**Alexis Tostado**

**C844 - Task 1**

1. **Network Topology**

* Screenshots of running nmap.

A screenshot of a computer program

Description automatically generated

* Screenshot of Zenmap Topology
* 10.168.27.20 – Host OS: Linux: 2.6.32 – Open Ports: 1
* 10.168.27.132 – Host OS: Linux 2.6.32 – Open Ports: 1

A screenshot of a computer

Description automatically generated



* 10.168.27.15 – Host OS: Microsoft Windows 7 - Open Ports: 10

A screenshot of a computer program

Description automatically generated



* 10.168.27.14 – Host OS: Linux 2.6.32 – Open Ports: 1

A screenshot of a computer program

Description automatically generated



* 10.168.27.10 – Host OS: Windows Server 2012 R2 – Open Ports: 8

A screenshot of a computer

Description automatically generated



* This network is set up as a Star topology.

A screenshot of a computer

Description automatically generated

**B. Summary of Vulnerabilities and Implications**

**First vulnerability**

A screenshot of a computer

Description automatically generated



* TCP 80 or HTTP is a network protocol that runs in the cleartext meaning it has no encryption. Therefore, leaving this port open you are essentially leaving a backdoor open for an attacker to leverage this vulnerability to bypass any authentication systems.

**Second vulnerability**

**A screenshot of a computer

Description automatically generated**



* TCP 21 or FTP is a File Transfer Protocol which is used to transmit files, credentials, and other information in cleartext. This makes it easier for attackers to retrieve this data and possibly use it to gain further access into the systems.

**Third vulnerability**

A screenshot of a computer

Description automatically generated

* Windows 7 is an older operating system which has reached its end of life. Therefore, no longer receiving important security patches and being open to cyber criminals to exploit this weak operating system.

**C. Wireshark Anomalies**– using Pcap 1

* **First Anomaly –** 16441 to 16448 – SMB is a network sharing protocol.

A screenshot of a computer screen

Description automatically generated

* **Second Anomaly –** Frame 14985 to 14998 – LDAP protocol transmit data without encryption.

A screen shot of a computer

Description automatically generated

* **Third Anomaly –** Frame 610 to 796 – DNS runs on port 53 it is the Domain Name System.

A screenshot of a computer

Description automatically generated

**D. Implications of each Wireshark Anomaly**

**Implications of taking no action 1 -** Using SMB for file transfer is very dangerous as it is not as secure as other options and can allow attackers to potentially hijack data in motion. An attacker can use a SQL Injection to access sensitive information or even execute further code in the system.

**Implications of taking no action 2 -** IfLightweight directory access protocol (LDAP), port 389, is accessed by an attacker it can be used to perform a denial-of-service attack that can easily be triggered by a single message sent over the TCP. LDAP also has a remote code execution vulnerability.

**Implications of taking no action 3 –** Remote attackers can craft DNS packets and flood them through port 53 which is essentially a denial-of-service attack. DNS is also susceptible to DNS Spoofing which uses altered DNS records to redirect traffic to a fraudulent site and potentially steal the victims’ credentials.

**E. Recommended Solutions**

**First Vulnerability –** Port 80 is the HTTP protocol, and it is unsecure, fortunately there is an alternative option that offers encryption. First, using the firewall to add a port rule that will block all traffic through port 80. Furthermore, switching to using only port 443 HTTPS will offer an encrypted connection to websites making it much safer. (GeeksforGeeks)

**Second Vulnerability –** FTP is an unsecure protocol used to transfer files between networks. Switching to SFTP which uses port 22 will be a much more secure option as SFTP uses different encryption methods to ensure the data in motion is secure. Furthermore, using the firewall to block all traffic from port 21 FTP will also need to be done as leaving unused ports open is still very dangerous and vulnerable to attacks. (Team)

**Third Vulnerability**– Windows 7 is very outdated, and we are now at windows 11. Windows 7 has reached its end of life, which means it no longer receives any security patches. Therefore, this OS is very susceptible now to many forms of attacks as any new exploits found are not being patched. To fix this upgrading/updating all workstations to the current OS will make the workstations a safer environment receiving security patches. (*Get Ready for the Windows 11 Upgrade*)

**First Anomaly –** SMB is a client-server communication protocol used for accessing files, printers, and other resources on the intranet. SMB set up properly can be secure if you are using the latest version. Therefore, setting the SMB protocol to use both SMBv2 and SMBv3 promotes the most secure version. Furthermore, you can block outside internet access by using a firewall to block ports 139 and 445. (PatAltimore)

**Second Anomaly –** LDAP is a protocol used for pulling data from directories related to organizations, people, and more. LDAP does not use encryption, therefore switching over to LDAPS would be the best action. LDAPS uses TLS/SSL for its encryption which ensures that the data in motion is secure and proper authorization for access of the data. Finally, blocking port (389) with a firewall will help to ensure that LDAP is not open to users. (Rublon)

**Third Anomaly –** Although DNS is not an issue alone, if not protected properly against DNS spoofing or other attacks, it can become a vulnerability to users or even systems. Some of the things you can do to prevent these attacks is to securely manage your DNS servers, keep DNS resolver private and protected, and configure DNS against cache poisoning. Followed by consistent audits to ensure nothing has been tampered with in the configuration and that no attackers are performing fraudulent DNS attacks. (Dizdar)

**References**

Dizdar, Admir. “5 DNS Attack Types and How to Prevent Them.” *Bright Security*, 20 June 2023, brightsec.com/blog/dns-attack/.

Authors, Rublon. “LDAP vs. LDAPS: What’s the Difference? - Rublon.” *Rublon.com*, rublon.com/blog/ldap-ldaps-difference/#:~:text=LDAPS%20stands%20for%20LDAP%20over. Accessed 19 Aug. 2023.

‌ “CVE - Search Results.” *Cve.mitre.org*, cve.mitre.org/cgi-bin/cvekey.cgi?keyword=port+53. Accessed 19 Aug. 2023.

“Difference between Http:// and Https:// - GeeksforGeeks.” *GeeksforGeeks*, 27 Sept. 2015, www.geeksforgeeks.org/difference-between-http-and-https/.

‌ Team, Cerberus. “Secure FTP - How to Secure Your Server. 8 Essential Tips.” *Cerberus FTP Server*, 9 Oct. 2018, www.cerberusftp.com/blog/eight-essential-tips-for-securing-an-ftp-or-sftp-server/.

‌GeeksforGeeks. “How to Secure HTTP Requests.” *GeeksforGeeks*, Mar. 2022, www.geeksforgeeks.org/how-to-secure-http-requests.

PatAltimore. “Secure SMB Traffic in Windows Server.” *Microsoft Learn*, 12 June 2023, learn.microsoft.com/en-us/windows-server/storage/file-server/smb-secure-traffic.

*Get Ready for the Windows 11 Upgrade*. support.microsoft.com/en-us/windows/getting-ready-for-the-windows-11-upgrade-eb50813f-c7da-4cf8-89a3-6ba0d33b2773#:~:text=To%20check%20if%20Windows%2011,proceed%2C%20download%20and%20install%20it.

‌