Network Security Assessment – Work from Home

Author: Arturo E. Correa Meléndez
Advisor: PhD. Jeffrey Duffany
Computer Science Department, Polytechnic University of Puerto Rico

Abstract

In the past two years, we have seen an increase in employees working from home. This is mainly due to the Covid-19 pandemic. Because of this, a study was conducted on a home network that was being used to work from home. The procedure for the study was an offensive approach to try to crack the password of the Wi-Fi router using Aircrack-ng, network mapping to check what devices were connected to the network using Nmap, and two vulnerabilities scan assessment using Metasploit and Greenbone vulnerability Manager (GVM). As a result of the assessment there was one vulnerability that surpassed the critical level established. However, since the vulnerability could not be exploited, there was not enough evidence to conclude that the network can be considered as unsafe for working from home purposes.

Introduction

There has been an increase on employees working from home due to the Covid-19 pandemic. This has raised security concerns regarding the home networks of the employees working remotely. In this study, a network security assessment was conducted on a home network that was configured with the default settings that the internet service provides. The assessment consisted of password cracking utilizing Aircrack-ng, network mapping utilizing Nmap with Vulners and Vulscan for vulnerabilities, and two vulnerabilities scanners Metasploit and GVM.

Problem

Due to an increase of employees working from home since the Covid-19 lockdown started, there has been a concern regrading network security. There is a level of uncertainty in the case that the company does not have a VPN or a procedure to certify that the home network of the employee is considered secured to be used for work. The purpose of this study is to examine and determine a way that an employee can conduct a network security assessment utilizing Open-Source tools.

Methodology

Aircrack-ng was used for the process of cracking the routers password. The procedure was to monitor the network using airodump to capture a handshake when a device tried to connect to the network using the following command:

sudo airodump-ng -c <channel> --bssid <access point MAC address> -w <output file> <network card name>.

After the package was captured, it was saved on a .cap file to then be compared to the words in the wordlist dictionary. What Aircrack essentially does is that it duplicates the handshake and compares it with every word in the world list. If it matches, then the key has been successfully found. Aireplay-ng was used to deauthenticate a device using the following command: ***sudo aireplay-ng -0 -a <access point MAC address> <network card name>.***

After capturing the handshake, Aircrack-ng was used to try to crack the password using the rockyou.txt wordlist provided on the Kali Linux distro.

Nmap was used for network mapping. The findings were compared with the devices that were available through the router settings manager. The goal was to find what devices were running in the network and what kind of services they were running. The following command was used to check the devices and services running in the network: ***sudo nmap -sP 192.168.0.0/24 –O***.

This command prompted the devices connected to the network and what OS were they likely using. To check the services running in the open ports the command was:

sudo nmap -sS 192.168.0.0/24.

After checking the devices and services connected to the network, the next step was to check the network for vulnerabilities using the Vulners and Vulscan scripts using the command:

sudo nmap --script vulscan, nmap-vulners -sV <Target's IP address> <output file name>

For scanning further for vulnerabilities, the tools Metasploit and GVM were used. The results of each tool were then compared to check if they had found critical vulnerabilities that were higher than the 7.0 level of security category. The vulnerabilities checked on Metasploit were based on the information gathered using Nmap (OS versions and services running). For GVM the automatic search for vulnerabilities on the network was used.

Results and Discussion

The password cracking process was unsuccessful since the pre-shared key of the router was not part of the world list utilized on the study and the key followed a strict password guideline. The process of mapping the network was quite successful. It was compared with the devices that were listed on the router set-up tool and there were only three missing devices focused on **Figure 1**.

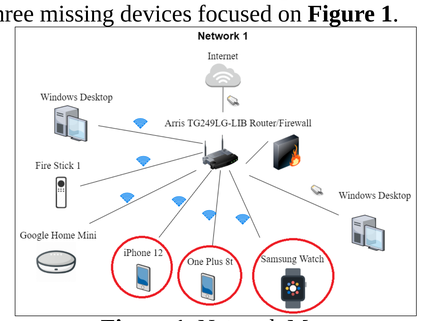

Figure 1. Network Map

Results and Discussion

The results gathered using Metasploit were not considered of high risk. The vulnerability was a way to disrupt the Fire Stick device flooding it with YouTube videos play requests. The other vulnerability was considered a higher risk, but it could not have been exploited because the services was SMB 3.0, and the working exploits were for 2.0 version and below. The GVM results are presented in **Figure 2**, in which only one vulnerability surpassed the 7 level of severity threshold.

Name	Severity ▼
Lighttpd Multiple vulnerabilities	9.8 (High)
SSL/TLS: Report 'Anonymous' Cipher Suites	5.4 (Medium)
SSL/TLS: Known Untrusted / Dangerous Certificate Authority (CA) Detection	5.0 (Medium)
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3 (Medium)
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)
TCP timestamps	2.6 (Low)

Figure 2. GVM Results

For the vulnerability above 7.0 threshold, the Vulners script was used to try to exploit it, but it was not successful. There were other sources online that were used but none of them managed to exploit the vulnerability. Nonetheless, the vulnerability was fixed using the vendor fix provided on the GVM report.

Conclusions

In the study there was only one critical vulnerability, even though the systems and services were not updated by the users of the network regularly. Home networks can be considered weaker than industry networks, but safe enough for work from home employees. The key element here is to have all devices and services up to date to minimize the vulnerabilities. If the owner of the network maintains the network and services regularly it can be considered a safe network to use for work from home.

Future Work

Since this network did not have a webserver running, there was no need to use a software tool suite to try to find vulnerabilities on a webserver. For future work a website security assessment can be conducted to check for vulnerabilities and to educate on how someone can test their website for security. Another subject that could be studied is the social engineering aspect of network security. There are a few techniques such as phishing and spoofing that can be used to prove if the infrastructure of the network has measurements to mitigate and protect the information.

Acknowledgements

I would like to acknowledge Dr. Jeffrey Duffany, professor at the Computer Science & Engineering department for guiding me and providing feedback throughout this work. I would also like to acknowledge Isabel Batteria for reviewing the article for the project.

References

[1] K. PARKER, J. MENASCE HOROWITZ AND R. MINKIN (2020, DECEMBER 9). How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work. From PEW Research Center. https://www.pewresearch.org/socialtrends/2020/12/09/how-the-coronavirusoutbreak-has-and-hasnt-changed-the-wayamericans-work/
[2] https://github.com/vulnersCom/nmapvulners.git
[3] https://github.com/scipag/vulscan.git