Final Project: Milestone One

Nouman Ali

IT-320 Network Security

SNHU

**Network Assessment - Gathering Evidence of the Vulnerabilities**

The following is a vulnerability study. The main goal of this analysis is to find and describe vulnerabilities in network equipment security. I have installed the Endian Linux firewall that supports Windows firewall, such that the system is protected. With Nmap on the Kali 2 Linux command I was able to detect the ports open on the firewall. The image below displays all service ports available. For the virtual machine (host), this is a huge challenge because other open port details should be given to anybody who can access it in plain text.A screenshot of a cell phone

Description generated with high confidence

The ports in the firewall were also a threat to the virtual machine (host). The unused opened ports will also require unsafe access to the network and the virtual system. Postgresql.exploit" was one of the most insecure on the Windows Server. This is effective if a session was not enabled on the Windows server with proper antivirus or malware security, as was the case. This technique may be used to build a session if the correct malware or antivirus security has not been enabled on the Windows machine.

Upon installation in the Microsoft Security Basics list, a scan was run to find any unauthorized files that might exist on the system network. The following image demonstrates that recently updated antivirus programs have detected a vital infection from the task I used before.

![A screenshot of a cell phone

Description generated with very high confidence]()

As I already mentioned, there has been no security software in place at all, which is a major security threat, as exploits can be used to gain access to the server and the system. By accessing the network a hacker can gain access to other systems that are also available on the network. By just not having malicious software to protect you, you are opening up a device to get exposed to the virus. One is to make sure safeguards by installing patches on the system automatically. This guarantees that exploitable vulnerabilities are closed and are not being exploited, as I did with Postgresql. Which is why keeping the network as it had been really was a major no in the defense of the network. When an intrusion occurred, it may go unchecked for a long period without the appropriate security measures in place.

To help analyze the network, I have used Wireshark to restructure a Telnet conversation. When I have filtered data with various keywords, tcp and ftp, I find a packet using telnet. I clicked the 1st packet right, used the TCP stream option and the result was shocking, the username and password are shown in front of me. For Wireshark output, see picture below.![A screenshot of a computer

Description generated with very high confidence]()

Under the lab11 tag I saved the results with Wireshark. I've opened the application of NetworkMiner. The NetworkMiner lab11.pcap file I dragged and lowered. I've got a range of viewing options. I clicked directly on the credentials tab and was in the top of the page a big surprise. The first entries using FTP were seen on the system page, as were the username and password credentials. The user name was masked and the password displayed as N / A, against the HTTP Protocol. See the image below for NetworkMiner results.A screenshot of a cell phone

Description generated with high confidence

**Vulnerability Assessment – Interpreting Evidence of Vulnerabilities**

When I checked the results of the network analysis, I found that the "ABC Manufacturing" operations did not need open ports. In the Wireshark and NetworkMiner applications, I was able to obtain username and password credentials from different protocols. When I accessed the Windows Server all unused ports and resources not used or needed have been shut down or disabled. The danger to the network is to open these unwanted ports. The following services were disabled by FTP Publishing Program, TCP / IP Basic Services and Telnet. In the Windows firewall settings tab exceptions, the following changes (deletion) have been made, "Chargen", "Daytime", "Echo", "FTP Server", "QOTD" and "Telnet". The following image illustrates all available ports on the server when unwanted and unused ports have been closed.

![A screenshot of a social media post

Description generated with very high confidence]()

There was no installed antivirus or malware on the server that’s why it was possible to exploit the Postgresql vulnerability to create files in the window server 2008, as seen in the network evaluation. This attack went undetectable because there was no antivirus was installed. If there was any antivirus was installed It would not lead to a long time non-detected breach. After installing "Microsoft Security Essentials" successfully on the server, I could search the server system and found a critical safety danger. The alert was quarantined, and in the background tab I could see the specifics of the incident. See the following two images for the results of scans and Microsoft Security Basics history tab section for the quarantined file.A screenshot of a cell phone

Description generated with very high confidence

![A screenshot of a cell phone

Description generated with very high confidence]()

With the OpenVAS method, I could search the server and other computers for vulnerabilities. Surprising to say the least were the findings of the scan. In total, there were 358 vulnerabilities. The PostgreSQL was one of the bugs I was explicitly searching for. The vulnerability which i find it claimed that you can login as the PostgreSquare with the password "postgres" in the vulnerability specification. It was suggested that the password be changed as soon as possible to prevent exploiting the vulnerability. I used Kali 2 Linux vulnerability to use it and the exploit showed database, "password", "lhost", "rport, username and Verbose information. See image below for vulnerability, open results, and weak password interpretation of postgresSQL results exploit.![A screenshot of a computer screen

Description generated with very high confidence]()

![A screenshot of a computer

Description generated with very high confidence]()

A screenshot of a cell phone

Description generated with very high confidence

As previously stated, I disabled some of the Windows firewall settings, because they were identified as being open from the Nmap server scan. Since the server was in risk, the firewall had to protect those vulnerabilities. In plain text, I was able to access and view information through Wireshark and NetworkMiner applications from ports such as "Telnet", "QOTD", "FTP Server", "ECHO", "DAYTIME" and "CHARGEN". Accessed from Wireshark is site specific files such as QOTD (Quote of the day). This is the open stream image of QOTD TCP.A screenshot of a cell phone

Description generated with very high confidence

After saving the Wireshark files, I opened the results in NetworkMiner. Tabs such as "hosting", "files", "notes", "photos", "passwords", "etc., have been available. As I mentioned before, unnecessary ports were opened to open the firewall. NetworkMiner shows username and password credentials with the result of a certain tab, FTP. One of the qualifications was the administrative account. It is one of the network's security risks facing unnecessary open ports. Network traffic for Wireshark can be collected and accessed for these ports. It allows information such as passwords, texts, data and more to be processed.

**References**

“INFOSEC LEARNING LLC. (n.d.). Configuring a Linux Based Firewall to Allow Incoming and Outgoing Traffic. Retrieved July 22, 2018, from”

<https://lab.infoseclearning.com/lab/configuring-linux-based-firewall-allow-incoming-and-outgoing-traffic>

INFOSEC LEARNING LLC. (n.d.). Patching, Securing Systems, and Configuring Anti-Virus.

“Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/patching-securing-systems-and-configuring-anti-virus>”

“INFOSEC LEARNING LLC. (n.d.). Vulnerability Scanners and Penetration Testing.

Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/vulnerability-scanners-and-penetration-testing>”

“INFOSEC LEARNING LLC. (n.d.). Deep Dive in Packet Analysis - Using Wireshark and

Network Miner. Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/deep-dive-packet-analysis-using-wireshark-and-network-miner>”

“Stewart, J. M. (2014). *Network security firewalls and VPNs* (2nd ed.). Burlington, MA:

Jones & Bartlett Learning.”

**Image References**

“INFOSEC LEARNING LLC. (n.d.). Configuring a Linux Based Firewall to Allow Incoming and Outgoing Traffic. Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/configuring-linux-based-firewall-allow-incoming-and-outgoing-traffic>”

“INFOSEC LEARNING LLC. (n.d.). Patching, Securing Systems, and Configuring Anti-Virus.

Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/patching-securing-systems-and-configuring-anti-virus>”

“INFOSEC LEARNING LLC. (n.d.). Vulnerability Scanners and Penetration Testing.

Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/vulnerability-scanners-and-penetration-testing>”

“INFOSEC LEARNING LLC. (n.d.). Deep Dive in Packet Analysis - Using Wireshark and

Network Miner. Retrieved July 22, 2018, from <https://lab.infoseclearning.com/lab/deep-dive-packet-analysis-using-wireshark-and-network-miner>”