Final VAPT Report Template

PREPARED BY: <Joshua Camara >

Submitted To: <Tech Shield>

Submission Date: <4/29/25>

__Sensitive__: The information in this document is strictly confidential and is intended for <Tech Shield>

TABLE OF CONTENTS

EXECUTIVE SUMMARY

A security assessment of the internal corporate network of **Tech Shield** on **4/25/25**. A Vulnerability Assessment and Penetration Test (VAPT) was conducted on the target environment to identify weaknesses that could be exploited by malicious actors. The objective was to assess the security posture of the systems and provide actionable recommendations to mitigate risk and strengthen defenses.The Greenbone vulnerability scan revealed several critical findings, notably the detection of a **backdoor** (score: 10.0) and the use of the **rexec service** (also score: 10.0). These findings represent immediate **system compromise risks** that need to be remediated with high priority. The **TCP timestamps** vulnerability, while low severity (score: 2.6), and the **XSS flaw** require attention to harden the system further.

The immediate focus should be on **remediating critical vulnerabilities** such as the **backdoor** and **rexec service** to prevent unauthorized access. Long-term actions, such as the implementation of **MFA** and **continuous security monitoring**, will help ensure that the system remains secure and resilient against future attacks.

CRITICAL	HIGH	MEDIUM	LOW
1	2	2	1

The highest severity vulnerabilities identified during the assessment give potential attackers the opportunity to gain persistent unauthorized access to the affected systems. The presence of a **backdoor** allows remote attackers to execute arbitrary commands with application-level or potentially system-level privileges, resulting in full compromise of the host. Additionally, the use of an **end-of-life operating system** exposes the environment to numerous publicly known exploits for which no vendor patches are available, significantly increasing the risk of remote code execution or privilege escalation. The enabled **rexec service**, which transmits credentials in plaintext, can be exploited for credential theft and lateral movement within the network. Furthermore, the **cross-site scripting (XSS) vulnerability** allows attackers to inject malicious scripts into web applications, potentially hijacking user sessions or stealing sensitive data through the browser. These combined issues pose a direct threat to data confidentiality, integrity, and availability across the environment. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

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

<Strength Category>

- **Patch Management**: The system has been maintained with **current patches**, and there are **no missing critical patches** for core services. This indicates proactive system management and reduces the risk of known vulnerabilities being exploited.

- **Firewall Configuration**: The system has a **properly configured firewall**, blocking unauthorized inbound and outbound traffic. This is a key defense mechanism, minimizing exposure to external threats.

- **SSH Configuration**: The system is configured with **SSH v2**, ensuring secure, encrypted remote access. Root login has been disabled, which prevents unauthorized administrative access.

- **No Exposed Critical Services**: Services like **FTP** and **Telnet**, which have known vulnerabilities, are **not exposed externally**, ensuring that attack surfaces are minimized.

Areas for Improvement

We recommend <Tech Shield> 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 Tech Shield’s information systems and/or reduce the impact of a successful attack.

Backdoor Detected (Score: 10.0):

Issue: A **backdoor** was identified on the system that allows an attacker to execute arbitrary commands in the context of the affected application. This poses a **critical risk** to the system's integrity and confidentiality.

- **Risk**: The backdoor could lead to full **system compromise**, data loss, or unauthorized access to sensitive information.

Rexec Service Enabled (Score: 10.0):

- **Issue**: The **rexec service**, an outdated and insecure remote execution service, is enabled on the system.
- **Risk**: This service is known to have security vulnerabilities and can be exploited to gain unauthorized access to the system, potentially leading to full compromise.

TCP Timestamps (Score: 2.6):

- **Issue**: TCP timestamps are enabled, which can potentially leak the **uptime** information of the system.
- **Risk**: While this is a **low severity** issue, attackers can use this information for **network reconnaissance**, or to identify systems running for extended periods and correlate that with other vulnerabilities.

Cross-Site Scripting (XSS) Flaw:

- **Issue**: The system is vulnerable to **XSS attacks** due to improper input sanitization.
- **Risk**: Malicious scripts could be injected by attackers, leading to session hijacking, unauthorized data access, or exploitation of web application users.

Short Term Recommendations

We recommend **Tech Shield** take the following actions as soon as possible to minimize business risk.

Backdoor Cleanup:

- **Action**: Perform a full **system cleanup** to remove the backdoor. Ensure that no other unauthorized access points remain on the system.
- **Rationale**: This is an **immediate priority** to prevent further compromise. Without addressing this, the system remains at high risk of exploitation.

Disable or Replace Rexec Service:

- **Action**: **Disable the rexec service** or replace it with a more secure remote access service like **SSH**.
- **Rationale**: The rexec service is outdated and inherently insecure. Replacing it with SSH ensures that communication is **encrypted** and authenticated, protecting against unauthorized access.

Disable TCP Timestamps:

- **Action**: Disable **TCP timestamps** to eliminate the potential leakage of system uptime data.

- **Rationale**: While not a high-risk vulnerability, it is a **minor security flaw** that can be easily mitigated to reduce exposure.

Fix XSS Flaw:

- **Action**: Implement proper **input sanitization** and **validation** for all user inputs.
- **Rationale**: Proper input sanitization is critical to **mitigating XSS attacks** and preventing the execution of malicious scripts.

Long Term Recommendations

We recommend the following actions be taken over the next 6 months to a year: fix hard-to-remediate issues that do not pose an urgent risk to the business. **Continuous Security Monitoring**:

- **Action**: Implement **continuous vulnerability scanning** and **real-time monitoring** to detect new vulnerabilities or suspicious activity early.
- **Rationale**: This will help detect and address vulnerabilities proactively, preventing future exploits.

Multi-Factor Authentication (MFA):

- **Action**: Implement **MFA** for all remote access points (e.g., SSH) and critical internal applications.
- **Rationale**: MFA adds an additional layer of security, making it much more difficult for attackers to compromise accounts or systems even if credentials are compromised.

Regular Security Audits:

- **Action**: Conduct **quarterly security audits** and vulnerability assessments to ensure that any new threats are identified and mitigated promptly.

- **Rationale**: Regular audits will help identify vulnerabilities in a timely manner and keep the system up-to-date with the latest security best practices.

Enforce Stronger Access Controls:

- **Action**: Review access controls to enforce **least privilege** principles across the system.
- **Rationale**: Reducing the number of users with elevated privileges helps limit the impact of potential attacks.

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

TESTING METHODOLOGY

<TEAM NAME GOES HERE>'s testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about **Tech Shields's** network systems. <TEAM NAME GOES HERE> used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. <TEAM NAME GOES HERE> simulated an attacker exploiting vulnerabilities in the **Tech Shields's** network. <TEAM NAME GOES HERE> gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

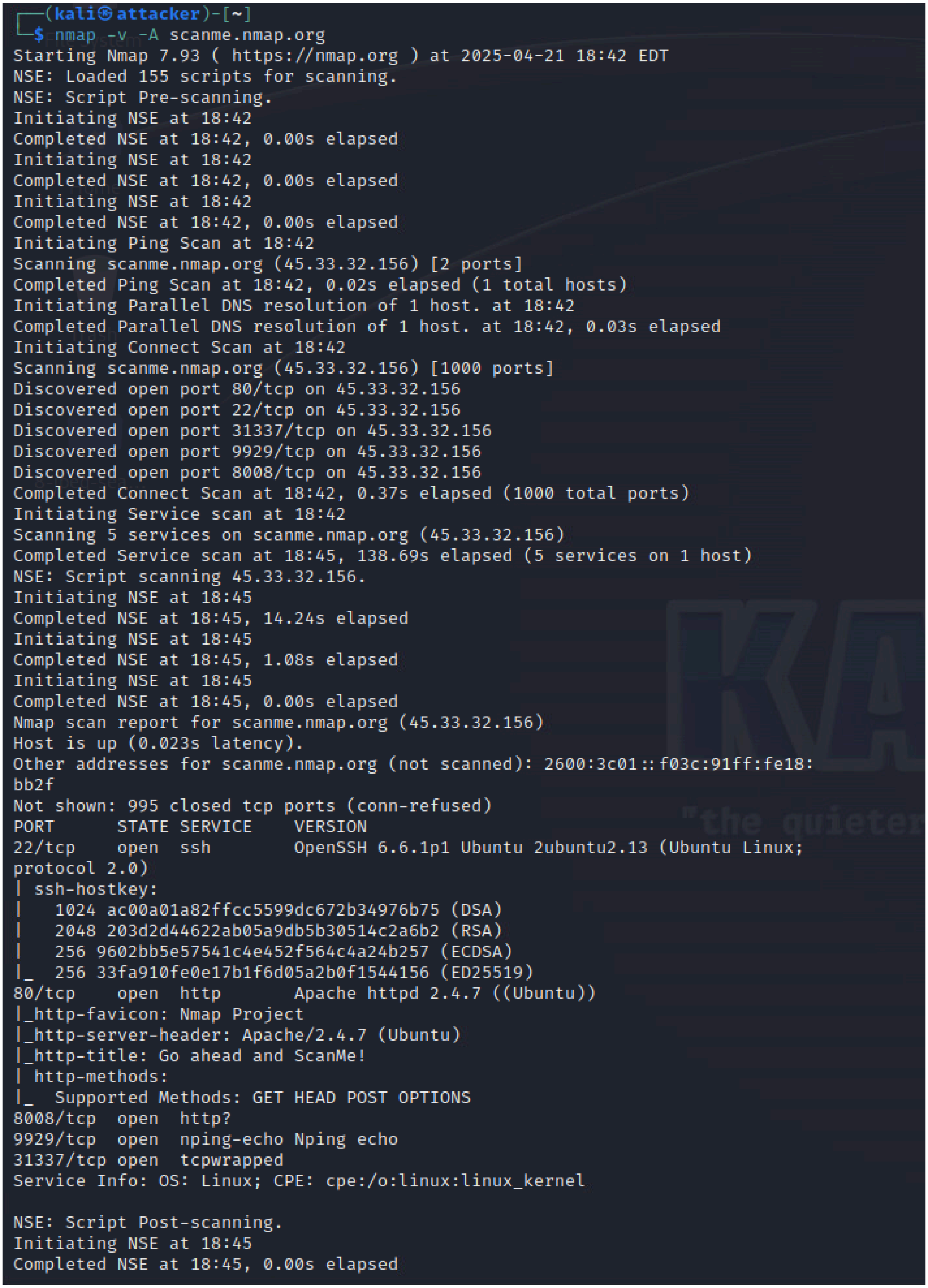
The security assessment followed a structured, multi-phase methodology combining automated tools, manual verification, and forensic analysis to identify vulnerabilities and collect potential evidence. The assessment covered external vulnerabilities, service misconfigurations, password weaknesses, and signs of compromise.

1. Vulnerability Scanning

- **Tools Used**: Greenbone Vulnerability Manager (GVM)
- **Purpose**: Automated scanning of the target systems to detect known vulnerabilities, outdated services, end-of-life operating systems, and insecure configurations.
- **Approach**: Scans were conducted against all reachable hosts in the client environment. Results were manually reviewed to eliminate false positives and confirm severity levels.

2. Network Mapping & Service Enumeration

- **Tools Used**: Nmap 192.68.57.10

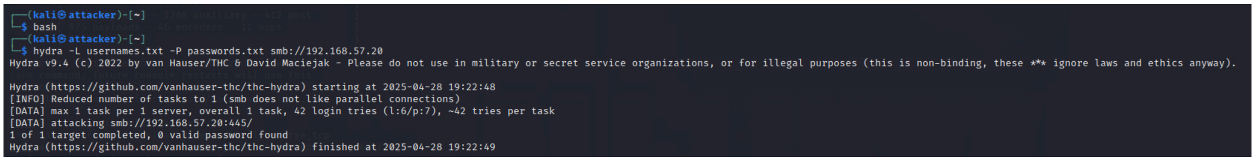


```
┌──(kali㉿attacker)-[~]
└─$ nmap -v -A scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-21 18:42 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:42
Completed NSE at 18:42, 0.00s elapsed
Initiating NSE at 18:42
Completed NSE at 18:42, 0.00s elapsed
Initiating NSE at 18:42
Completed NSE at 18:42, 0.00s elapsed
Initiating Ping Scan at 18:42
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 18:42, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:42
Completed Parallel DNS resolution of 1 host. at 18:42, 0.03s elapsed
Initiating Connect Scan at 18:42
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 8008/tcp on 45.33.32.156
Completed Connect Scan at 18:42, 0.37s elapsed (1000 total ports)
Initiating Service scan at 18:42
Scanning 5 services on scanme.nmap.org (45.33.32.156)
Completed Service scan at 18:45, 138.69s elapsed (5 services on 1 host)
NSE: Script scanning 45.33.32.156.
Initiating NSE at 18:45
Completed NSE at 18:45, 14.24s elapsed
Initiating NSE at 18:45
Completed NSE at 18:45, 1.08s elapsed
Initiating NSE at 18:45
Completed NSE at 18:45, 0.00s elapsed
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.023s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:
bb2f
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   1024 ac00a01a82ffcc5599dc672b34976b75 (DSA)
|   2048 203d2d44622ab05a9db5b30514c2a6b2 (RSA)
|   256 9602bb5e57541c4e452f564c4a24b257 (ECDSA)
|_  256 33fa910fe0e17b1f6d05a2b0f1544156 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Nmap Project
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
8008/tcp  open  http?
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 18:45
Completed NSE at 18:45, 0.00s elapsed
```

- **Purpose**: To identify live hosts, open ports, running services, and their versions.
- **Approach**: TCP SYN scans and service version detection were used to map the network perimeter and help scope further testing.

3. Password Brute-Forcing

- **Tools Used**: Hydra

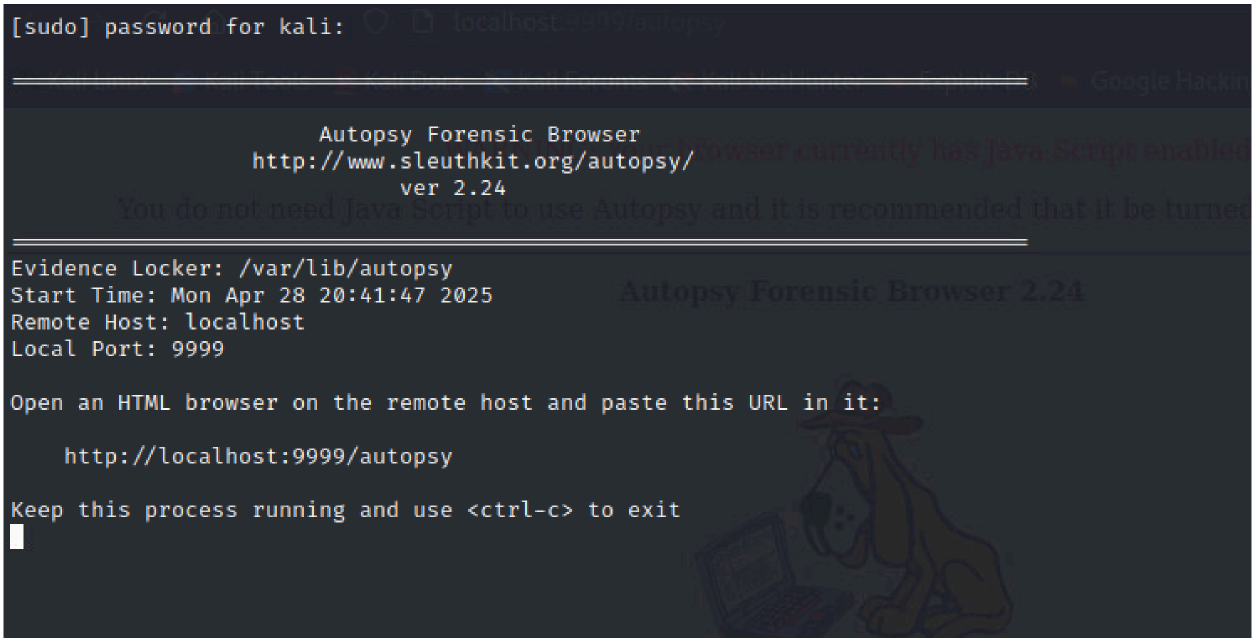


```
┌──(kali㉿attacker)-[~]
└─$ bash
┌──(kali㉿attacker)-[~]
└─$ hydra -L usernames.txt -P passwords.txt smb://192.168.57.20
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-28 19:22:48
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 42 login tries (l:6/p:7), ~42 tries per task
[DATA] attacking smb://192.168.57.20:445/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-28 19:22:49
```

- **Purpose**: To test the strength of login credentials against identified services such as SSH, FTP, and web logins.
- **Approach**: Brute-force attacks were attempted with controlled username/password combinations to validate password complexity and account lockout settings.

4. Digital Forensic Analysis

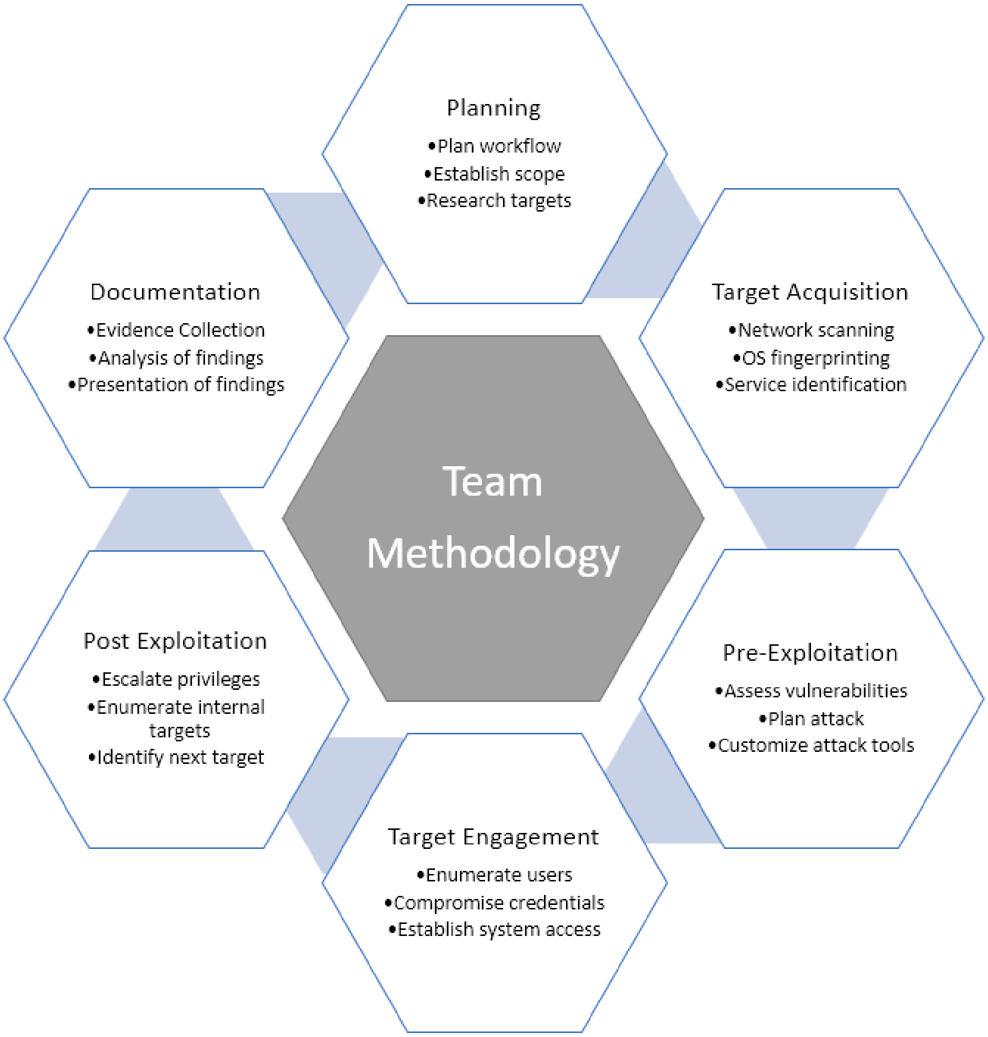
- **Tools Used**: Autopsy, FTK Imager
- **Purpose**: To analyze a forensic image for malicious files, hidden data, suspicious artifacts, and evidence of compromise.
- **Approach**: The disk image was loaded into forensic tools to inspect browser history, deleted files, persistence mechanisms, and time-stamped logs.



```
[sudo] password for kali:

============================================================================

                       Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                             ver 2.24

============================================================================
Evidence Locker: /var/lib/autopsy
Start Time: Mon Apr 28 20:41:47 2025
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
```

Each tool and method was selected based on its relevance to the scope of the assessment. All findings were validated where applicable to ensure accuracy and relevance. This approach ensures a thorough understanding of the system's current security posture.

The following image is a graphical representation of this methodology.



CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	**10**	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	**7-9**	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.

Medium	**4-6**	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	**1-3**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	**0**	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. Understanding of the underlying system is required for successful exploitation.
Unlikely	Exploitation requires deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

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)

1 - Tech Shield Greenbone Vulnerability Finding

10.0 (High)	
Exploitation Likelihood	Highly Likely
Business Impact	Severe
Remediation Difficulty	Moderate

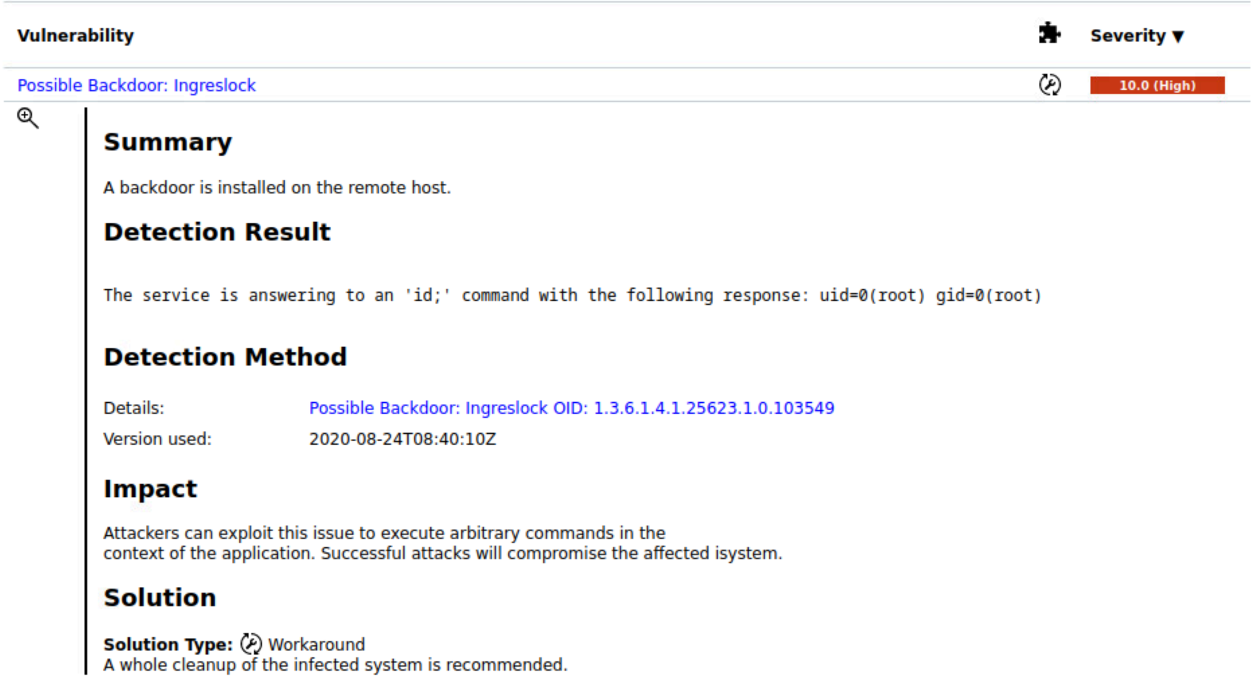
Synopsis

A backdoor was discovered on the system, allowing remote attackers to execute arbitrary commands. If exploited, this could lead to total system compromise.

Analysis

The Greenbone scan identified an active backdoor service running on the target host. This service permits unauthenticated remote code execution, giving an attacker the ability to control the system, extract sensitive data, or pivot to other systems in the network.

This vulnerability represents a severe breach of system integrity and confidentiality. The presence of such a backdoor strongly suggests previous or ongoing malicious activity and should be treated as an active compromise.



Vulnerability	Severity ▼
Possible Backdoor: Ingreslock	10.0 (High)

Summary

A backdoor is installed on the remote host.

Detection Result

```
The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)
```

Detection Method

Details:	Possible Backdoor: Ingreslock OID: 1.3.6.1.4.1.25623.1.0.103549
Version used:	2020-08-24T08:40:10Z

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution

Solution Type: Workaround
A whole cleanup of the infected system is recommended.

SUGGESTED REMEDIATION

Recommendations

- Immediately isolate the affected system from the network.
- Perform a full malware scan and forensic investigation to assess the extent of compromise.
- Wipe and rebuild the system from a clean, trusted backup.
- Review and harden all system configurations to prevent future unauthorized access.

FORENSIC EVIDENCE COLLECTION AND ANALYSIS

Scope

The objective of this forensic analysis was to investigate a compromised system 192.168.57.10 by identifying suspicious image files, analyzing metadata, and preserving potential evidence using industry-standard digital forensic practices. The investigation aimed to identify artifacts left by attackers and understand how the compromise may have occurred

Obtain and Verify Forensic Image Test File

- The forensic image **`8-jpeg-search.dd`** was located at **`C:\kali\Desktop\8-jpeg-search\.`**
- The hash of the image was verified using **`md5sum`** and/or **`sha256sum`** to ensure its integrity.
- The image was kept in a read-only format during the analysis to preserve evidence and maintain forensic soundness.

Create and Import Forensic Image into Autopsy:

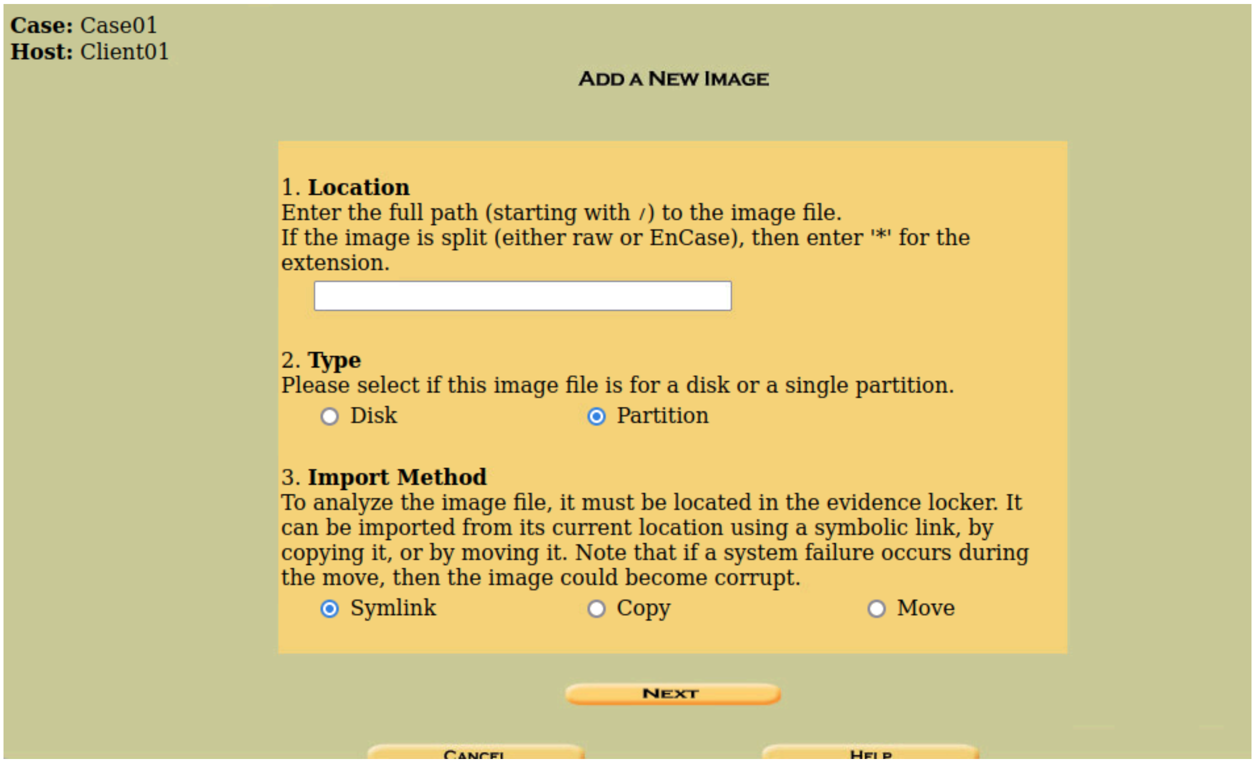
1. Opened Autopsy and created a new case titled "JPEG Search Analysis".

2. Selected **"Add Data Source"** → **Disk Image or VM File**.

3. Imported the forensic image from the path:
 C:\kali\Desktop\8-jpeg-search\8-jpeg-search.dd

4. Enabled modules for **File Analysis**, **Pictures**, **Extracted Content**, and **Metadata Viewer**.

5. Autopsy successfully parsed the image and displayed directory structures, media files, and deleted content.



Case: Case01
Host: Client01

ADD A NEW IMAGE

1. **Location**
Enter the full path (starting with /) to the image file.
If the image is split (either raw or EnCase), then enter '*' for the extension.

2. **Type**
Please select if this image file is for a disk or a single partition.
○ Disk ● Partition

3. **Import Method**
To analyze the image file, it must be located in the evidence locker. It can be imported from its current location using a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
● Symlink ○ Copy ○ Move

Analyze Forensic Image

- Navigated through the image contents and located a directory containing multiple .jpg files.

- Used the **Pictures** module to filter and view all JPEGs recovered from the disk image.

- Observed several suspicious or out-of-place images based on:

  - File path

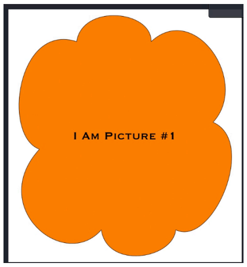
    - Timestamps
    - Metadata (e.g., altered EXIF data)

- Some of the images were found in **unexpected directories**, while others had signs of manual tampering or deletion.

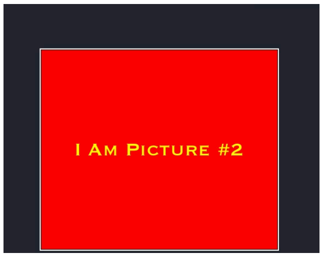
- Recovered and tagged **five key image files** as forensic artifacts for reporting.

Export Evidence Files

- **File1.jpeg**



- **file2.dat**



- **file3.jpg**

- **file4.png**
- **File5.txt**

Exported **Pictures 1–5** from the forensic image for documentation and reporting.

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
BurpSuite Community Edition	Used for testing of web applications.
Metasploit	Used for exploitation of vulnerable services and vulnerability scanning.
Nmap	Used for scanning ports on hosts.
OpenVAS	Used to scan the networks for vulnerabilities.
PostgreSQL Client Tools	Used to connect to the PostgreSQL server.

Table A.1: *Tools used during assessment*

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

Client	<CLIENT NAME>
Primary Contact	<Person Name>, <Person's Title>
Approvers	The following people are authorized to change the scope of engagement and modify the terms of the engagement ● <PERSON NAME 1> ● <PERSON NAME 2>

Version Information

Version	Date	Description
1.0	<DATE HERE>	Initial report to client

Contact Information

Name	<Tech Shield> Consulting
Address	Denver, CO
Phone	555-185-1782
Email	<REPLACE WITH PROVIDED EMAIL>