**C844 Task 1: Mapping and Monitoring**

1. **Nmap Summary**

After using Zenmap the topology of the network was a star topology (see Figure 1). It showed five hosts connected to a switch; one computer had no identifiable OS, 2 computers were running Windows OS, and 3 computers were running Linux. Star topology has a central point for all the connections which can be beneficial in many ways. It is easier to add new computers to the network without causing interruptions and you can centrally manage devices. The topology also allows for nodes of the network to malfunction without affecting the rest of the network. A downside of a start topology is that there is a single point of failure. If the switch were to malfunction it could affect the rest of the network. The network performance will be determined by the capacity of the switch. If too many devices are present a bottleneck could occur and result in delays or packet losses.

A screenshot of a computer

Description automatically generated

(Figure 1)

1. **Summary of Vulnerabilities and Implications**

The first vulnerability I noticed was with host 192.168.27.15. Port 21 is open on this host and is used for FTP traffic (see Figure 2). This creates a vulnerability because FTP uses cleartext. This means that anyone listening to the port can see what is being sent because there is no encryption. This host would be vulnerable to MINTM and malware attacks. Credentials could also be found during packet sniffing operations which could lead to unauthorized access of the network.

On the same host port 25 is also open (see Figure 2). Port 25 uses SMTP for email communication and this port sends packets with cleartext as well. This means that MINTM and phishing attacks could occur over this port. It is not unusual for the port to be used by red hats looking to acquire user credentials, deploy malware, or steal information. Port 25 is also used in DoS attacks. Since the port is open and used frequently it would be easy to flood the server with messages to where the server would stop responding or crash.

A screenshot of a computer

Description automatically generated

( Figure 2)

Hosts 192.168.27.15 and 192.168.27.10 present different vulnerabilities. The hosts are running Windows 2008 and 2012 respectively. This is an issue because these versions of Windows no longer receive patches or security updates. Any zero-day vulnerabilities found would be left unfixed making the network permanently vulnerable. Also, because no updates are available for the hosts at going forward, they could be effected by worms or other computer viruses or even ransomware.

1. **Wireshark Anomalies**

In Wireshark, I filtered for TCP protocol traffic. I found multiple stealth scans coming from an IP address listing of 172.16.80.24. Red hats were targeting systems by looking at multiple ports to see which were open and if they could be exploited (see Figure 3).

A screenshot of a computer

Description automatically generated

Figure 3

When filtering for FTP more anomalies were seen. A red hat was able to gain access to a file and give it a password. This could hinder users of that file from accessing it and allow the red hat to insert ransomware (see Figure 4).

A screenshot of a computer

Description automatically generated

Figure 4

When filtering for HTTP communications could be seen. A user at 10.16.80.243 tried to exploit the unencrypted system (see Figure 5).

A screenshot of a computer

Description automatically generated

Figure 5

1. **Implications of Each Wireshark Anomalies**

The stealth scans that occurred were trying to map the network. This would allow a red hat to gather information about your network that could lead to a more serious attack. The stealth scans provide the attacker with the knowledge they need to best infiltrate the network.

FTP is unsecure because it will allow anonymous logins. By letting someone log in without credentials anyone could access the network. In this case, the red hat attached a password to a file. This is the basics of ransomware and could cause major financial loss to the owner of the network. FTP also sends information in cleartext which allows proprietary information to be seen.

HTTP is not a secure transmission option. In relation to current security measures, the security of HTTP is outdated and could allow red hats an opening to the network. This would mean that the network is more prone to exploits.

1. **Recommended Solutions**

To secure port 21, you could require a password for all file transfers. This would create a more secure file transfer so not just anyone would be able to send files. You could also limit the number of IP addresses allowed to the network so you have a better idea of how many and what devices are present. (Is Port 21 Secure? Fully Explained. Exavault)

Instead of using port 25, port 587 should be used as it is a more secure version. Port 587 uses TLS encryption to so only desired parties can access the information. There is also checks to ensure data has not been altered. (What SMTP port should be used? Port 25 or 587? Cloudfare)

Your operating system should always stay up to date. Keeping it current will allow you to receive any patches or firmware updates that may be necessary to keep your device and network safe from attacks. Keeping your computer up to date can help mitigate things like viruses or worms. (Update Your Operating System and Software. Brown University)

To mitigate port scans and network mapping you should frequently scan your own network. You can then see firsthand what ports are open and what vulnerabilities they may cause. You can then close or configure the ports to fit the security needs of the network. (nmap.org, n.d,)

NDLP solutions can be used to mitigate FTP issues. This would allow for the configuration to allow or block certain transfers based on business policies and actions. NDLP would allow you to inspect and control FTP traffic and offer encryption. (Lord, 2018, digitalguardian.com)

HTTP is not secure for communication and HTTPS should be used instead at port 443. HTTPS offers encryption that can stop XXS, SQL injection, or CSRF attacks. HTTP leaves the network vulnerable to attackers and red hats. HTTPS offers encyrtion through SSL or TLS to make transmissions safer. (HTTP and HTTPS. Harvard University)

1. Sources

(n.d.). Is Port 21 Secure? Fully Explained. Exavault. Retrieved January 28, 2024, from <https://www.exavault.com/blog/port-21-secure-fully-explained>

(n.d.). What SMTP port should be used? Port 25 or 587? Cloudfare. Retrieved January 28, 2024, from <https://www.cloudflare.com/learning/email-security/smtp-port-25-587/>

(n.d.). Update Your Operating System and Software. Brown University. Retrieved January 28, 2024, from <https://ithelp.brown.edu/kb/articles/update-your-operating-system-and-software>

*Vulnerability scanners – SecTools Top Network Security Tools*. (2005). Nmap.Org. <https://sectools.org/tag/vuln-scanners>

*What is FTP Security? Securing FTP Usage.* (2018, September 7). Digital Guardian. <https://digitalguardian.com/blog/what-ftp-security-securing-ftp-usag>

(n.d.). HTTP and HTTPS. Harvard University. Retrieved January 28, 2024, from https://web.stanford.edu/~ouster/cgi-bin/cs142-fall10/lecture.php?topic=http