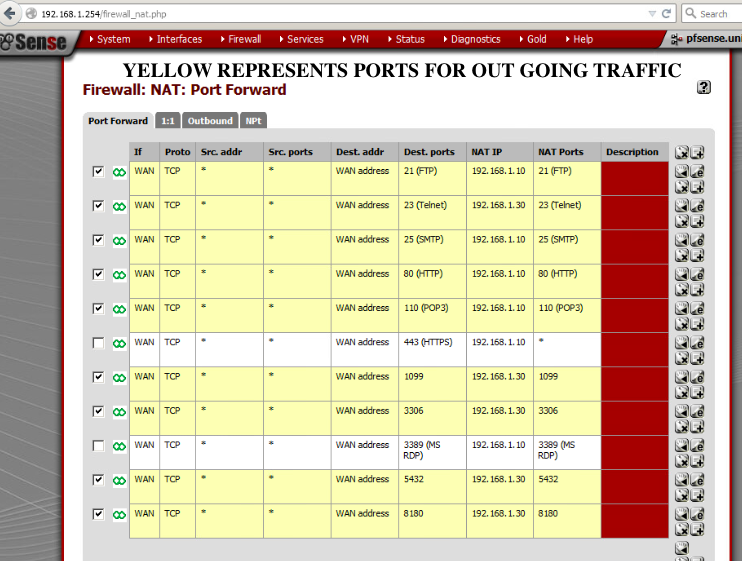
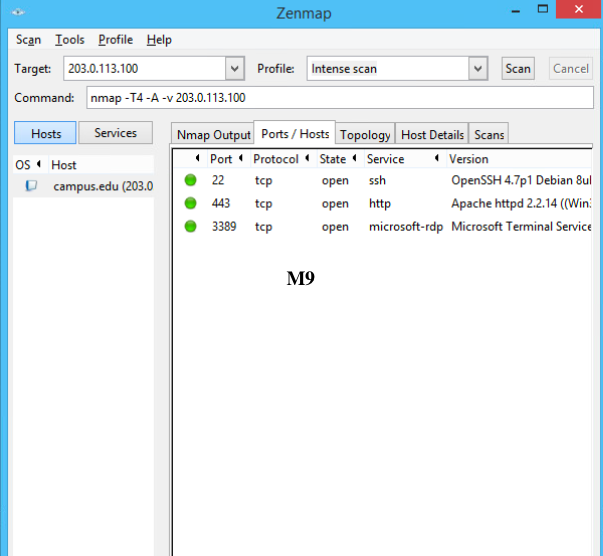


Image 5



References

2016. [online] Available at: <http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.140051> [Accessed 29 November 2021].

Chauhan, S. and Panda, N., 2015. *Hacking Web Intelligence*. [online] Available at: <https://www.sciencedirect.com/topics/computer-science/weak-password> [Accessed 29 November 2021].

Docs.oracle.com. 2021. *RMI Security Recommendations*. [online] Available at: <https://docs.oracle.com/javase/8/docs/technotes/guides/rmi/rmi\_security\_recommendations.html> [Accessed 29 November 2021].

Tunggal, T., 2021. *What is an Open Port? | Definition & Free Checking Tools for 2021 | UpGuard*. [online] Upguard.com. Available at: <https://www.upguard.com/blog/open-port> [Accessed 29 November 2021].

Whitney, L., 2021. [online] TechRepublic. Available at: <https://www.techrepublic.com/article/how-weak-passwords-could-put-your-organization-at-risk/> [Accessed 29 November 2021].

dummies. 2021. *Ports, Protocols, and IP Address Ranges for Firewalls - dummies*. [online] Available at: <https://www.dummies.com/computers/computer-networking/internet-access/ports-protocols-and-ip-address-ranges-for-firewalls/> [Accessed 15 November 2021].

Vanzara, A., 2021. *How Outdated Software Can Put Your Business at Risk*. [online] OpenGrowth. Available at: <https://www.opengrowth.com/article/how-outdated-software-can-put-your-business-at-risk> [Accessed 15 November 2021].

Wiki.sni.pitt.edu. 2019. [online] Available at:

<http://wiki.sni.pitt.edu/images/1/16/Firewall\_Standard.doc> [Accessed 15 November 2021].