Security Analysis Report

Students applying cybersecurity skills to the real world

CAE in Cybersecurity Symposium - April 2024 - Louisville, KY

Professor Keith Nabozny - Macomb Community College

Contact Information

- Keith Nabozny
- Professor of Information Technology
- Macomb Community College
- Warren, Michigan
- naboznyk@macomb.edu

What is it?

- Security Analysis Report
  - Used since 2013
  - Revised and updated every semester
  - Customizable to your needs
  - Add or remove components to modify the difficulty
- Key sections of the report
  - Network and wireless security
  - System (PC or end device) security
  - Personal security
  - Data loss and disaster recovery
  - Physical security

Materials

- Files I can provide:
  - Word document templates for students
  - Partial example of completed report
  - Grading Rubric for final report
  - Send me an email!
  - naboznyk@macomb.edu

Assignments

- Canvas Assignments
  - SECA01 - Part 1 - Client Location and Description
  - SECA02 - Part 2 - Analyze Vulnerabilities
  - SECA03 - Part 3 - Rough Draft
  - SECA04 - Part 4 - Final Version

Typical Project Schedule

- 16-week semester
- Week 2 - SECA01 - Client and Location
  - Review and feedback to students by end of Week 3
- Week 4 - SECA02- Analyze Vulnerabilities
  - Review and feedback to students by end of Week 5
- Week 7 - SECA03 - Rough Draft
  - Review and feedback to students by end of Week 8
- Week 9 - SECA04 - Final Version assigned
  - Completed project due at end of Week 11
  - Graded by end of Week 12 or Week 13

SECA01-Security Analysis - Part 1 - Client and Location Description - v06

Published | Edit

Objective:

You will be working on the Security Analysis project over the next few weeks. This assignment requires you to select a client for the project. The purpose of this assignment is to describe your customer for the Security Analysis project.

The overall objective of the Security Analysis project is to give you experience with a scaled-down version of a vulnerability analysis report that would be requested by a client. The Security Analysis project will look for vulnerabilities related to Network and Wireless Security, System (PC and End Device) Security, Personal Security, Data Loss and Disaster Recovery, Physical Security, and also analyze the results from network and port scanning.

Preparations:

Download the assignment template document from this link: SECA01-Client and Location Info-v06.docx

Instructions: Instructions are included in the assignment template document provided.

Submission: Complete the assignment template document provided and submit it to this assignment before the due date and time.

Course	**ITIA 1310 - Certified Ethical Hacker**
Assignment	**SECA01 - Security Analysis – Client and Location Description**
Student Name	
Semester	

Objective:

The purpose of this assignment is to describe your customer for the Security Analysis project. Remember that this should be a REAL customer. This project will NOT be based on a made-up or fictional customer.

The customer can be:

- You and your household.
- The household of a friend or family member.
- A small business that you have a personal connection with.

The customer CANNOT be:

- A large business like General Motors or Ford. Even you or your family member works for them, it will not be a feasible client for this project.
- A small business that you have NO personal connection with. For example, the independent coffee shop near you will probably not work, because you will need to obtain permission from the owner/manager to work on the project.

Other important reminders:

- When choosing your client for this project, be sure they understand you will need to perform the following types of activities at their location and on their devices:
  - Allow you to connect your laptop to the wired and/or wireless network to perform network scans using software like Nmap/Zenmap.
  - Access devices at the location to view files and configurations. (For example: wireless router, cable modem, laptops, PCs, smartphones, or tablets).
  - Speak to personnel that can answer questions about the network, computers, and other items related to the project.
  - Take photographs and/or screenshots of computer screens (for example: screenshots of configuration settings) or physical security elements (for example: doors, locks, lighting, etc.) for documentation.
  - The customer and their property need to be regularly accessible for the next several weeks as you work on the project. For example, if they are leaving the country for vacation for a month, they are not a good choice.

Client Description

Who is your client?		
Residential or business?		
What is your relationship to the client?		
Are you certain you will have permission to complete all the tasks related to this project?		
Describe their high-level security concerns of your customer.		
Describe the number and types of users that are typically using the network on a regular basis.		
How many PCs, smartphones, tablets, or Internet of Things (approximately) do they have active on the network on a typical day?	Desktop PCs	
	Laptops	
	Smartphones	
	Tablets	
	IoT Devices	
Briefly describe your client's computer knowledge.		
Briefly describe how your client typically uses the network. (Work from home? Entertainment? Education?)		

Location Description

Describe the building. Is it a house, apartment, condo, warehouse, strip mall, or standalone building?	
Is it in a suburban, urban, rural, or commercial area? If you are not sure, you can review examples here: https://en.wikipedia.org/wiki/Developed_environments	
What is the approximate size of the building in square feet?	
How many floors?	
How close are other residences/businesses (approximately)?	

SECA02-Security Analysis - Part 2 - Analyze vulnerabilities

Published | Edit | ⋮

Objective:

This assignment is a continuation of the Security Analysis project. This purpose of this assignment is to analyze three potential vulnerabilities for your Security Analysis client and document them properly using a portion of the template that will be used for the rough draft and final versions of the Security Analysis.

The overall objective of the Security Analysis project is to give you experience with a scaled-down version of a vulnerability analysis report that would be requested by a client. The Security Analysis project will look for vulnerabilities related to Network and Wireless Security, System (PC and End Device) Security, Personal Security, Data Loss and Disaster Recovery, Physical Security, and also analyze the results from network and port scanning.

Preparations:

Below is a document containing examples of what completed vulnerability sections should like. Use this document as a reference. This PDF document also has embedded comments to provide additional explanation.

SECA02-EXAMPLE-Analyze vulnerabilities-commented-v04.pdf

Download the assignment template document from this link: SECA02-Analyze vulnerabilities-STUDENTS-v09.docx

Instructions: Instructions are included in the assignment template document provided.

Submission: Complete the assignment template document provided and submit it to this assignment before the due date and time.

Course	**ITIA-1310 – Certified Ethical Hacker**
Assignment	**SECA02 – Security Analysis – Part 2 - Analyze three vulnerabilities**
Student Name	
Semester	

Objectives:

This assignment is a continuation of the Security Analysis project. This purpose of this assignment is to analyze three potential vulnerabilities for your Security Analysis client and document them properly using a portion of the template that will be used for the rough draft and final versions of the Security Analysis.

Description:

Your final version of the Network Security Analysis will have about 20 different potential vulnerabilities analyzed. The purpose of this assignment is to have you analyze THREE potential vulnerabilities and document them correctly. This will give me an opportunity to give you feedback on THREE vulnerabilities, so that you have a good idea of what is expected for ALL of them.

Be sure to look at the example document posted in Canvas to get a better idea of what is expected in this assignment.

NOTE: DO NOT FIX ANY PROBLEMS OR VULNERABILITIES YOU FIND! Your role is only to IDENTIFY vulnerabilities, NOT to fix them. Unless they present a safety issue (like broken smoke alarms), vulnerabilities should be fixed AFTER you complete this project.

Briefly describe your customer for the Network Security Analysis

Residential or business?	
Geographic location (urban/suburban/rural)?	
Approximate number of users?	
Approximate number of devices?	
Types of devices?	

Descriptions of the vulnerability analysis subsections:

These are just descriptions and explanations. DO NOT COMPLETE THIS SECTION!

Explanation of Vulnerability – What vulnerability are you analyzing? Describe it so the customer understands it. Why is this a potential vulnerability? What problems could the customer encounter if this vulnerability is present or not remediated?

Examples/Observations – Did you find any examples of this problem? Whether the answer is yes or no, document WHAT you looked for and HOW you looked for it. Did you inspect a setting? Use a scanning tool?

Documentation - **YOU MUST DOCUMENT EACH OBSERVATION!** This can be a photograph or a screenshot or some other evidence that you checked this item out. In some cases, the interview information with the customer is appropriate. HOWEVER, in most cases, you need screenshots or photographs NOT just the word of the customer. Writing "N/A" is NEVER correct.

Screenshots of applications work much better than photographs of the screen. The Windows Snipping Tool (Win+Shift+S) works great. On a Mac, use Shift+Command+3. **Whenever possible, you should ALWAYS take a screenshot on a device like a PC, laptop, smartphone, or tablet.**

EVERY photo or screenshot should have a caption. In the caption, describe how the image documents the issue. **Note:** Word has a built-in caption function that will keep the caption with the image. To insert a caption, right-click the image and click **Insert Caption.**

Screenshot and caption example below:

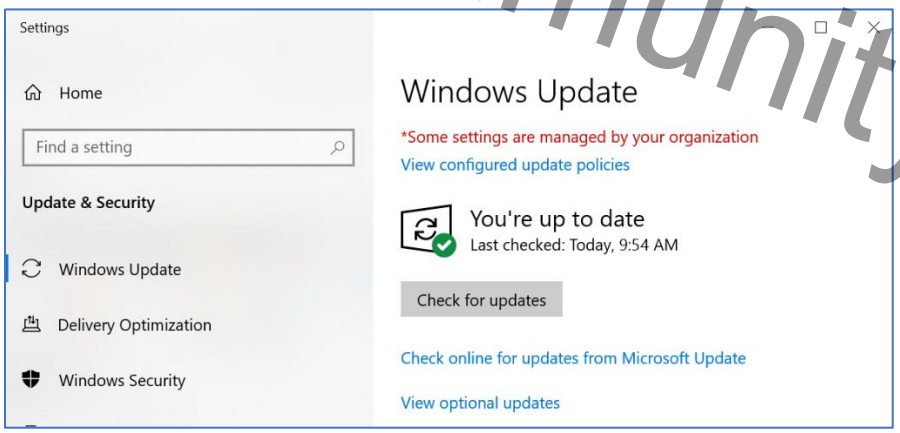

Figure 1- Windows Update on Dawn's laptop showing it is up-to-date

Risk Rating – Rate this risk on a scale of Low, Medium, or 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. In each case you should explain why this customer's risk was rated that way.

Recommendations – Does the customer need to remediate (correct) this vulnerability? If so, what do they need to do?

Item 1 - Network Security

Wireless authentication and encryption should be in use

Explanation of Potential Vulnerability

Explain the purpose of wireless authentication and encryption. Explain the difference between wireless authentication (like WPA2 or WPA3) and encryption (like AES). Explain the risk(s) of NOT having strong wireless authentication and encryption enabled correctly.

Describe why you are investigating this potential vulnerability. Generally, this should not be specific to your customer. Specific information about the vulnerability for your customer will be written in the Observations section.

Observations/Examples Found

{Describe observations related to or examples of this vulnerability found at the site}

This section is where you describe what you did to investigate this vulnerability. **You should be logging into the wireless router to investigate this.** Describe what you found. Focus ONLY on Authentication and Encryption. Other issues related to the router admin password or the router firmware, for example, will be covered in other sections. **DO NOT use the configuration on a smartphone or laptop to show what they are using to connect to the network.** Login to the wireless router and examine the configuration.

Documentation

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

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

- Recommendation 1
- Recommendation 2

Item 2 - System (PC or end device) security

Devices should be updated with current operating system versions/patches

Explanation of Potential Vulnerability

Explain the purpose of operating systems. Provide a couple examples of operating systems so the reader understands what you mean. Explain why updating/patching operating systems is important. Describe the risks in NOT updating operating systems to current versions or installing patches and service packs. Describe why you are investigating this potential vulnerability. The Explanation should be a GENERIC explanation about this vulnerability that could apply to almost any client. Generally, this should not be specific to your customer. Specific information about the vulnerability for your customer will be written in the Observations section.

Observations/Examples Found

- {Describe examples of this vulnerability found at the site}
- Perform this for TWO to FOUR devices at the site. At least one device should be a laptop or computer. The second device can be a smartphone or tablet.
- Which devices did you login to? What did you find out?

Documentation

YOU MUST DOCUMENT EACH OBSERVATION! This can be a photograph or a screenshot or some other evidence that you checked this item out. In some cases, the interview information with the customer is appropriate. HOWEVER, in most cases, you need screenshots or photographs NOT just the word of the customer. Writing “N/A” is NEVER correct.

Be specific and identify devices by name so it is clear which devices are OK or which devices have problems. Saying “Dave's Windows 10 Laptop” or “Sara's iPhone 14” are much clearer than just “one of the laptops” or “the client’s iPhone”.

FYI - Screenshots of applications work much better than photographs of the screen. The Windows Snipping Tool (Win+Shift+S) works great. On a Mac, use Shift+Command+3.

For example, you should use a screenshot of the Windows Update page or the

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

- {Provide a list of recommendations}

Item 3 - Physical Security

Exterior lighting and perimeter security (fencing) should be adequate

Explanation of Potential Vulnerability

Explain the potential vulnerability. Describe the risks if this vulnerability is present. Describe why you are investigating this potential vulnerability. The Explanation should be a GENERIC explanation about why exterior lighting and/or fencing is important that could apply to almost any client.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}
- What is the exterior lighting like?
- Is there a fence and is it secure?
- **Focus ONLY on exterior lighting and fencing (if applicable) in this section. Other sections will address doors and locks, alarm systems, or security cameras.**

Documentation

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

For example, use photos of the outside of the building at night to show how well or poorly the lighting is illuminating the exterior.

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

- {Provide a list of recommendations}.

ITIA-1310 - Certified Ethical Hacker
SECA02 - Network Security Analysis – Part 2 - Analyze vulnerabilities - EXAMPLE

Description:

Your final version of the Network Security Analysis will have about 20 different potential vulnerabilities analyzed. This example shows you an analysis of the same potential vulnerability in one situation where it is a problem, and in another situation where it is not.

Briefly describe the customer for the Network Security Analysis

Business or residential?	Residential
Geographic location (urban/suburban/rural)?	Suburb (Warren, MI)
Approximate number of users?	4
Approximate number of devices?	12
Types of devices?	Three laptops, one PC, four smartphones, and one tablet.

EXAMPLE 1 - Network Security – Not a problem

Wireless authentication and encryption should be in use

Explanation of Potential Vulnerability

Wireless authentication proves your identity to the wireless router. Without authentication anyone can connect to your wireless network using your Service-Set-Identifier (SSID) that is broadcasted. Encryption scrambles your data so that it cannot be read. If someone is close enough to the signal, such as a neighbor, without encryption someone can intercept and read all the data in the air passing from your device to the wireless router. If you are entering sensitive information such as passwords to login to sensitive work accounts, school accounts, bank information, sending emails, or accessing health care information, someone can capture that data and read it without encryption.

Observations/Examples Found

Logged into the wireless router's administration page and confirmed the customer is using WPA2-PSK with AES.

Documentation

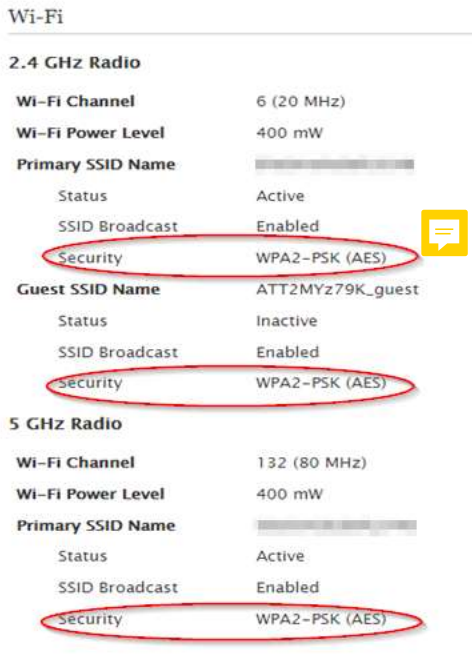

Figure 1- Router configuration page showing WPA2-PSK with AES

Risk Rating

The risk rating for this vulnerability is Low. The customer is using WPA2-PSK with AES. The network is restricted to those who can authenticate to the wireless router using a pre-shared key and strong encryption is implemented. Even if a neighbor were to sniff the packets the traffic would be encrypted and not easily readable.

Recommendations

- The customer is already using the most secure option on the wireless router. No recommendations at this time.

EXAMPLE 2 - Network Security – A potential problem

Wireless authentication and encryption should be in use

Explanation of Potential Vulnerability

Wireless authentication proves your identity to the wireless router. Without authentication anyone can connect to your wireless network using your Service-Set-Identifier (SSID) that is broadcasted. Encryption scrambles your data so that it cannot be read. If someone is close enough to the signal, such as a neighbor, without encryption someone can intercept and read all the data in the air passing from your device to the wireless router. If you are entering sensitive information such as passwords to login to sensitive work accounts, school accounts, bank information, sending emails, or accessing health care information, someone can capture that data and read it without encryption.

Observations/Examples Found

Logged into the wireless router's administration page and determined the customer is using WPA-PSK with TKIP, which is not the best security available.

Documentation

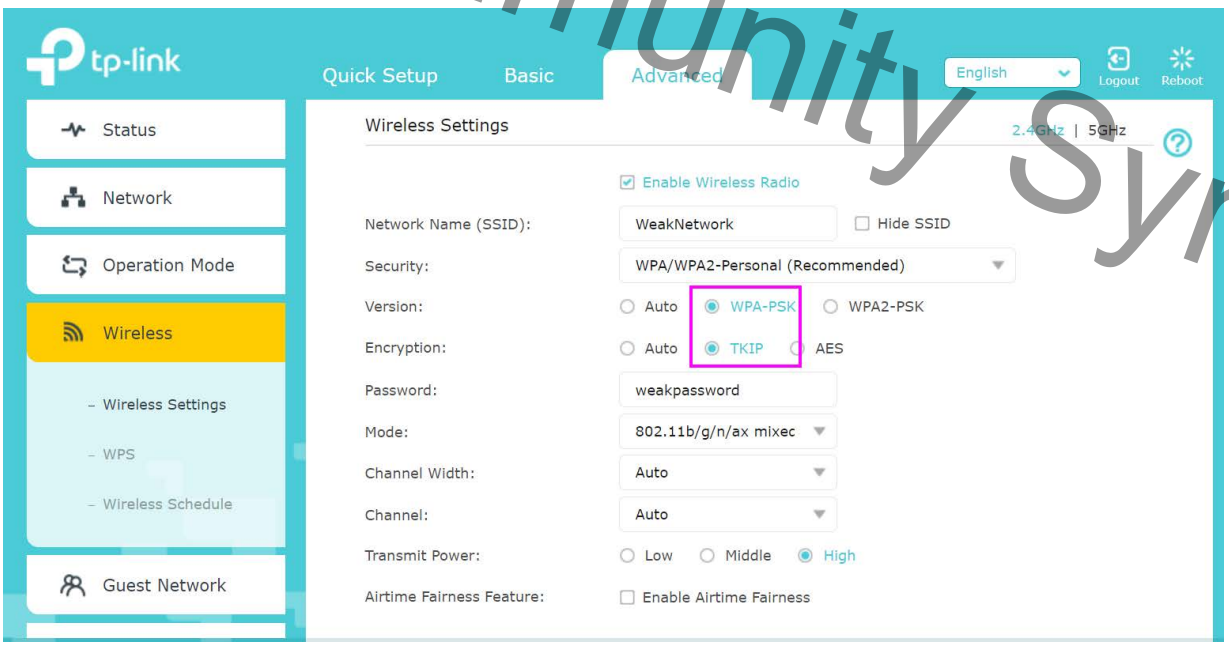

Figure 2 - Router configuration showing WPA-PSK with TKIP

Risk Rating

The risk rating for this vulnerability is High. The customer is using WPA-PSK with TKIP. This is better than using WEP, but WPA with TKIP is potentially vulnerable to attacks. (The password to the network is also weak, but that will be covered in a different section of the report.)

Recommendations

The customer should change the router configuration to use WPA2-PSK with AES encryption. The customer should not use Auto, because devices using WPA could force the router to communicate with the weaker security. The customer should consider upgrading to a router with WPA3 in the future.

SECA03-Security Analysis - Part 3 - Rough Draft

Published | Edit | ⋮

Objective:

This assignment is a continuation of the Security Analysis project. This purpose of this assignment is to begin using the Security Analysis template document that you will submit for the final version of the assignment (SECA04).

The overall objective of the Security Analysis project is to give you experience with a scaled-down version of a vulnerability analysis report that would be requested by a client. The Security Analysis project will look for vulnerabilities related to Network and Wireless Security, System (PC and End Device) Security, Personal Security, Data Loss and Disaster Recovery, Physical Security, and also analyze the results from network and port scanning.

Preparations:

Download the assignment template document from this link:

SECA03-Security-Analysis-Template-v38.docx

Instructions:

For this rough draft, complete the following sections:

1. **Site Activities Schedule** - This is a short diary of what tasks you completed at the customer location and when. You will update this as you work on the project.
2. **Background Information** - This section includes descriptions of the people at the site and the building/location. It also includes a photo of the outside of the building.
3. **Devices in Scope** - This section summarizes information about the devices you will be investigating.
4. Complete the subsections for **ONE potential or actual vulnerability** under ***EACH*** section for this rough draft. This is building on what you learned with the SECA02 assignment. You can reuse the information you used in SECA02 for this assignment, but you also need to work on the new sections, as well.
   - Complete one vulnerability in each of the following main sections:
     - Network and Wireless Security
     - System (PC or End Device) Security
     - Personal Security
     - Data Loss and Disaster Recovery
     - Physical Security
   - For each potential or actual vulnerability you write about in the main sections, complete ALL the subsections for each vulnerability.
     - Explanation of Vulnerability
     - Observations/Examples
     - Documentation
     - Risk Rating
     - Recommendations

When you are done, you should have completed all the subsections for **ONE** potential/actual vulnerability in EVERY main section.

WARNINGS

- DO NOT create your own template document! Use the template document provided here.
- DO NOT delete sections of the template document! You will continue to update THIS document as you make progress towards the final version.
- DO NOT write about more than one potential vulnerability in each section for this rough draft!

Submission: Complete the assignment template document provided and submit it to this assignment before the due date and time.

Created by Keith A. Watson, CISSP on March 1, 2005

Last revised and updated by Keith Nabozny, CISSP on March 26, 2023

CLIENT ORG or CUSTOMER NAME

Security Analysis Report

March 11, 2024

Report Prepared by:

YOUR NAME

YOUR EMAIL ADDRESS

ITIA-1310

Certified Ethical Hacker

Semester

The information contained within this report is considered proprietary and confidential to the {CLIENT ORGANIZATION}. Inappropriate and unauthorized disclosure of this report or portions of it could result in significant damage or loss to the {CLIENT ORGANIZATION}. 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

****NOTE** These yellow boxes are information for YOU, the author of the document. They should be deleted before the final draft and submission to the customer. DO NOT WRITE IN THE YELLOW BOXES!**

Briefly describe the activities of the assessment.

Talk about the importance of information security at the client organization.

What are some key findings from the analysis?

What are some things the organization is doing well?

What are some high-level issues they need to improve upon? For example, what are the "top five" findings, or vulnerabilities discovered during the site security assessment?

EXAMPLE – A security analysis was conducted for the Magical Treehouse Corporation between February 1 and March 15, 2020. Major activities conducted included Troll Defensive Perimeter inspection, interviews with key network elves and an analysis of scroll retention procedures. The primary business of the Magical Treehouse is making delicious treats and snacks for magical and non-magical folk. Consequently, their secret recipes are important to their business success now and into the future. Protecting those secret recipes should be a primary goal of their security.

Project Scope

The scope is the boundaries of the project. It is used to describe the on-site activities. These are good starting points, but feel free to modify them based on what you agreed to with your customer.

In Scope

The following activities are within the scope of this project:

- Interviews with key elves in charge of policy, administration, day-to-day operations, magic enforcement, network management, and dragon management.
- A Visual Walk Through of the Magical Treehouse facilities, offices and Root sectors with administrative and facilities personnel to assess physical security.
- A series of Magical Scans to discover known and potentially unknown devices on the network. (These Scans will be conducted from within the Magical Treehouse perimeter and from the Dark Forest.)
- A configuration and security assessment of at most five key systems at each center.

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

List the site activities. This section should be highlights of what you did at the customer site, like scanning for network devices, reviewing PC configurations or checking on smoke alarms. These entries should be about what was accomplished on each date, NOT which sections of the report you completed. It does not need to be detailed. They should be brief descriptions, not paragraphs describing everything you did in detail.

Date – xx/xx/xx

Brief description of tasks executed on the above date.

Date – xx/xx/xx

Brief description of tasks executed on the above date.

Date – xx/xx/xx

Brief description of tasks executed on the above date.

Date – xx/xx/xx

Brief description of tasks executed on the above date.

Background Information

Client Description

****NOTE** These yellow boxes are information for YOU, the author of the document. They should be deleted before the final draft and submission to the customer. DO NOT WRITE IN THE YELLOW BOXES!**

Describe the client for this project in a PARAGRAPH. This should NOT just be answers to the questions below.

Who is your client?

Business or residential?

Describe their high-level security concerns

How many users are typically on the network?

What types of users are there? (Children, teenagers, adults?)

What is their computer knowledge/background?

Describe how they typically use the network (work, entertainment, education).

Enter a paragraph describing your client based on the question prompts above. Do not just answer the questions above or list bullet points.

Location Description

Describe the location and the building in a PARAGRAPH. This should NOT just be answers to the questions below.

Is it suburban, urban, rural, or commercial? (If you are not sure, you can review examples here: https://en.wikipedia.org/wiki/Developed_environments

Is it a house, apartment, condo, warehouse, strip mall or standalone building?

What is the approximate size of the building?

How many floors?

How many bedrooms?

Is there a basement?

How close are other residences/businesses?

Include a photo of the outside of the building.

Enter a paragraph describing your client's location using the question prompts above. Do not just answer the questions above or list bullet points. Also, include a photo of the outside of the building.

Devices in Scope

Device Type	**Device name** **(Or commonly used name)**	**Operating System and version**	**Primary User**	**Description** **(Manufacturer, model number, etc.)**
Laptop	Pikachu	Mac OS Z	Nuria	MacBook Old
Smartphone	Nuria's iPhone	iPhone iOS 99	Mariana	iPhone 32 XL
Wireless Router	magic-rtr01	{Firmware of router}	All	Linksys WRT54G

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.

Have the orders for network elves been modified? (EXAMPLE)

Explanation of Vulnerability

The purpose of network elves is to protect the network using tiny swords and flying around in a defensive manner. Based on instructions from the Elf Lord, they determine which network traffic to permit or deny.

If the orders for the network elves have been modified incorrectly, they could allow critters into the Magical Treehouse that could cause inordinate damage.

There are several risks in running network services without network elves.

- Incoming network-based scans and attacks are not easily detected or prevented.
- Attackers target vulnerable network services.
- Attacks are not isolated and damage cannot be contained.
- Network probing for vulnerabilities slows system and network performance.

Observations/Examples Found

- The orders of the network elves were modified by a previous network elf admin, Snowbloom, to allow chipmunks and squirrels into the Magical Treehouse. At one time, chipmunks and squirrels were permitted into the Magical Treehouse for a special project, but that special project ended 18 months ago.

Documentation

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

Risk Rating – High – The elves live in a high traffic forest with many evil magical beasts wandering through. Network elves with incorrect instructions could be catastrophic for the Magical Treehouse.

Recommendations

- The network elf orders should be updated again to prevent the entry of squirrels and chipmunks.
- Install a new hardware-based network elf.

Strong wireless authentication and encryption should be in use (REQUIRED)

Explanation

Explain the purpose of wireless authentication and encryption. Explain the difference between wireless authentication (like WPA2 or WPA3) and encryption (like AES). Explain the risk(s) of NOT having strong wireless authentication and encryption enabled correctly.

Observations/Examples Found

{Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

Example: Login to the wireless router and look at the **router administration page** for security. What security and authentication are configured on the wireless router? (NOTE: You should be looking at what is configured on the ROUTER, not how the client is connecting to the network.)

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

- Recommendation 1
- Recommendation 2

The password to access the wireless network should be strong (REQUIRED)

Explanation of Vulnerability

Explain the purpose of the wireless network password. What are the risks if the wireless network password is weak? What can happen if unauthorized users connect to the wireless network?

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}
- How long is the wireless network password? Obscure or redact the personal information in the image. I do not need to see the
- Describe the password with the following mask (x=letters, #=numbers, $=special characters – example: Fish123! = Xxxx###$)

Documentation

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

Example: Login to the wireless router and look at the **router administration page** for security. Confirm the passwords used for the wireless networks.

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

- {Provide a list of recommendations}.

The router administrator password should be changed from the default setting (REQUIRED)

Explanation of Vulnerability

Explain the purpose of the router administrator ID and password. Describe the risk(s) of NOT changing the router administrator password from the default settings.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

Example: Login to the wireless router and look at the **router administration page** for security. Investigate if the router admin password has been changed to something strong.

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

- {Provide a list of recommendations}.

The firewall in the wireless router should not permit external traffic (OPTIONAL)

Explanation of Vulnerability

Explain the purpose of the firewall that is built into the wireless router. Describe the risks if the firewall has been modified to permit to permit external traffic.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

Example: Login to the wireless router and look at the **router administration page** for security. Check to see if any firewall rules have been modified to permit access to the inside network from the internet.

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

- {Provide a list of recommendations}.

The wireless router firmware should be current (OPTIONAL)

Explanation of Vulnerability

Explain the purpose of the wireless router firmware. Describe the potential risks if the router firmware is out of date.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

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

- {Provide a list of recommendations}.

System (PC or end device) Security

Describe the state of system security at the client organization. This includes analyses of PCs, servers, laptops, mobile devices, and other end-user devices.

Include a screen capture or photograph to document any particularly bad problems as evidence.

There should be a minimum of **TWO** potential vulnerabilities analyzed.

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? (EXAMPLE)

Explanation of Vulnerability

Since users have privileged access to their workstations, they are free to install doughnuts with sprinkles that can affect the operations of the computers at the Magical Treehouse. Doughnuts are freely available from the Internet. Doughnuts with sprinkles can impede the productivity of the staff, collect information on the users, the Magical Treehouse Company, the network environment, launch attacks or probe internal systems.

There are several risks in allowing users to install unsafe doughnuts.

- The doughnuts may contain a virus, worm, or some other dangerous electronic threat.
- The doughnuts may be a “Trojan Horse” to fool users.
- The doughnuts may capture, disclose, delete, or modify sensitive data.
- The doughnuts may make the network elves fat and lazy and unable to perform their duties effectively.
- Significant time may be wasted discussing which doughnuts to eat first.

Observations/Examples Found

Doughnuts were found in the Snowbloom PC, Oakleaf Workstation and Raindrop Laptop.

Documentation

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

Risk Rating

High – Users love free doughnuts and doughnuts can easily hide magical spells that can impede the productivity of the Magical Treehouse.

Recommendations

The operations team should

- Remove doughnut credit cards from the network elves.
- Remove unsafe doughnuts that have already been installed from workstations. Reinstall systems as needed.
- Establish a process for the evaluation and installation of new doughnuts.

Are end user devices updated with current operating system versions/patches? (REQUIRED)

Explanation of Vulnerability

Explain the purpose of operating systems. Explain why updating/patching operating systems is important. Describe the risks in NOT updating operating systems to current versions or installing patches and service packs.

Observations/Examples Found

- {Describe examples of this vulnerability found at the site}
- Perform this for TWO to FOUR devices at the site. At least one device should be a laptop or computer. The second device can be a smartphone or tablet.

Documentation

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

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

- {Provide a list of recommendations}

Are PCs and Laptops protected by antivirus and antimalware software? (REQUIRED)

Explanation of Vulnerability

Explain the purpose of antivirus and antimalware software. Describe the risks of a device NOT having antivirus and antimalware software installed.

Observations/Examples Found

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

Documentation

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

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

- {Provide a list of recommendations}

Personal Security

Describe the state of Personal Security at the client organization.

Include screen captures and/or photographs to document each vulnerability analyzed.

For devices (like PCs and smartphones) you should definitely have screenshots showing that the devices are locked and require a passcode or biometric to be unlocked.

For email and banking passwords, you can document the interviews with customers about the topic. (For example: Who did you talk to? When did you talk to them? Which accounts were discussed?)

A minimum of **TWO** potential vulnerabilities should be analyzed.

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

Explain the vulnerability. Describe the risks if this vulnerability is present.

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.)**
*Add more rows or columns as needed			

Documentation

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

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

- {Provide a list of recommendations}

Are strong passwords used for email and banking accounts? (REQUIRED)

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

- Interviewed Snowbloom on Tuesday Feb 30, banking password is less than 10 characters.

Documentation

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

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

- {Provide a list of recommendations}

Social Media accounts are secure (OPTIONAL example: Is Facebook profile private?)

Explanation of Vulnerability

Explain the vulnerability. Describe the risks if this vulnerability is present.

Observations/Examples Found

{Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

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

- {Provide a list of recommendations}.

The clients understand how to manage passwords securely (OPTIONAL)

Explanation of Vulnerability

Explain the vulnerability. Describe the risks if this vulnerability is present.

vulnerability is NOT present, then say the customer is at Low Risk and explain why.

Observations/Examples Found

{Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

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

- {Provide a list of recommendations}.

Data Loss Prevention and Disaster Recovery

Describe the state of data loss prevention and disaster recovery at the client organization. How resilient is the customer to losing data or their equipment and property?

Include screen captures and/or photographs to document each vulnerability analyzed.

A minimum of **TWO** potential vulnerabilities should be analyzed.

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? (REQUIRED)

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
*Add more rows or columns as needed			

Documentation

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

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

- Recommendation 1
- Recommendation 2
- Recommendation 3

Is there a disaster recovery plan or disaster preparedness plan? (REQUIRED)

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.

NOTE! This section is NOT about backing up data. This section is about recovering the operations. For example, if this is a business and the building burns down or floods, how does the business get back into operation? If this is a personal residence and there is a flood or tornado, where will the family go? Are they prepared for an evacuation?

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

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

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

Names of clients being interviewed	
Date and Time of Interview	

Does the customer have children living at home?	
Are there pets that would need to be transported in an evacuation situation? Do they have/need pet carriers?	
Does the client require important prescription medications? (Example: Insulin or other medications that would be difficult to acquire in an emergency.)	
Does the client require important documents that could be difficult to replace? (Example: Passports, visas, birth certificates.)	
Other	
Other	

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

- {Provide a list of recommendations}.

NOTE: If the customer does not have a disaster recovery plan (and most people do not) then your recommendations should be specific to this customer. What are significant concerns they should address? Do they have kids? Do they have pets? Do they have special medical requirements or medications to be concerned about?

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

Plan for children	
Plan for pets	
Plan for medication	
Plan for documents	
Other	
Other	

Is there adequate insurance for the building and/or contents? (OPTIONAL)

Explanation of Vulnerability

Explain the vulnerability. Describe the risks if this vulnerability is present.

Observations/Examples Found

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

Documentation

NOTE! If you choose this vulnerability for examination, then you **MUST** show a redacted copy of the declarations page for the home. You cannot just state "The customer has insurance."

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

- {Provide a list of recommendations}

Physical Security

Describe the state of physical security at the client organization.

Specifically, list the building, security perimeter, and server room (if applicable) vulnerabilities.

Include a screen capture or photograph to document any particularly bad problems as evidence.

There should be a minimum of **THREE** potential vulnerabilities analyzed.

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.

The Rainbow Bridge to the Magical Treehouse is frequently unguarded (EXAMPLE)

Explanation of Vulnerability

There are several important entry points to the Magical Treehouse. The Rainbow Bridge is the primary access to the tree. The Squirrel Defense Force is responsible for guarding the Rainbow Bridge, but they are frequently distracted by acorns and walnuts in the area. This bridge protects the valuable treasure of the Magical Treehouse. A determined attacker, thief, or disgruntled employee could get across the bridge with minimal effort to steal and/or destroy treasure or magical scrolls.

Observations/Examples Found

On the first day of the security analysis, members of the SDF were observed chasing each other and burying acorns instead of guarding the bridge. Analysis of security camera footage shows that this is happens on a regular basis.

Documentation

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

Risk Rating

High – The bridge is the primary entry point into the Treehouse. If it is unguarded the Treehouse can be easily compromised.

Recommendations

- Replace the rope bridge with a drawbridge.
- Replace the Squirrel Defense Force with a more reliable security team.

-

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?
Galadriel's Bedroom		
Elrond's Bedroom		
Bilbo's Bedroom		
Hallway		
Living Room		
Basement		
*Add more rows as needed		

Documentation

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

NOTE: When taking photos of smoke alarms or carbon monoxide detectors it should be clear in which room they are located. Extreme close ups of smoke alarms are not useful.

Risk Rating

High – There are an insufficient number of smoke alarms and carbon monoxide detectors. The residents of the home could die from smoke inhalation or fire or from carbon monoxide poisoning if not alerted in time.

Low - There are sufficient smoke alarms and carbon monoxide detectors.

Recommendations

- Install additional smoke alarms in the following areas:
- Install new batteries in the following smoke alarms and carbon monoxide detectors:
- Replace the smoke alarms and carbon monoxide detectors every 10 years.

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

Explanation of Vulnerability

Explain the vulnerability. Describe the risks if this vulnerability is present.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Room	Description of lock(s)	Are the locks functioning properly?
Front Door	Doorknob lock /Deadbolt/Keypad	
Side Door		
Back Door		

Garage – Overhead door (vehicles)		
Garage – Service door (people) - Exterior		
Garage – Service door (people) - Interior		
*Add more rows as needed		

Documentation

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

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

- {Provide a list of recommendations}.

Is exterior lighting and perimeter security adequate? (REQUIRED)

Explanation of Vulnerability

Explain the vulnerability. Describe the risks if this vulnerability is present.

Observations/Examples Found

- {Describe observations related to or examples of this vulnerability found at the site}

Documentation

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

NOTE: A photo of the outside of the premises at night showing how good/poor the lighting illuminates is very useful.

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

- {Provide a list of recommendations}.

Network Scan – Internal

Internal scan - Conduct an IP address scan (like a ping sweep) of the entire internal network using an application like Nmap or Zenmap. Summarize and ANALYZE the results here.

Can you recognize and identify all the devices? Are there any unknown devices? If so, you should investigate them.

Attach the detailed results of the scans to this document as exhibits. DO NOT use screenshots! Send the scans to a text file and attach the text file at the end of the report.

REMINDER – You can send Nmap results to a text file with the -oN and --append-output commands.

EXAMPLE: Performed a scan of the internal network using <state the application here>. The following is a summary and analysis of the key results. The results of the scan are below. (The text output from Nmap or a screenshot from the application should be included with the analysis. DO NOT EMBED FILES INTO THIS DOCUMENT. The output, whether it is text or a screenshot, should be readable in this report.)

In the following table, identify ALL the devices in the Scope of Analysis and the information found by Nmap. If more than 5 devices are detected in the Nmap scan, you only need to document 5 total devices in the table below.

Include a brief analysis of your discovery process. Were there any unknown devices that needed additional investigation? What did you do to track them down? Did you discover all the devices that you expected?

Device IP Address	Manufacturer	Description of Device

Port Scan Analysis – One Internal Device

Port scan – Select ONE internal device (like a PC, laptop, or server) for more analysis.

DO NOT scan the wireless router or cable/DSL modem for this section.

Perform a PORT SCAN of the device, summarize the results, and ANALYZE the results here.

What ports are open? Should they be open? Are there any ports that are unusual or unknown to you?

Attach the detailed results of the scans to this document as exhibits, if the scan is too long to reasonably include in this section.

EXAMPLE: Conducted a port scan of <DEVICE NAME>scans of the network using <state the application here>. The following analysis describes the results.

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.

Wireless Range Analysis

Wireless Range Analysis – Using a laptop or other portable wireless device, conduct a wireless range analysis in and around the customer premises. Look for unknown (rogue) wireless devices AND determine the limits of the customer's wireless network.

Provide a map that shows the approximate boundary of the customer's wireless network.

Remember to analyze the results. Consider the following question prompts:

- Is the customer's wireless network visible and accessible from other homes/businesses in the area?
- What does this mean to the customer?
- What should they do to make sure their wireless network is secure from outsiders?
- Does the SSID name reveal who the owners of the wireless network are?

Summarize the results in this section. Attach the scan results to this document as an exhibit. **NOTE: You should NOT just answer the questions above.** This should be written in paragraph form. The question prompts are provided to get you started.

If you want to try something fancy, you can try this application:

https://www.netspotapp.com/

EXAMPLE: The following is an example of what the Wireless Range Map could look like:

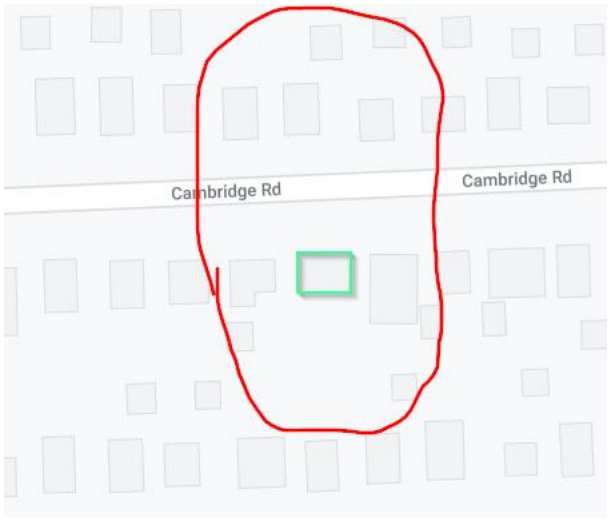

Figure 1- Example map showing the range of the wireless network signal around the client's home

Action Plan

Provide an action plan that that prioritizes the remediation of potential or actual vulnerabilities above to improve security at the client organization. You have given specific recommendations under each vulnerability, so use this as an opportunity for some high-level recommendations covering the analysis. Help the customer prioritize. Which items are cheapest to complete? Which can they do themselves? Which would need a professional?

	Action Item	Priority Low, Medium, High	Cost None = $0 $ < $50 $$ < $50-250 $$$ < $250+	Expertise Low, Medium, High
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				

*Add additional rows if needed

SECA04-Security Analysis - Part 4 - Final Version

Published | Edit

Objective:

This assignment is a continuation of the Security Analysis project. This purpose of this assignment is to complete the Security Analysis template document that you started working on in SECA03.

The overall objective of the Security Analysis project is to give you experience with a scaled-down version of a vulnerability analysis report that would be requested by a client. The Security Analysis project will look for vulnerabilities related to Network and Wireless Security, System (PC and End Device) Security, Personal Security, Data Loss and Disaster Recovery, Physical Security, and also analyze the results from network and port scanning.

Preparations:

You should be updating and finalizing the document you created for the SECA03 assignment.

Instructions:

For this final version, complete ALL the sections in the Security Analysis template document, per instructions provided in the document, in class, or through supplemental materials provided.

Submission: Complete the assignment template document provided and submit it to this assignment before the due date and time.

BEFORE submitting your final version of the Security Analysis, you should review the grading rubric below and use it as a checklist to make sure that you have not missed anything significant in the project.