Network Security Assessment – Work from Home

Arturo E. Correa Meléndez
Master in Computer Science
Dr. 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 were 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. As a result of the assessment there was only one vulnerability that surpassed the critical level established. However, since the vulnerability could not be exploited, there is not enough evidence to conclude that the network can be considered as unsafe for working from home purposes.*

Key Terms *- Kali Linux, Network Scanner, Aircrack-ng, Nmap, Metasploit, Greenbone Vulnerability Manager*

INTRODUCTION

In the past two years, we have seen an increase in employees working from home. This is mainly due to the Covid-19 pandemic. PEW Research Center conducted a survey in which 71% employees were currently working from home and among those 54% would want to work from home after the coronavirus outbreak ends [1]. A concern that has been raised from working from home is the network security of the employees' networks. If the company is small or close to midsize, it is more likely that they will not have a VPN to provide to their employees. The purpose of this study is to conduct a security assessment on a home network in which there are people who are working from home. We are looking for vulnerabilities in that network that are configured with the default setting used by the internet providers. Aside from default setting, the network do not go through the process of updating firmware. In this case if the ISP does not set an auto-update mechanism for the firmware, the firmware is going to be outdated.

The assessment will consist of three steps. The first step will be an offensive attack using the Aircrack-ng suite to try to crack the network password. The second step will be a passive scan, where we are going to find information about the devices that are connected in the network using Nmap with Vulners and Vulscan scripts for vulnerability scan. The last step will be an active search for vulnerabilities that are exploitable in the network using Metasploit and Greenbone Vulnerability (previously known as OpenVas). The tools are going to be briefly discussed and explained. The results will be analyzed to determine if the network has severe vulnerabilities and how it could impact the workflow of a person that is working from home in that network.

In this study we should not expect to have a vulnerability on every device since most of the devices on the network are going to be running Windows OS and Windows is known for having forced updates when you shut down or restart your device. Furthermore, the purpose of this paper is also to show mechanisms and tools that anyone can use to check if there are vulnerabilities in the network that need to be fixed.

SOFTWARE TOOLS AND USAGE

The Operating System that is going to be used in this study is Kali Linux. The software tools that are going to be used in the study are pre-installed on Kali Linux except for Greenbone Vulnerability Manager. Greenbone Vulnerability Manager, which was previously known as OpenVas, can be installed by running the following command:

sudo apt install gvm -y

Aircrack-ng – Cracking Password

The software tool suite that is going to be used to try to crack the password of the router is Aircrack-ng. This tool will serve three purposes: motoring, attacking, and cracking. First the networks are going to be monitored. The goal is to capture a handshake when a device tries to connect to the network. You can achieve this by waiting on a device to connect the network or you can proceed to attack the network to force a handshake. In the attacking step, the devices on the network are going to be disconnected from the network by a deauthentication attack. The goal of this attack is to wait for one of the devices to reconnect if they have auto-reconnect enabled.

Once the device has re-established the connection, the monitoring system should have captured the handshake. With the handshake capture it is possible to try to crack the password using a wordlist. For this study, the wordlist that is going to be used is rockyou.txt, which is a wordlist that comes pre-installed on Kali Linux. It is important to note that if you have a wordlist that has weak passwords, the chance of cracking the router password is going to be less likely. If the password follows a strict format (like alphanumeric and special characters) then it is also unlikely to be cracked.

Nmap – Device and Port Scanning

The software suite that is going to be used in the study for scanning the devices in the network and the open ports is going to be Nmap. To take an offensive approach Nmap will be used with Vulners and Vulscan scripts to check for vulnerabilities. The scripts are not going to be discussed since they are out of the scope of this study. For more information on these scripts, you can find it on the Vulners GitHub [2] and the Vulscan GitHub [3]. Nmap is going to be used to check the devices that are running on the network. This software tool can also detect the OS that the device is running using the Nmap database.

After the devices and system information is retrieved from the devices, Nmap is going to be used to check which ports are running and what are some possible services that are running on them. Here, with the aid of Vulners and Vulscan databases, Nmap is going to be checking if there are some possible vulnerabilities that the services may have. It is important to know that these checks are mostly based on the OS and version running in the devices and services. If the user has taken the necessary steps to protect the device and/or services from those vulnerabilities, then the attack will fail. The goal here is to detect if there are some vulnerabilities on the devices/services running in the network. If there are vulnerabilities, Nmap will not be used to attack them, and the next step would be to try to find a proof of concept (POC) for attacking a device/service with that vulnerability. Vulners and Vulscan will prompt websites with POC and documentation of the vulnerability if they are on the databases.

Metasploit – Check Vulnerabilities and Exploits

This part of the study is going to be hands on. Here Metasploit is going to be used to try to detect vulnerabilities in the devices/services in the network and try to exploit them. The software tool is capable of setting payloads and to check how likely is the device/service to be vulnerable to a specific attack. For the attack, the command/services that are going to be used are auxiliaries, exploits, and payloads. Auxiliaries are scripts that are written to perform a task. These scripts are going to be useful to detect vulnerabilities in the devices and services running on the network. Exploits are going to be the pieces of code that are used to perform the attack against the vulnerability. In term of exploits, the payload is going to be an action that is performed after executing the exploit.

The Metasploit framework is user friendly and has the actions and services categorized. So, if you were to explore what Metasploit has for Windows OS you can go to the Windows OS module and find everything available related to Windows OS.

Greenbone Vulnerability Manager – Check for Vulnerabilities

The Greenbone Vulnerability tool suite is fairly similar to Metasploit. In this study, the GUI version is going to be used. The Greenbone Vulnerability tool suite is powered by Greenbone, and it was previously known as OpenVas until 2017. The goal with this tool is to find vulnerabilities on the devices and services running in the network. Once the results are retrieved from the scanning, the results are going to be compared with the Metasploit's findings.

Contrary to Metasploit, Greenbone Vulnerability Manager is going to be used just to scan and find vulnerabilities. If there are critical findings in the report, a search for a POC to exploit the vulnerability is going to be conducted to try to exploit it. Greenbone results are going to be presented on a graphic report with the severity of the vulnerabilities found in the scanning. If the severity is above 7.0 then the search for the exploit is going to be conducted.

SECURITY ASSESSMENT

For this part of the study, the process of doing the assessment is going to be described briefly as a matter of example on how an individual can perform a security assessment on their network.

Cracking Router Password

First, to set up the network on the machine running Kali Linux the tasks running in the network manager need to be closed. To do so use the following command:

sudo airmon-ng check kill

After stopping the network manager tasks, the network card can be set to monitor mode utilizing the following command:

sudo airmon-ng star <network card name>

In order to check the networks that are available the next command is going to be used:

sudo airodump-ng <network card name in monitor mode>

Once the BSSID of the network is identified, copy the MAC address and the channel of the network. This MAC address is going to be used to monitor the network and to capture the handshake. To start monitoring the network the following command is going to be used:

sudo airodump-ng -c <channel number> --bssid <MAC address> -w <output file name> <network card name in monitor mode>

Note: the output file name is going to be the name of the file containing the capture.

Once Airodump-ng has started to monitor the network for the handshake, the next step is deauthenticating a device in the network on a different terminal instance. Note that you can stay in monitor mode until a device tries to connect to the network and then the handshake would be captured but for simplicity and time saving you can disconnect devices in the network to capture the handshake once they are reconnecting to the network. The command to deauthenticate devices on the network is:

sudo aireplay-ng -0 -a <MAC address> <network card name in monitor mode>

in which *-0* deauthenticates the attack and *-a* would be the MAC address of the access point.

After running the deauthentication attack, check the terminal instance running the monitoring. If a handshake has been captured proceed to crack the password with the wordlist, otherwise wait for the handshake to be captured. The command for starting the cracking process is the following:

sudo aircrack-ng -a2 0w <wordlist file path location> -b <Access' point MAC address> <output file name>.cap

The last step is to wait until the cracking has been completed. The terminal should prompt if the password was found or not. It is important to note that these types of attacks are going to be successful depending on the type of password (whether it's strong or not), the wordlist used, and if the password used has been leaked and published on the internet.

Network Mapping and Vulnerability Scanning

In this study, Nmap is going to be used for network mapping. The findings are going to be compared with the devices that are available through the router setting manager. The goal is to find what devices are running in the network and what kind of services are they running. The following command is going to be used to check the devices and services running in the network:

sudo nmap -sP 192.168.0.0/24 -O

This is going to prompt the devices connect to the network and what OS are they likely using. To check the services running in the open ports the command would be:

sudo nmap -sS 192.168.0.0/24

After checking the devices and services connected to the network, the next step is going to be to check the network for vulnerabilities using the Vulners and Vulscan scripts. To obtain the scripts you need to clone them from their GitHub repositories [2] [3]. The command to run the scripts is the following:

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

After the scripts are done the results are going to be saved on the specified file.

The next tool suite that is going to be used for vulnerability scanning is Metasploit. The auxiliary modules that are going to be used in the study are going to depend on the devices and services running in the network. The following command are going to be used to navigate through the Metasploit command-line:

To start the command-line:

sudo msfconsole

To navigate through the auxiliary modules:

use auxiliary + tab

To navigate through the exploit modules:

use exploit + tab

To show the configuration needed:

show options

Once it has been determined if there is a vulnerability that can be exploited, the payload would be set and run on the target.

The Greenbone Vulnerability Manager is going to be the last tool suite utilized in this study. Since Kali Linux does not include Greenbone Vulnerability Manager on the pre-installed software the following command is going to be needed to install it:

sudo apt install gvm -y

Then, once the software tool suite has been installed, the software needs to be setup with the following command:

sudo gvm-setup

After setting up the software suite, a check is going to be executed to make sure that the packages and services are updated:

sudo gvm-check-setup

If there are services or packages that need to be updated the command-line terminal will prompt the command needed to update them. After setting up the GVM and checking if the services are up-to-date the next step is to copy the IP address provided on the command-line and use admin for username and the password provided on the command-line terminal.

Once the login has been completed, a task is going to be started using the task tab on the main page. The target IP address is going to be 192.168.0.0/24 to check 254 possible consecutive hosts on the network. The settings are going to be left as default on this task. After setting up the tasks and clicking save, the tasks is going to start running. Once it has been completed the results are going to be available on the Results and Report tabs. The results are going to be gathered and saved to compare them with the findings on Metasploit. If there are a vulnerability with 7.0 rating of severity or higher an online search is going to be conducted to try to exploit the vulnerability.

Finally, once all the scans and test have been completed if there are severe vulnerabilities, they are going to be fixed for the benefit of the people using the network. If there are no vulnerabilities, then it can be considered to use other software tools to conduct an assessment in the future.

RESULTS

Aircrack-ng was not able to crack the password of the router. The router was using the pre-shared key that the ISP configured. In order to protect a router password from being cracked, the password needs to be strong, and the password should not have been leaked. Since this password was strong enough and it was not leaked, the cracking process was not successful. The wordlist rockyou.txt did not have the password that the router was configured with. Nonetheless, an individual should be aware if the ISP set a password that is not considered strong and the set of passwords of the ISP is not available online.

In terms of network mapping for this study, the findings using Nmap are going to be compared with the devices that are found on the router manager page. The information retrieved from the router manager page is presented in figure 1.

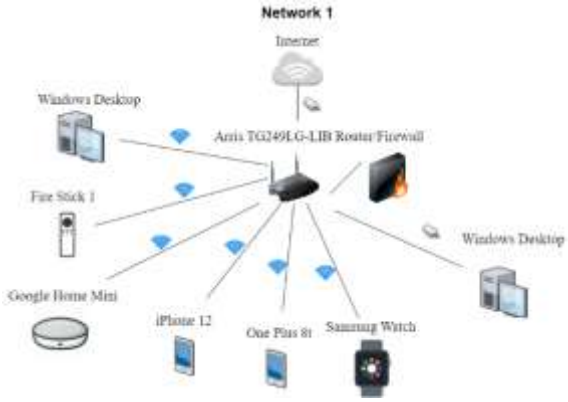

Figure 1. Network 1 Diagram

The devices connected to the network 1 found using Nmap were:

Nmap scan report for 192.168.0.1
Host is up (0.0048s latency).
MAC Address: AC:F8:CC:5E:BA:0A (Arris Group)
Nmap scan report for 192.168.0.2
Host is up (0.078s latency).
MAC Address: 68:DB:F5:C0:F0:1B (Amazon Technologies)
Nmap scan report for 192.168.0.3
Host is up (0.081s latency).
MAC Address: 00:F6:20:6A:92:3B (Google)
Nmap scan report for 192.168.0.4
Host is up (0.080s latency).
MAC Address: AC:67:5D:C2:72:5C (Intel Corporate)
Nmap scan report for 192.168.0.7
Host is up (0.078s latency).
MAC Address: 68:DB:F5:C0:F0:1B (Amazon Technologies)
Nmap scan report for 192.168.0.3
Host is up (0.081s latency).
MAC Address: 00:F6:20:6A:92:3B (Google)
Nmap scan report for 192.168.0.4
Host is up (0.080s latency).
MAC Address: AC:67:5D:C2:72:5C (Intel Corporate)
Nmap scan report for 192.168.0.7
Host is up (0.078s latency).
MAC Address: 60:6B:FF:AD:41:6F (Nintendo)-
Nmap scan report for 192.168.0.9
Host is up (0.067s latency).
MAC Address: 54:27:1E:06:B3:E3 (Azure Technology)
Nmap scan report for 192.168.0.252
Host is up (0.0048s latency).
MAC Address: 00:00:CA:01:02:03 (Arris Group)
Nmap scan report for 192.168.0.8
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 2.93 seconds

Nmap managed to map most of the devices connected to the network except for iPhone 12, OnePlus 8t, and Samsung Watch. The Nmap scripts Vulscan and Vulners did not find any possible vulnerabilities on their databases. This does not mean that there are not vulnerabilities, but it does point out that there are no superficial ones.

For Metasploit there were only two results that can be used as a possible exploit. One of them was a file transfer service that was running on Windows OS. The implementation of the exploit was not successful since it has been patched on the 3.1.1 version of SMB. The other one was a rather rudimentary exploit for a fire stick TV device. For casting YouTube videos there is a services running that you can use to send the video ID of the video

you want to play. With a script looping the auxiliary module you can sort of DoS the fire stick on a loop of launching the video on YouTube making the device unusable in the meantime.

The results of the report made using Greenbone Vulnerability Manager are presented in the figure 2. In the scan there was one vulnerability that surpassed the 7.0 severity threshold. The other ones were below 5.5. For the vulnerability above 7.0 threshold, the Vulners script was used to try to exploit it, but it was not successful. Since there were no other POC to exploit with the tools that were used in this study, there was no further research on that matter. The vulnerability was patched using a vendor fix available that GVM prompted in the report.

In terms of which tools performed better for vulnerability scanning, it would be GVM. GVM was the tool that did find the most quantity and severe vulnerabilities on the network. It can be pointed out that the findings both in GVM and on Metasploit were different. This could be due to the fact that when using Metasploit you need to check all the services almost manually and in GVM you can make them automatically with just running one task. The vulnerability found in Metasploit could have been exploited if the SMB version was 2.0 or lower. For versions 3.0 and higher, there are a couple of POC on how to exploit them but none of them worked on this study.

CONCLUSION

In the study there was only one critical vulnerability, even though the systems and services are 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 it can be used to proof if the infrastructure of the network has measurements to mitigate and protect the information.

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)
SSL/TLS: Report Non Weak Cipher Suites	0.0 (Log)
Check open ports	0.0 (Log)
HTTP Server type and version	0.0 (Log)

Figure 2. GVM Scan Results

REFERENCES

[1] K. Parker, J. M. Horowitz, and R. Minkin, “How the coronavirus outbreak has—and hasn’t—changed the way Americans work,” PEW Research Center, December 9, 2020 [Online]. Available: https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work/

[2] Github, “vulnersCom / nmap-vulners.” Accessed February 10, 2022 [Online]. Available: https://github.com/vulnersCom/nmap-vulners.git

[3] Github, “scipag / vulscan.” Accessed February 10, 2022 [Online]. Available: https://github.com/scipag/vulscan.git