**Research Report: Ransomware Recovery**

Adrian Varela

WTAMU

CIDM 6340-70: Network Management and Information Security

Professor Murray Jennex

August 6, 2023

WHAT DID YOU DO

The inventory list I created from the NMAP software I was able to locate the six devices that were connected, by utilizing the nmap -sn function that gave me all the devices that were connected to my network. When viewing this and the importance of each device, I decided which of these products I could not pay bills, complete my assignments for school and work, and which would stop the functions of the house. In this assignment I did not have any servers in my home, but I did put the importance of the router as top priority due to all IOT devices being connected to this.

The second portion I did was identifying the vulnerabilities for specific devices with the utilization of Wireshark. I also utilized ShieldsUp and Nessus through these products from the utilization of which ports were left open or comprised. I first went through Wireshark which could help identify which of these devices had the vulnerabilities. Through the use of this application, I was able to view vulnerabilities through my network and devices. This gave me detail of what devices I needed to locate as well as the details of destination. Once this was completed, I went and inputted the IP addresses for my devices and networks to view if there were any specific ports or even more vulnerabilities I missed with Wireshark with the use of Nessus. ShieldsUP gave me the specification that none of my ports were open or closed but stayed in Stealth.

The devices I chose to utilize passwords are the DSL, the 2 phones, Adrian’s Air 2 and the Firestick. The DSL has a guest account to log into and the primary account. The phones will utilize biometrics as what they have and a passcode for what they know. The Air 2 will also utilize the biometrics and passcode rule. Finally, the Firestick will be implemented with a passcode due to it traveling with me at work all the time. The list I created can be viewed as Figure 1. and Figure 2. (I did not add the IP addresses for security purposes.)

|  |  |  |
| --- | --- | --- |
| Device Name | Device Priority | Device vulenrabilies |
| dsldevice.attlocal.net | 1 Critical | 0 |
| Adrians-iphone.attlocal.net | 2 Critical | 0 |
| Olivias-iphone.attlocal.net | 3 Vital | 0 |
| Adrians-Air-2.attlocal.net | 4 Vital | 4 |
| Adrians-Firestick.attlocal.net | 5 | 0 |
| 50SharpRokuTV.attlocal.net | 6 | 0 |

*Figure 1. Inventory Checklist*

|  |  |  |
| --- | --- | --- |
| Components for Backup | List of Backups | Passwords that need to be backed up |
| Apple ID for apple devices | A second Authorizing account | Apple ID password |
| AT&T Router | A second router for my devices to connect | My Network password  My Router password |
| My applications | A backup for all applications utilized through my network | I vary through passwords and would have to utilize haveibeenpwned for security |

*Figure 2. Back up Inventory List*

WHAT WERE THE RESULTS

The results were just as expected from the devices as majority of the devices were secure and up to date. The use of the Air 2 as a destination, displayed that there two packets in which there was a TCP RST which may correlate some suspicious activity. There were also two packets that relayed the Air 2 was attempting to access a destination and again there was a TCP reset. The further this investigation went the further in-depth I went to utilize ShieldsUP and Nessus to find more details. The result for ShieldsUP displayed that none of the ports were open from my network as well as it being in stealth. The outcome of this suspicious device was that the SSL Certificate cannot be trusted. For this easy fix all I would have to do is to purchase or generate a proper SSL certificate for this service. That means that I have to gain an SSL certificate that is utilized properly for the destination in which I am trying to gain entry. My other device displayed were all secure for this exercise as well. The other part I did was test my network in which there was one particular vulnerability I needed a DNS recursion to be allowed.

As for finding out what passwords are good for my login devices, I utilized the site of haveibeenpwned to see if my email passwords have been compromised. As hypothesized, they have not due to the fact I continually change my passwords in a quarterly basis.

WHAT DID YOU LEARN

For this activity I learned the vulnerability of any IOT device. The utilization of a personal network in which I keep up to date and ensure t compliance for a great defense against a cybersecurity attack was still at risk. This is really eye opening as there are limited devices that can utilize my network. In a large company there are many people that can cause vulnerabilities an administrator might overlook due to having complex situations that they may be unfamiliar with dealing. The other issue is that with many packets coming and going with a large or small business the attack surface is much larger due to the incoming packets coming from unknown sources. If this happens Wireshark makes a great tool to see where the source is from the attack. This is great for after ransomware has infected the network or device. The best way I learned to prevent ransomware from all these exercises and from real world scenarios is to utilize training. Once a business or person understands the signs of an attack the prevention of malware and ransomware obtaining information or blocking access becomes much easier to handle. If the attack has occurred there are scenarios in which a person has lost all of the information that was saved in that device.

The final part that I learned much from in this last week was the use of passwords. I learned of haveibeenpwned and the practical use of the website to ensure you or your company are not utilizing a password that has not been compromised. Although it is not advised to utilize a repeated password, it’s even less useful to utilize a password that has been compromised.