­­

**Adriana Manzano-Romo**

Network Vulnerability Assessment Report

December 6, 2023

Report Prepared by:

**Michael Relva-Manzano**

**Michaelrelva04@gmail.com**

ITIA-1310

Certified Ethical Hacker

**Fall**

The information contained within this report is considered proprietary and confidential to the {Adriana Manzano-Romo}. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss to the {Adriana Manzano-Romo}. This report should be distributed to individuals on a Need-to-Know basis only. Paper copies should be locked up when not in use. Electronic copies should be stored offline and protected appropriately.

Executive Summary 4

Project Scope 4

In Scope 4

Out of Scope 4

Site Activities Schedule 5

Date – xx/xx/xx 5

Date – xx/xx/xx 5

Date – xx/xx/xx 5

Date – xx/xx/xx 5

Background Information 6

Client Description 6

Location Description 7

Devices in Scope 8

Network and Wireless Security 9

Potential or Actual Vulnerabilities 9

Strong wireless authentication and encryption should be in use 10

The password to access the wireless network should be strong 11

The router administrator password should be changed from the default setting 12

The firewall in the wireless router should not permit external traffic 13

The wireless router firmware should be current 14

System (PC or end device) Security 14

Potential or Actual Vulnerabilities 15

Do regular users on PCs and Laptops have Administrator privileges? 15

Are end user devices updated with current operating system versions/patches? 16

Are PCs and Laptops protected by antivirus and antimalware software? 16

Personal Security 18

Potential or Actual Vulnerabilities 18

Are all devices protected with strong passcodes and/or biometrics? 18

Are strong passwords used for email and banking accounts? 19

Social Media accounts are secure 20

The clients understand how to manage passwords securely 20

Data Loss and Disaster Recovery 22

Potential or Actual Vulnerabilities 22

Are key computer systems backed up regularly? 22

Is there a disaster recovery plan or disaster preparedness plan? 23

Is there adequate insurance for the building and/or contents? 25

Physical Security 26

Potential or Actual Vulnerabilities 26

The Rainbow Bridge to the Magical Treehouse is frequently unguarded 26

Are adequate smoke alarms and carbon monoxide detectors installed and functioning? (REQUIRED) 27

Are entry points (exterior doors and locks) functional and secure? 28

Is exterior lighting and perimeter security adequate? 29

Network Scan – Internal 31

Port Scan Analysis – One Internal Device 32

Network and Port Scan Analysis – External 32

Wireless Range Analysis 33

Action Plan 35

# Executive Summary

A network vulnerability assessment was conducted for Adriana Manzano from September 6th, 2023 – November 15th, 2023. Tests included so far are network scans that mapped hosts, open ports, and operating systems. Also, an inspection was conducted to assess physical security. Perimeter fencing, lighting, router security, and more were evaluated. Information security is extremely important for my client. My client works for the government remotely from home. Bank information, passwords, personal information, and other work-related information travel in and out of the network, so the security of my client’s data is extremely important.

# Project Scope

## In Scope

The following activities are within the scope of this project:

* A physical walk through of the client’s home to assess physical vulnerabilities.
* A series of scans to map all hosts, open ports, operating systems, etc.
* Making sure operating systems are up to date.
* Assessment of network and wireless security
* System Security assessment
* Data loss and disaster recovery assessment
* Wireless Range Assessment

## Out of Scope

The following activities are NOT part of this security assessment:

* Penetration Testing of systems, networks, buildings, laboratories or facilities.
* Social Engineering to acquire sensitive information from staff members.
* Testing Disaster Recovery Plans, Business Continuity Plans, or Emergency Response Plans.

# Site Activities Schedule

### Date – 09/13/2023

Perform Nmap scan on host network to identify all devices. A port scan was also performed to identify open ports. An external scan of the public IP address was also conducted.

### Date – 09/20/2023

Identified what type of encryption is being used on the router (wpa2) and made sure that the network is private and not publicly accessible.

### Date – 9/20/2023

Walked around client’s premises and checked for fencing, lighting, door locks, etc.

**Date - 9/27/2023**

Assessed wireless network password, router’s administrator account password, firewall settings, and firmware.

**Date – 10/5/2023**

Assessed System security such as if regular users have Admin privileges, are operating systems up to date, do devices have antimalware/ antivirus, do all devices have strong passwords and or biometrics, etc.

**Date – 10/22/2023**

Assessed account security, do email and bank accounts have strong passwords, are social media accounts secure, do clients know how to manage passwords securely?

**Date – 11/2/2023**

Assessed data loss and recovery. Are key computer systems backed up regularly, is there a disaster recovery plan, does the home and its contents have insurance?

**Date 11/12/2023**

Physical security was assessed. Are there adequate smoke and carbon dioxide alarms, are entry points functional and secure, is exterior lighting adequate?

**Date 11/14/2023**

Wireless network range was assessed to see how accessible the network is from outside the client’s home.

# Background Information

## Client Description

My client is Adriana Manzano-Romo, I am reporting on her home, the biggest concerns I have are the fact that WPA2 is being used on the router and password information is written on a sticker which is right on the back of the router. The administrator account is also still using the default password, smoke alarms are taken out, and wireless range stretches outside of the home. Typically, 3 users are always on the network, 1 teenager and 2 adults. The teen, and oldest adult (client) don’t have much computer knowledge. The other adult has more computer knowledge than his other family members because he is studying cybersecurity. The network is used to remotely work from home, education, and entertainment.

## Location Description

The building is in a suburban area. It is a house that is about 1500 sq ft. It has 2 floors along with a basement and 3 bedrooms. It has houses on both sides, each about 15 feet away and a main road directly behind.



# Devices in Scope

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Type** | **Device name**  **(Or commonly used name)** | **Operating System and version** | **Primary User** | **Description**  **(Manufacturer, model number, etc.)** |
| Laptop | Marianas Laptop | Windows 11 | Mariana | HP, Model 15-dy4037nr |
| Smartphone | Adrianas iPhone | IOS 17 | Adriana | iPhone 13, apple |
| Wireless Router | Technicolor CH USA | Linux 3.x-4.x | All | Technicolor, **DPC3941T** |

# Network and Wireless Security

## Potential or Actual Vulnerabilities

Listed below are the ***potential or actual*** network security vulnerabilities analyzed during the assessment. Use the Risk Rating to evaluate the significance of the vulnerabilities and the Recommendations for suggested actions to remediate the vulnerabilities.

### Strong wireless authentication and encryption should be in use

**Explanation**

Wireless authentication and encryption are essential for the security of a network. WPA3, the latest form of encryption/authentication provides increased protection of data as it moves across a wireless network. It provides a private key exchange between clients and servers. A unique session key is generated for every individual session a user initiates. AES is an encryption algorithm; it is what helps secure data transmission and storage. AES is the encryption which is used in WPA3. Not having proper authentication and encryption poses a big risk to a network. Someone with malicious intentions could sniff network traffic and then use tools to unencrypt the data and see information such as passwords and personal information if encryption isn’t present or strong enough.

**Observations/Examples Found**

At the site, the router has a sticker which says what type of encryption is being used which is WPA2.

**Documentation**

A blue and orange marker on a black device

Description automatically generated

**Risk Rating**

The risk of this vulnerability is medium. If someone targets this network specifically and knows the encryption used, it can be a big risk since there is a lot of sensitive data coming in and out of the network. But on a day-to-day basis, since it is a residence and not an organization with many people coming in and out, the chances of someone sophisticated enough to be able to find the vulnerability and exploit it is low.

**Recommendations**

* Upgrade to WPA3 by contacting your ISP to replace the router.
* If your ISP doesn’t want to give you a new router, change and go to another ISP that provides WPA3 routers.

### The password to access the wireless network should be strong.

**Explanation of Vulnerability**

A strong password to gain access to a wireless network is essential. If a wireless network password is weak, it can allow unauthorized devices to access the network. With access to the network, a malicious actor can do many things such as use sniffers to intercept network traffic and other man-in-the-middle attacks. It also makes it easier for an attacker to spread malware/malicious code to other hosts on the network. It will make it very easy to map network devices and perform reconnaissance.

**Observations/Examples Found**

Wireless network password is strong, it is 10 characters long with uppercase, lowercase, numbers, and special characters (Xxxxxx###$)

**Documentation**

Confirmed on the administrator account that the password is strong enough. A screenshot of a computer

Description automatically generated

**Risk Rating**

The password is very short and has no special characters. It would be easy to use a tool to crack it and get unauthorized access to the network. This could allow someone to log into the router and change configurations, which is a very big vulnerability.

**Recommendations**

* I have no recommendations for my client.

### The router administrator password should be changed from the default setting.

**Explanation of Vulnerability**

The router administrator password is what is used to access the router’s administrator page. In this page, you can do many things such as see devices connected to the network, change network settings like the Wi-Fi password and SSID, and configure many other things on the router. There are many things that could happen, for example, since routers use DHCP for hosts on the network, an attacker could change the DNS server that devices connect to, to his own DNS server and redirect traffic to malicious websites to get personal information. You could also change the default gateway to something else and in turn, intercept all wireless traffic.

**Observations/Examples Found**

* Since the client never logged onto the router administrator page, I called Xfinity to see if I could find a way to get that information. They then told me that if no one has ever logged onto it, that it should still have the default username and password. After putting in the default username and password, I was able to log in and a “You are using a default password. Please change the password.” message appeared.

**Documentation**

. A screenshot of a computer

Description automatically generated

**Risk Rating**

The risk of this vulnerability is medium. My client often has workers that do jobs in the house and other people. If someone with the wrong intentions enters the house and logs onto the administrator account with the default password, it can be very dangerous.

**Recommendations**

* It is recommended that my client changes both her username and password from the default setting to something longer and more complex.

### The firewall in the wireless router should not permit external traffic

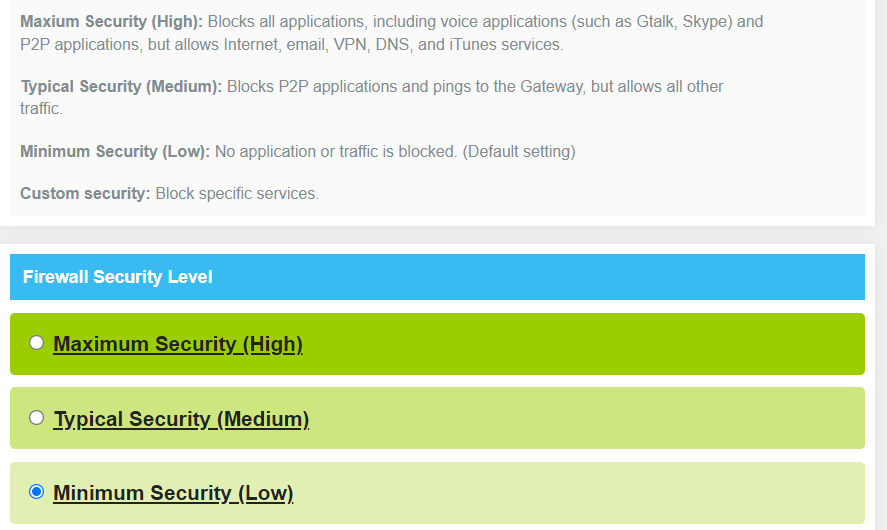
**Explanation of Vulnerability**

The purpose of a firewall is to act as a barrier between the internal network and the internet. It can block connections from certain ports/protocols and certain rules can be set to protect your network. For example, by blocking external traffic, inbound connections from the internet will be dropped. This means that the router will only let established connections initiated from inside the network to pass through. Without this configuration, anyone on the internet who has your public IP address, at the very least, can attempt to breach your network and its devices.

**Observations/Examples Found**

When I logged onto the router’s administrator page to look at the firewall settings, I noticed that the “minimum security (low)” option was selected. This option specifies that no applications or traffic is blocked.

**Documentation**



**Risk Rating**

This is a medium risk vulnerability. Having the lowest security level can be very risky. Although a network may be secure, everyone on the internet has at least a chance to breach it since no type of traffic or external connections are blocked.

**Recommendations**

My recommendation is to block external traffic. On top of this, it would make sense to enable custom security and block traffic from certain protocols and services that are not needed in the client’s home.

### The wireless router firmware should be current

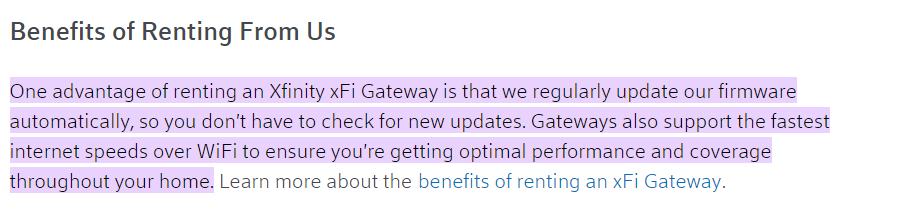
**Explanation of Vulnerability**

The purpose of the wireless router firmware is to control & manage the hardware and software of the router. It provides it the necessary instructions to function properly. Outdated firmware could pose a big risk to a network if it has known vulnerabilities which could then be exploited by a hacker. If not up to date, hackers could intercept network traffic and take control of devices on the network, including the router.

**Observations/Examples Found**

* The router’s firmware is up to date.

**Documentation**

The routers administrator page doesn’t show what version of firmware the router is on, so I called Xfinity customer support. They mentioned that the router’s firmware is up to date since Xfinity automatically updates all of their routers without the client having to do anything. To make sure, I also checked on Xfinity’s official site. 

**Risk Rating**

The customer is at low risk. The reason why is because the router is updated automatically without any work from the client.

**Recommendations**

* I have no recommendations other than if the client switches to another ISP, that they make sure that the new router also has automatic firmware updates so that they mitigate vulnerabilities in their network.

# System (PC or end device) Security

## Potential or Actual Vulnerabilities

Listed below are the potential or actual system security vulnerabilities analyzed during the assessment. Significant problems are noted and recommendations to remediate them are described.

### Do regular users on PCs and Laptops have Administrator privileges?

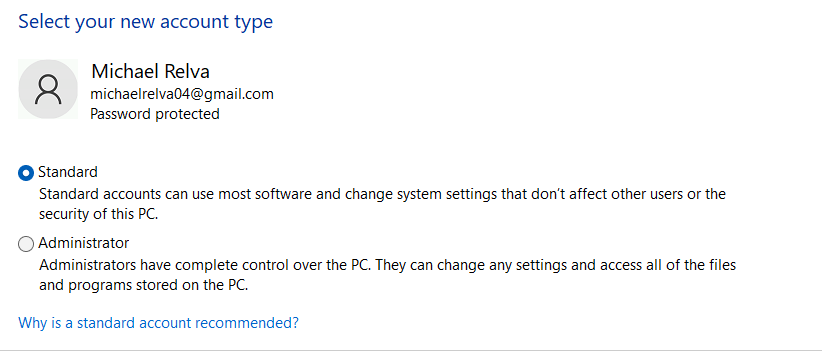
**Explanation of Vulnerability**

If regular users on PCs and Laptops have administrator privileges, it is a very big vulnerability to a network. It would allow regular users to make changes to system-wide settings such as network configurations, security policies, and user permissions. Regular uses could also accidentally, or on purpose uninstall/ install software, and modify system files. These software’s that are downloaded could be malicious to a network and modifying the system and its files could negatively impact the systems performance and security.

**Observations/Examples Found**

No users on the network have administrator privileges.

**Documentation**



The other two laptops in the network don’t have administrator privileges since one is a work laptop, and the other one is a laptop provided by a school.

**Risk Rating**

The risk rating is low since this vulnerability is not present. All devices have standard privileges, not administrative privileges.

**Recommendations**

Make sure that administrative privileges are only used when needed and turned off when not.

### Are end user devices updated with current operating system versions/patches?

**Explanation of Vulnerability**

An operating system is like the brain of the computer. It manages computer hardware and software, allowing users to interact with the computer. Updating/patching operating systems is very important. This is because with every update, there are fixes that relate to both security and performance. If operating systems are not updated, it can be a big vulnerability. It could allow unauthorized access, data breaches, and execution of malicious code on a system.

**Observations/Examples Found**

* After looking at all of the laptops, pcs, and tablets in the home, all were up to date except a smartphone. It was an iPhone XR that needed to be updated to iOS 17.
* All were up to date except for one phone.

**Documentation**

A screenshot of a phone

Description automatically generatedA screenshot of a computer update

Description automatically generated

**Risk Rating**

This is a low-risk vulnerability. The reason why is because after looking at the update and what it specifies, there are only enhancements to performance and the visual aspect rather than any security patches.

**Recommendations**

* Although there aren’t any security improvements, I still recommend that the operating system be upgraded just as best-practice.

### Are PCs and Laptops protected by antivirus and antimalware software?

**Explanation of Vulnerability**

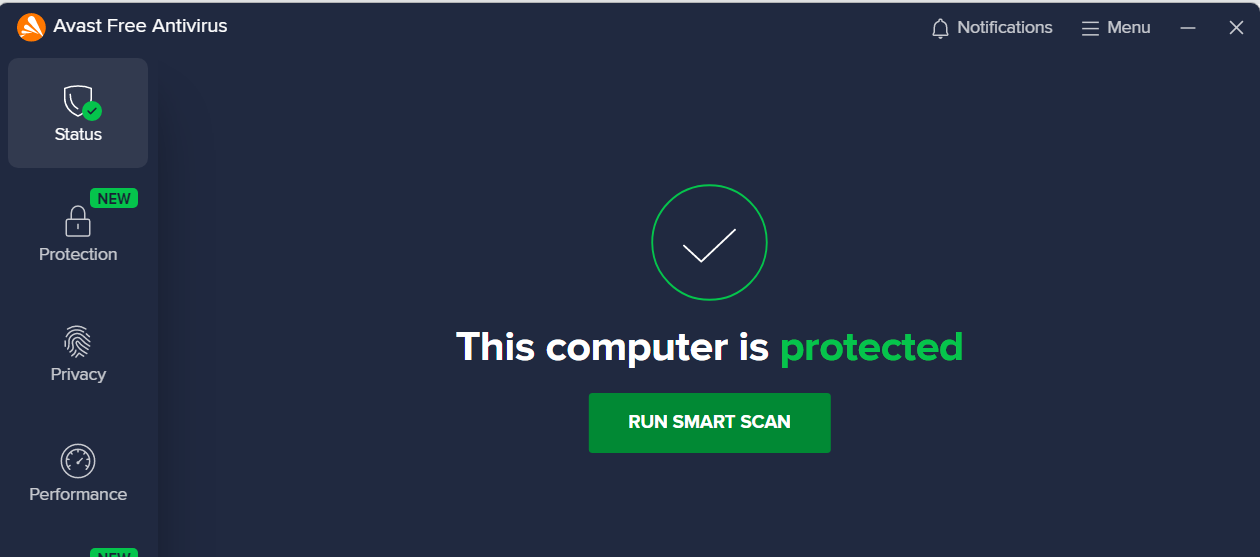
The purpose of antivirus and antimalware is to have an extra layer of defense against malware and viruses. They are software that can be bought, or some can be installed for free. Antivirus is used for finding worms, viruses, Trojans, and removing them. These are known and more established threats. Antimalware on the other hand, focuses on scanning and removing a broader range of threats like spyware, adware, ransomware, and much newer exploits like polymorphic malware. The possible consequences of not having either could be detrimental to a network depending on the virus/ malware, and which device gets infected. Hackers could gain remote access to your device, steal personal information like passwords and credit card information, and much more.

**Observations/Examples Found**

* Out of the three laptops at the home, all of them have antivirus/ antimalware.

**Documentation**

Document this observation with a screenshot, photo, or some other means.

A blue screen with white text

Description automatically generated

The second screenshot is for the client’s work laptop. She has Symantec antivirus and antimalware but does not have permission to open the software.

**Risk Rating**

The risk is very low because the vulnerability is not present. There could be a risk of false negatives with these software’s, but Symantec has a 99.9999% accuracy rating and Avast has a 97%.

**Recommendations**

* My only recommendation is to keep renewing antivirus/ antimalware subscriptions and if my client can’t afford it anymore, she can always use free versions for her devices.

# Personal Security

## Potential or Actual Vulnerabilities

Listed below are the potential or actual vulnerabilities related to Personal Security analyzed during the assessment. Use the Risk Rating to evaluate the significance of the vulnerabilities and the Recommendations for suggested actions to remediate the vulnerabilities.

### Are all devices protected with strong passcodes and/or biometrics? (REQUIRED)

**Explanation of Vulnerability**

Strong passwords and/or biometrics are extremely important to guaranteeing security to your devices. Without these security measures, in the case that you’re away from your device, or someone has possession of it, they have the possibility of logging into it and stealing whatever personal information they want.

**Observations/Examples Found**

* {Describe examples of this vulnerability found at the site}

|  |  |  |  |
| --- | --- | --- | --- |
| **Device name**  **(Or commonly used name)** | **Protected with passcodes or biometrics?** | **Is current passcode strong?** | **Describe the passcodes or biometrics**  **(Passcode length, alphanumeric, complexity, fingerprint, Face ID, etc.)** |
| Router | Password | Yes | 10 character length password with numbers and special characters |
| Adriana’s Laptop | Both | Yes | 10 character length password with numbers and special characters, also uses Okta for dual authentication. |
| Mariana’s Laptop | Password | Yes | Strong password 9 characters with numbers and special characters |
| Adrianas iPhone | Biometrics | 6-digit passcode | Uses face scan ID |

**Documentation**

Spoke to Adriana about her work laptop security. She explained that it requires her to put in her password (10 characters) and once that is entered, Okta asks for a second form of authentication through her phone to make sure it’s her.

A screenshot of a phone

Description automatically generatedThe picture to the left is the face id for Adriana’s iphone. It requires her to either scan her face or enter a 6-digit passcode.

**Risk Rating**

There is a low risk of anything happening to all devices except the router. The router’s password is not strong and if anyone manages to log into it, the consequences can be very big. This will allow whoever to change configurations and do many more things. All other devices are secure.

**Recommendations**

I have no recommendations but to keep making sure that all devices always have strong password and to use biometrics to your advantage.

### Are strong passwords used for email and banking accounts?

**Explanation of Vulnerability**

Banking and email accounts are two of the most important websites or applications used by users. Users should use strong, unique passwords for both of these services to prevent unauthorized access to their financial and communication systems. Two-Factor Authentication (2FA) should be used when available.

**Observations/Examples Found**

* The youngest daughter doesn’t have an email or bank account, but the two adults use strong unique passwords for both email and bank accounts.

**Documentation**

Both adults have their emails under Gmail which has a requirement that users have a password of at least 8 characters long, contains uppercase and lowercase characters, numbers, and special characters. Both emails also use Two-Factor Authentication. For web banking accounts, both adults have passwords which are 10+ characters in length which includes uppercase, lowercase, numbers, and special characters.

**Risk Rating**

Rate this risk on a scale of low, medium, and high, and EXPLAIN how the risk for this vulnerability if it is present. (This is a subjective rating, but you should rate the risk and then explain why you rated it that way.) This should be in the context of this customer and their situation, NOT the worst-case scenario. If the vulnerability seems to not exist, then say the customer is at “low risk” and explain why.

**Recommendations**

* I recommend using passwords which are different than banking and email for other online services and applications so in the case that one gets compromised, it won’t affect anything else.

### Social Media accounts are secure.

**Explanation of Vulnerability**

Having secure social media accounts includes using strong passwords, using two-factor authentication, being cautious about information posted online, and whether accounts are private or public. It is best practice to only accept those who you know and trust to have access to view your social media accounts. Without proper security, someone with malicious intent can hack your account, send phishing messages, and possibly cause harm in person if personal information is shared online.

**Observations/Examples Found**

All 3 of the people who live in my clients home have social media. The client’s son has Instagram and Snapchat with secure passwords but doesn’t use two-factor authentication. His accounts are also public. My client uses both Facebook and Instagram with strong passwords, but her Instagram account is public. The youngest daughter has TikTok, Instagram, and Snapchat. Although she has strong passwords, all of her accounts are public.

**Documentation**

Document this observation with a screenshot, photo, or some other means.

A screenshot of a social media account

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a social media account

Description automatically generated

These are screenshots of public social media profiles of the people living in the client’s home.

**Risk Rating**

Based on there not being too much information to be found about family members and their personal life off of their social media posts, this is a low risk vulnerability.

**Recommendations**

* I recommend that my client and her family make their accounts private.

### The clients understand how to manage passwords securely.

**Explanation of Vulnerability**

Properly storing passwords is a crucial part of network security. By doing so, it makes it easier for users to use more complex passwords and different passwords for different accounts. There are different ways to store passwords such as a password manager. Most of the time, these are cloud-based services where you can store passwords for all your accounts into one service. To access this, you just have to remember the password to the password manager account. Without practicing secure password management, passwords can be forgotten to important accounts or compromised if not stored securely.

**Observations/Examples Found**

Youngest daughter does not manage passwords securely, she claims she remembers them all. The client’s son manages his and her passwords securely with a password manager.

**Documentation**

A yellow and black logo

Description automatically generatedThis is the password manager used by the client and her son.

**Risk Rating**

The risk is low if the youngest daughter remembers her passwords and doesn’t start using the same password for every account. The client and son are practicing good password management.

**Recommendations**

It’s recommended that the daughter also gets a password manager of her own to more securely store her passwords.

# Data Loss and Disaster Recovery

## Potential or Actual Vulnerabilities

Listed below are the potential or actual vulnerabilities related to backups and disaster recovery analyzed during the assessment. Use the Risk Rating to evaluate the significance of the vulnerabilities and the Recommendations for suggested actions to remediate the vulnerabilities.

### Are key computer systems backed up regularly?

**Explanation of Vulnerability**

The purpose of backups is to allow the customer to restore data that has been deleted or corrupted. If a device used by the customer is not backed up on a regular basis and the hard drive crashes or the computer is destroyed in an accident the information will be lost. If the data is lost the customer could lose valuable personal data or even files required for regulatory or tax reasons.

**Observations/Examples Found**

{Describe examples of this vulnerability found at the site}

|  |  |  |  |
| --- | --- | --- | --- |
| **Device ID or Name** | **Currently backed up?** | **Describe backup method** | **Date of last backup** |
| Michael’s Computer | Yes | Microsoft OneDrive | 10/8/2023 |
| Michael’s iPhone | Yes | Apple iCloud | 10/8/2023 |
| Mariana’s iPhone | Yes | Apple iCloud | 10/8/2023 |
|  |  |  |  |

**Documentation**

A screenshot of a computer

Description automatically generated

A screenshot of a phone

Description automatically generated

**Risk Rating**

Rate this risk on a scale of low, medium, and high, and EXPLAIN how the risk for this vulnerability if it is present. (This is a subjective rating, but you should rate the risk and then explain why you rated it that way.) This should be in the context of this customer and their situation, NOT the worst-case scenario. If the vulnerability seems to not exist, then say the customer is at “low risk” and explain why.

There’s a low risk since all information on the devices is backed up on the cloud. If anything happens to the physical device, it will be accessible as long as you log onto the same account on another device.

**Recommendations**

* I have no recommendations other than keeping password information safe and accessible in the case of a disaster.

### Is there a disaster recovery plan or disaster preparedness plan?

**Explanation of Vulnerability**

It is critical for a homeowner or business owner to have an established plan in place for what to do in case of a disaster. Plans and processes should be established BEFORE a disaster occurs. If the customer has any special needs personnel, they may require more planning to ensure that their needs will be taken care of in the event of an emergency evacuation.

The Department of Homeland Security has guides to help people prepare for disasters:

<https://www.ready.gov/make-a-plan>

**Observations/Examples Found**

The family does not have a disaster recovery plan in place. Important documents cannot easily be found in the case of an evacuation.

**Documentation**

Document the interview with the client(s) and answer the following questions:

|  |  |
| --- | --- |
| Names of clients being interviewed | Adriana Manzano-Romo |
| Date and Time of Interview | 7:30 PM 11/13/2023 |
| Does the customer have children living at home? | Yes |
| Are there pets that would need to be transported in an evacuation situation? Do they have/need pet carriers? | Yes there is one dog in the home, no she does not need a pet carrier. |
| Does the client require important prescription medications?  (Example: Insulin or other medications that would be difficult to acquire in an emergency.) | No |
| Does the client require important documents that could be difficult to replace?  (Example: Passports, visas, birth certificates.) | Yes, the client and her children require passports and birth certificates. |
| Other |  |
| Other |  |

**Risk Rating**

The risk of a successful evacuation without all of the important documents needed is very high. As these documents are not used in everyday life, they have been kept in different areas all around the house and it would take a while to find them all.

**Recommendations**

I recommend that a disaster recovery plan is made in case of an emergency. All important documents should be kept in a secure spot that is also easily accessible in the case of an emergency.

Describe your recommendations for plans the client should have in place for each of the situations described above.

|  |  |
| --- | --- |
| Plan for children | There are no small children in the home, but there should be plans for different scenarios, for example in case of a tornado, run to the basement, or in case of a fire, run outside when smoke alarms go off. |
| Plan for pets | Dog doesn’t need a carrier and is always on the first floor of the house which is important in case of an evacuation |
| Plan for medication | No important medication is needed for the family. |
| Plan for documents | They should be kept in an easily accessible but secure spot in the house. |
| Other |  |
| Other |  |

### Is there adequate insurance for the building and/or contents?

**Explanation of Vulnerability**

In the case of a disaster, this can be a huge vulnerability if the house and/ or it’s contents aren’t insured. A family could lose everything they have worked for their whole lives.

**Observations/Examples Found**

The client does have insurance over the home, additional structures, personal property, additional living expenses, personal liability, and medical expenses.

**Documentation**

A screen shot of a computer

Description automatically generated

**Risk Rating**

The risk is low in case of a disaster happening. The house and all its contents are insured in case anything happens.

**Recommendations**

I have no recommendations for my client.

# Physical Security

## Potential or Actual Vulnerabilities

Listed below are the potential vulnerabilities analyzed related to Physical Security. Use the Risk Rating to evaluate the significance of the vulnerabilities and the Recommendations for suggested actions to remediate the vulnerabilities.

### Are adequate smoke alarms and carbon monoxide detectors installed and functioning? (REQUIRED)

**Explanation of Vulnerability**

Smoke alarms are used to detect the presence of smoke before a fire occurs and alert the residents with a loud alarm. This gives the residents time to leave the premises or eliminate the source of smoke or contact the fire department.

Carbon monoxide detectors are used to detect the presence of carbon monoxide (CO) and alert the residents with a loud alarm so that they can leave the premises and alert the fire department to determine the source of CO.

The NFPA (National Fire Protection Association) has guidelines and recommendations for using both smoke alarms and carbon monoxide detectors:

<http://www.nfpa.org/Public-Education/By-topic/Smoke-alarms>

<http://www.nfpa.org/Public-Education/By-topic/Fire-and-life-safety-equipment/Carbon-monoxide>

**Observations/Examples Found**

Per the NFPA guidelines, were adequate smoke alarms and carbon monoxide detectors found to be installed properly and functioning correctly?

|  |  |  |
| --- | --- | --- |
| **Room** | **Smoke alarm present?** | **Smoke alarm functional?** |
| Son’s Bedroom | Yes | Yes |
| Daughter’s Bedroom | Yes | Yes |
| Adriana’s Bedroom | Yes | Yes |
| Hallway | No | No |
| Living Room | No | No |
| Basement | No | No |
| Kitchen | Yes | Yes |

**Documentation**

A light on the ceiling

Description automatically generated

These are the two spots in the home where smoke alarms were removed due to the battery dying. The left picture is in the hallway, and the right picture is the basement.

**Risk Rating**

The risk rating for this vulnerability is high. The hallway smoke alarm that is missing is in the vicinity of all the bedrooms, which can be a serious danger. The other smoke alarm that is missing is in the basement, which is also very serious, since houses are made of wood in Michigan, fires spread extremely fast.

**Recommendations**

* Install additional smoke alarms in the following areas: Living room
* Install new batteries in the following smoke alarms and carbon monoxide detectors: Basement and upstairs hallway
* Replace the smoke alarms and carbon monoxide detectors every 10 years.

### Are entry points (exterior doors and locks) functional and secure?

**Explanation of Vulnerability**

Working locks for exterior doors are extremely important. In the case of someone having malicious intentions to steal from the home or cause harm to those inside, not having functional and secure locks is a huge problem.

**Observations/Examples Found**

There are functional locks on all doors, front/back. The garage can only be opened with a remote, it can’t be opened from the outside even if you try to pull it up because it locks by itself

|  |  |  |
| --- | --- | --- |
| **Room** | **Description of lock(s)** | **Are the locks functioning properly?** |
| Front Door | Doorknob lock | Yes |
| Back Door | Doorknob lock | Yes |
| Garage | Locks by itself, can only be opened with controller. | Yes |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Documentation**

A wooden door with a gold handle

Description automatically generated A wooden door with black knobs

Description automatically generated

**Risk Rating**

The risk is very low. Working locks are on every door and the area where this house is located is very safe.

**Recommendations**

* Locks are sufficient but it would be recommended to add some type of key pad that can increase security.

### Is exterior lighting and perimeter security adequate?

**Explanation of Vulnerability**

Having exterior lighting is a big part of physical security. It can detour intruders and make it easier for homeowners to spot them. Without perimeter fencing, it makes it very easy for an intruder to take a scan at your home from the outside and see who’s inside and whether it’s worth it to attempt to intrude.

**Observations/Examples Found**

My client’s home has fencing about 7 feet tall all around the house and lighting in the front and back of the house.

**Documentation**

A house with lights at night

Description automatically generatedA deck with a light on it

Description automatically generated

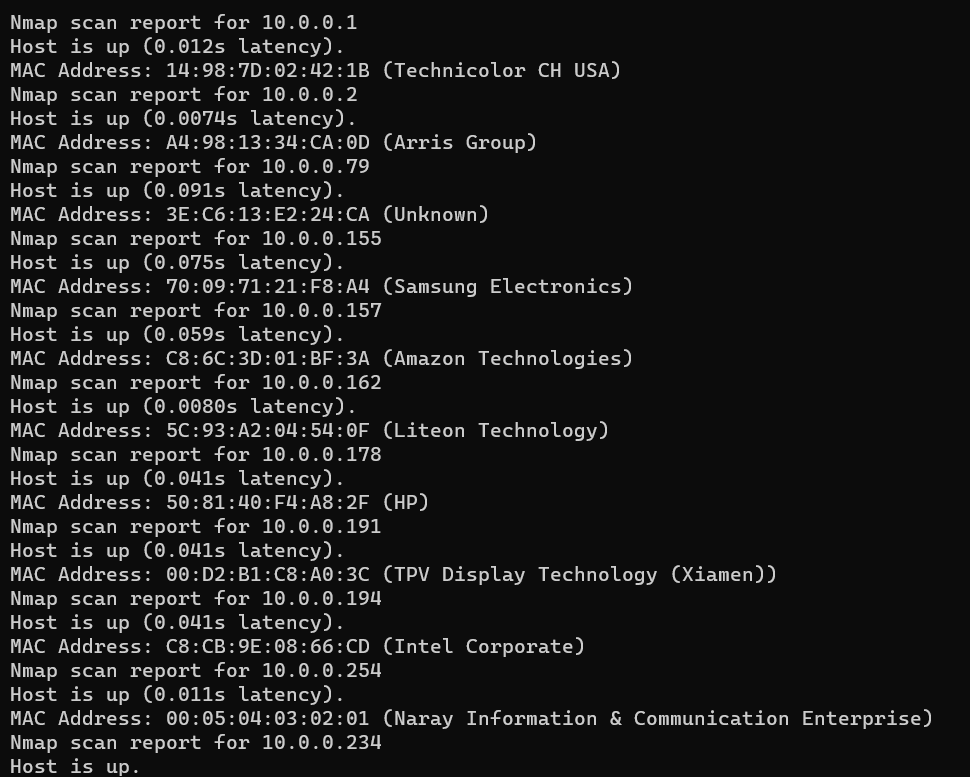
**Risk Rating**

There is no vulnerability present, the risk is low. There is adequate fencing and lighting.

**Recommendations**

There are no recommendations other than making sure fence is always stable and making sure to change lightbulbs in exterior lighting.

# Network Scan – Internal

Performed a scan of the internal network using Nmap. The following is a summary and analysis of the key results. The results of the scan are below 

During the discovery process of devices through the Nmap scan, it was a bit of a challenge to find what device is what by the information given in the ping sweep. But by searching up Mac addresses and manufacturer information, it made the process a little easier. This home has a lot of devices related to entertainment like TVs, gaming systems, and other Iot devices, with a couple of laptops as well as smartphones.

|  |  |  |
| --- | --- | --- |
| Device IP Address | Manufacturer | Description of Device |
| 10.0.0.1 | Technicolor CH USA | This is the network’s router |
| 10.0.0.157 | Samsung Electronics | This is one of the TVs in the network. |
| 10.0.0.179 | HP | The client’s work laptop |
| 10.0.0.79 | Arris Group | Apple smartphone |
| 10.0.0.162 | Amazon Technologies | Amazon TV |
| 10.0.0.194 | TPV Display Technology | Smart Tv |

# Port Scan Analysis – One Internal Device

Conducted a port scan of the Amazon TV, using Nmap. The following analysis describes the results.

A computer screen with white text

Description automatically generated

There are 3 open ports on the TV, 1080, 6543, and 8888. These are all necessary ports that should be open on a TV. 1080 is used for routing network traffic through a proxy server for extra security. Port 6543 is used to allow users to access and manage their DVR system through a web browser. Port 8888 is used for accessing technical documentation.

# Network and Port Scan Analysis – External

|  |
| --- |
| External scan – Conduct an IP address and port scan of the customer network from the internet. Scan their outside IP address and look for vulnerabilities. Look for open ports or other vulnerabilities from the outside. Does the customer have an external facing web server or public FTP server?  You can determine your outside IP address using a website like <https://ipchicken.com/>  You can use Nmap or Zenmap (or another scanning tool) from OUTSIDE the network you are trying to scan.  You can also use the <https://hackertarget.com/nmap-online-port-scanner/> as another scanner.  Summarize AND analyze the results in this section. Attach the scan results to this document as an exhibit. |

After doing an external Network scan of the public IP address using Nmap, I was able to find 6 open ports which are 22, 23, 80, 443, 8080, and 8181. While on most routers, port 80 and 443 will be open due to needing to communicate on the internet, ports 22 and 23 can be a big vulnerability. Ports 22 and 23 are used for remote access. Since my client doesn’t use any type of remote access services, there is no reason for these ports to be open. If exploited, a hacker can have control of the router remotely without even having to be there physically. Port 8181 is used by the ISP to monitor devices, connections, and network health. Port 8080 is used for a proxy server.

# A computer screen shot of a computer program Description automatically generated

# Wireless Range Analysis

The figure below shows the networks wireless range. The network Is accessible from other homes in the area. This is a vulnerability because the client’s wireless network should only be accessible to her, no one else. This can be a big problem if someone in the neighborhood has malicious intentions, they can attempt to access the network. To better mitigate this, the router should be positioned strategically so that no one except those in the home can access the network. Also, by disabling SSID broadcasting, this makes the network less accessible to those outside. The SSID does not reveal who the owners are.

A map with a red circle

Description automatically generated

Figure 1- Example map showing the range of the wireless network signal around the client's home

# Action Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Action Item | Priority  Low, Medium, High | Cost  None = $0  $ < $50  $$ < $50-250  $$$ < $250+ | Expertise  Low, Medium, High |
| 1 | Change Administrator Account password from default | High | $0 | Low |
| 2 | Upgrade to a newer router that uses WPA3 | High | <$100 | Medium |
| 3 | Change firewall setting for better security block unused ports and external traffic | High | $0 | Medium-High |
| 4 | Better secure social media accounts | Low | $0 | Low |
| 5 | Have the youngest daughter of client learn how to better manage passwords. | Medium | $0 | Medium |
| 6 | Create a disaster preparedness plan | High | $0 | Low |
| 7 | Change batteries for smoke/ carbon dioxide alarms and install one in the living room | High | <$100 | Low |
| 8 | Fix wireless range so only people in the clients home can access the network | Medium | $0 | Medium |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |

\*Add additional rows if needed