Vulnerability Assessment and Digital Forensics for Tech Shield

...

By: Joshua Camara
4/30/25
Stack Route Boot Camp

2. Problem Statement / Project Overview

Tech Shield is a managed IT services provider supporting clients like Orion Financial, CloudBase, and Mystore.

The purpose of this vulnerability assessment was to acknowledge the potential cyber incidents, threats, and raising concerns for Tech Shields security posture. TechShield needed a proactive **Vulnerability Assessment and Penetration Testing (VAPT)** to identify weaknesses before attackers could exploit them.

A **Digital Forensic Analysis** was also requested to understand how past incidents may have occurred and to gather evidence from a simulated attack.

This project entailed a full-security evaluation using industry tools to uncover risks, provide remediations, and ensure forensic evidence handling.

3. Project Outline & Testing Approach

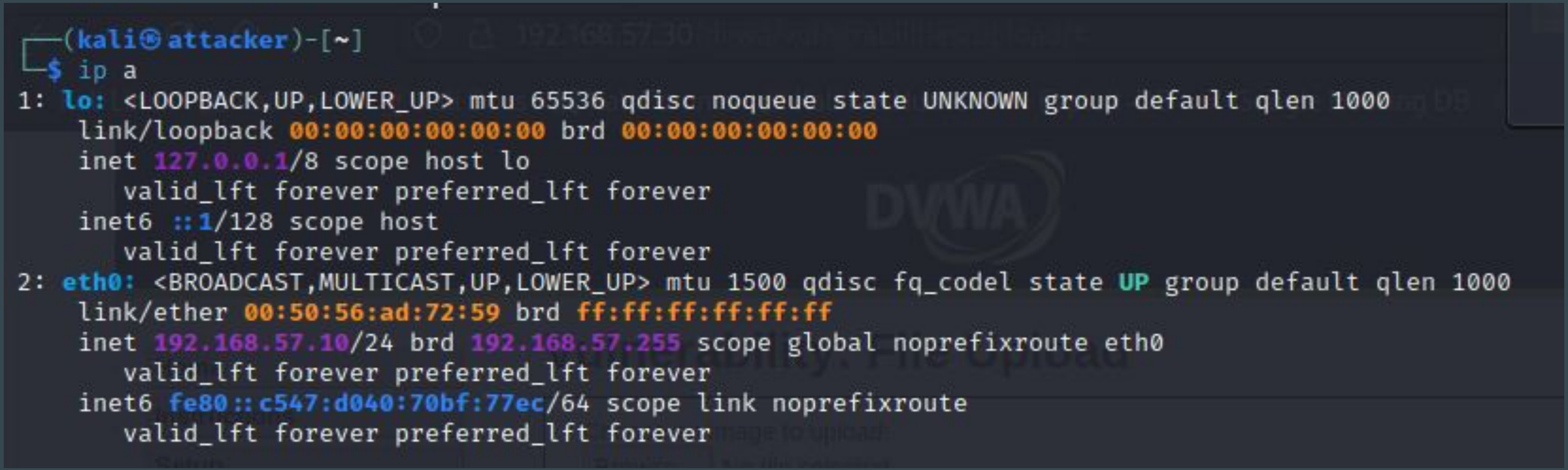
We conducted a full vulnerability assessment, identified and prioritized risks, while also performing digital forensic analysis, and documented all findings in a professional VAPT report.

- Penetration Testing → Vulnerability Identification → Forensics.
- Multi-tool strategy: Nmap, Greenbone, Hydra, Autopsy.
- Structured documentation and evidence gathering.

4.. Reconnaissance Phase

Before initiating the Nmap scan, we first identified the IP address by running the ip a command within the test environment. This allowed us to retrieve the necessary network interface details and was a great return point during our assessments.

IP: 192. 168. 57. 10/24   Subnet: 127 . 0 . 0 .1/8



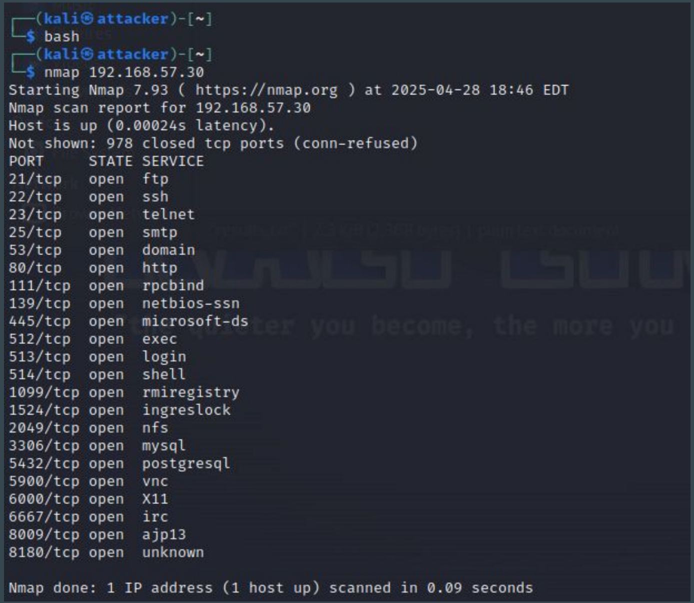
```
┌──(kali㉿attacker)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:ad:72:59 brd ff:ff:ff:ff:ff:ff
    inet 192.168.57.10/24 brd 192.168.57.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::c547:d040:70bf:77ec/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

5. Reconnaissance Phase (Cont...)

We then conducted a Nmap scan where we were able to identify open ports, live hosts , and services within the network. Enabled services helped guide vulnerability scan.

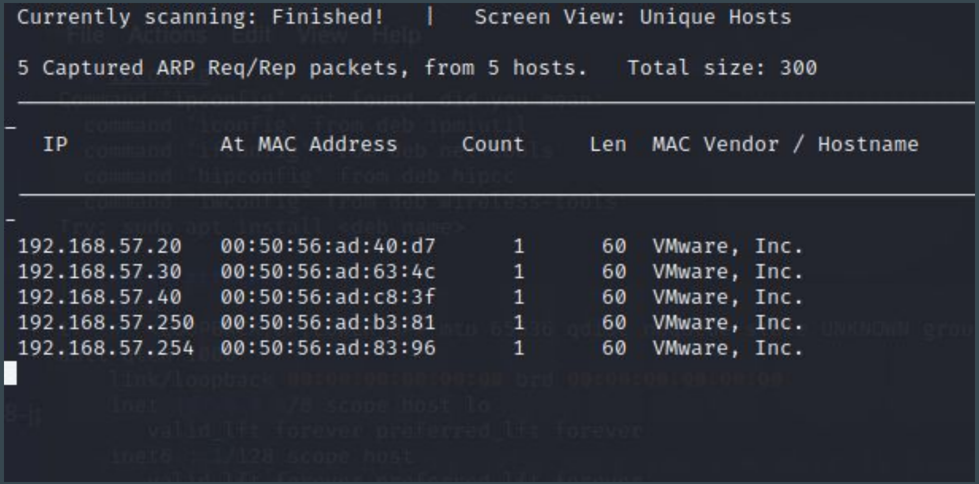
Key Findings: open ports: 22 (SSH), 80 (HTTP, 445 (SMB, 3389 (RDP)

Nmap Scanning:



```
┌──(kali㉿attacker)-[~]
└─$ bash
┌──(kali㉿attacker)-[~]
└─$ nmap 192.168.57.30
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-28 18:46 EDT
Nmap scan report for 192.168.57.30
Host is up (0.00024s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Hosts Detected:

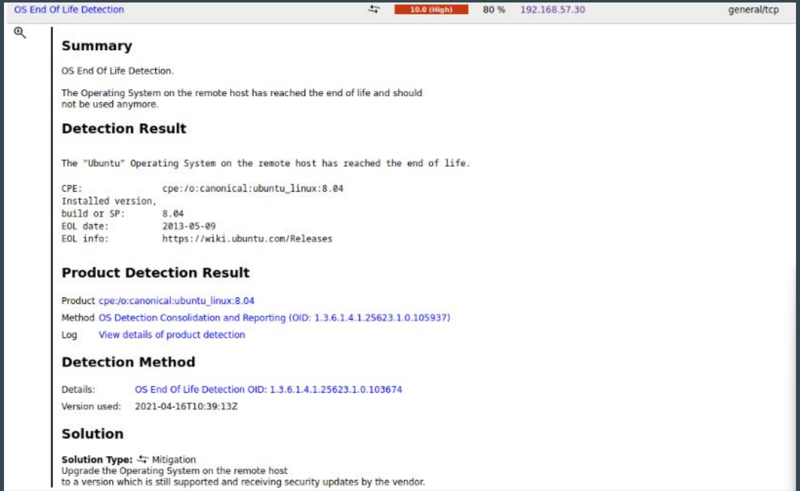


```
Currently scanning: Finished!   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP             At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.57.20    00:50:56:ad:40:d7      1      60  VMware, Inc.
192.168.57.30    00:50:56:ad:63:4c      1      60  VMware, Inc.
192.168.57.40    00:50:56:ad:c8:3f      1      60  VMware, Inc.
192.168.57.250   00:50:56:ad:b3:81      1      60  VMware, Inc.
192.168.57.254   00:50:56:ad:83:96      1      60  VMware, Inc.
```

6. Vulnerability Identification

We initiated the Greenbone Vulnerability Assessment to provides comprehensive scanning and to identify security weaknesses across networks, systems, and applications. While executing we were able to find; OS End-of-Life, Backdoor service installed, Rexec service open, Cross-site scripting issue.

OS End of Life Detection:



OS End Of Life Detection | 10.0 (High) | 80 % | 192.168.57.30 | general/tcp

Summary

OS End Of Life Detection.

The Operating System on the remote host has reached the end of life and should not be used anymore.

Detection Result

```
The "Ubuntu" Operating System on the remote host has reached the end of life.

CPE:                cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:        8.04
EOL date:           2013-05-09
EOL info:           https://wiki.ubuntu.com/Releases
```

Product Detection Result

Product cpe:/o:canonical:ubuntu_linux:8.04

Method OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Log View details of product detection

Detection Method

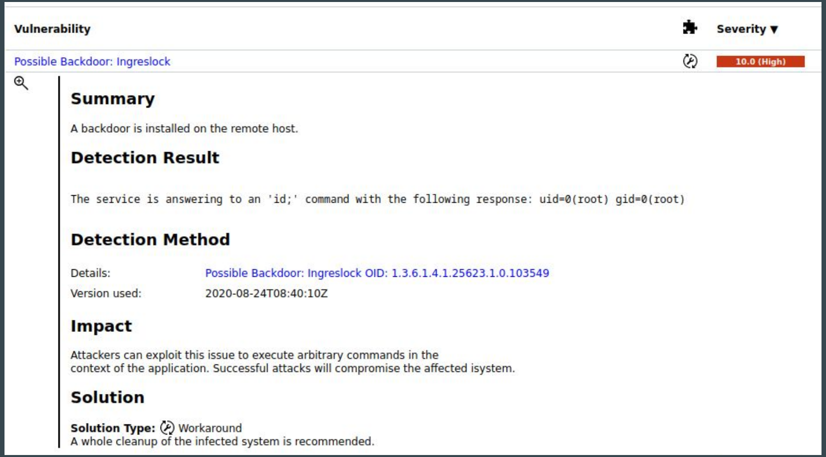
Details: OS End Of Life Detection OID: 1.3.6.1.4.1.25623.1.0.103674

Version used: 2021-04-16T10:39:13Z

Solution

Solution Type: Mitigation
Upgrade the Operating System on the remote host
to a version which is still supported and receiving security updates by the vendor.

Back Door:



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.

Risk Scores: Multiple CVEs ranked as 10.0 (Critical)

7. Vulnerability Assessment Finding: OS End of Life Detection:

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

- The Greenbone scan identified that the target system is running an End-of-Life operating system meaning this can no longer receive security updates or patches from the vendor.
- This makes the system highly vulnerable to known exploits, even if configurations appear secure.
- Attackers actively target unsupported systems to exploit unpatched vulnerabilities.

8. Vulnerability Assessment Finding: Back Door

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

This was one of the most critical findings of the scan.

- The back door allows unauthenticated remote command execution. If exploited, it can result in full system compromise and unauthorized access to sensitive data.
- Attackers may use this to extract files, escalate privileges, or move laterally across the network.
- This finding suggests a potential active compromise and represents a critical risk to system confidentiality, integrity, and availability.

9. Web Application Vulnerabilities

Tool Used: DVWA – Damn Vulnerable Web Application used to simulate real-world web vulnerabilities.

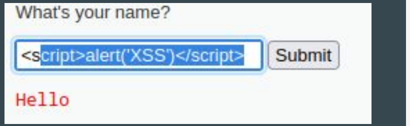
Vulnerability Identified: Cross-Site Scripting (XSS)

Testing Method: Injected malicious JavaScript (<script>alert("XSS")</script>) into input fields.

Outcome: XSS was successfully executed, demonstrating that the input fields were not properly sanitized.

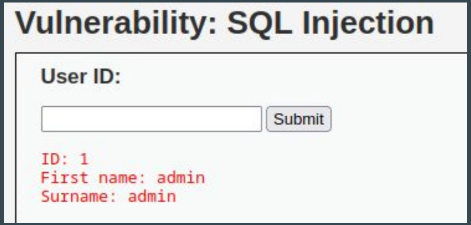
Impact: Attackers could steal session cookies, impersonate users, or perform unauthorized actions in a real-world scenario.

Screenshots:


What's your name?

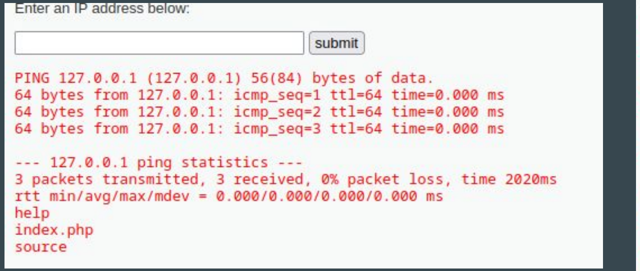
<script>alert('XSS')</script>

```
Hello
```

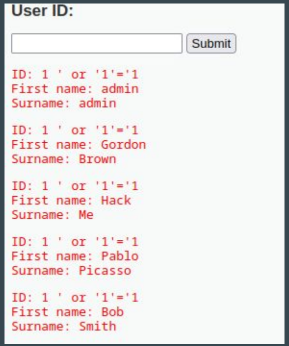

Vulnerability: SQL Injection

User ID:

```
ID: 1
First name: admin
Surname: admin
```


Enter an IP address below:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.000 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.000 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
help
index.php
source
```


User ID:

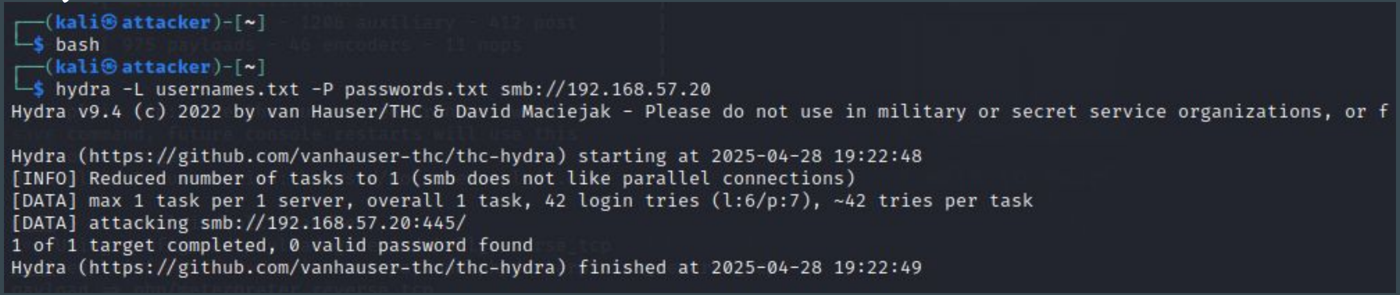
```
ID: 1 ' or '1'='1
First name: admin
Surname: admin

ID: 1 ' or '1'='1
First name: Gordon
Surname: Brown

ID: 1 ' or '1'='1
First name: Hack
Surname: Me

ID: 1 ' or '1'='1
First name: Pablo
Surname: Picasso

ID: 1 ' or '1'='1
First name: Bob
Surname: Smith
```

10. Password Attacks: Hydra

The tool we used was Hydra (Brute force password testing) and the targeted service was SMB (Server Message Block) on port 445 with the target IP: 192. 168. 57. 20.

Using Hydra, we performed a brute-force attack on the SMB, the tool attempted 42 logins combinations, but no valid credentials were identified. While no breach occurred, this test was essential in verifying that default or weak credentials were not in use. The result indicates that SMB is not easily compromised using basic dictionary attacks, which is a positive sign of password policy enforcement.

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 f

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
```

11. Forensic Analysis Process

The tool used was Autopsy and the forensic image used: **(8-jpeg-search.dd)** During the Forensic findings we were able to use and focus on images appearing from File1.jpeg to file5.dat.

Challenge 1: Tool Integration & Compatibility

- Difficulty running some tools simultaneously or configuring them properly (e.g., Autopsy or Hydra setup).
- *Solution:* Researched error messages, updated tool dependencies, and adjusted virtual machine settings to improve performance.

Challenge 2: Interpreting Vulnerability Scan Data

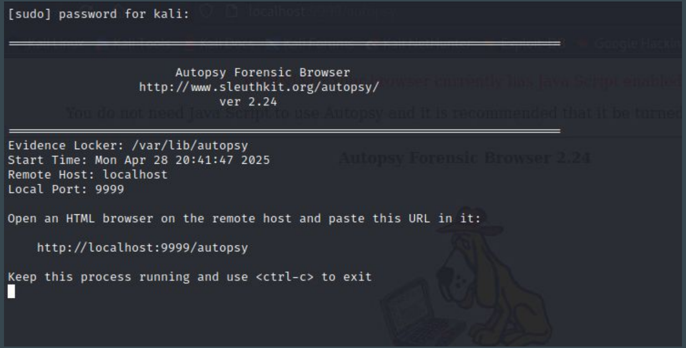
- Greenbone scan produced a large volume of data, making it difficult to prioritize.
- *Solution:* Focused on CVSS scores and sorted vulnerabilities by severity to extract key findings for the report.

Challenge 3: Limited Forensic Clues in Drive Image

- Initially hard to locate meaningful evidence inside the .dd image file.
- *Solution:* Used keyword searches, JPEG analysis, and explored hidden directories using Autopsy to uncover forensic artifacts.

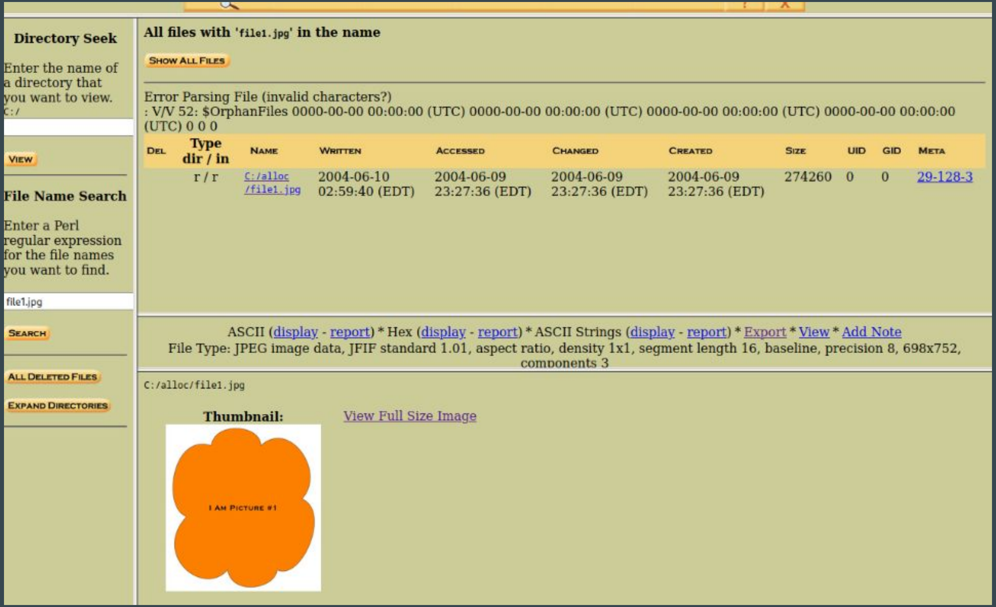
12. Forensic Evidence Process

Example of File1.jpeg retrieval of the forensic file which was then downloaded. We conducted the same process for each file example of one below.



```
[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
█
```

>



Directory Seek

Enter the name of a directory that you want to view.

C:/

File Name Search

Enter a Perl regular expression for the file names you want to find.

file1.jpg

All files with 'file1.jpg' in the name

Error Parsing File (invalid characters?)
: V/V 52: $OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	r / r	C:/alloc /file1.jpg	2004-06-10 02:59:40 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	2004-06-09 23:27:36 (EDT)	274260	0	0	29-128-3

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 698x752, components 3

C:/alloc/file1.jpg

Thumbnail: View Full Size Image

13. Forensic Evidence Findings

Finding: Multiple suspicious image files (file1.jpeg to file5.jpeg) were discovered in the forensic disk image (8-jpeg-search.dd) using Autopsy.

- **Location:** Files were found under `C:\kali\Desktop\8-jpeg-search\` during image examination.
- **Observation:** The presence of JPEGs in unusual locations and without clear context may indicate exfiltrated or hidden data.
- **Gap Identified:** Lack of host-based monitoring or file integrity checks made it difficult to detect tampering or unauthorized file placement.
- **Suggested Improvement:**
  - Implement centralized log management and file monitoring systems.
  - Train IT staff on early indicators of compromise and forensic readiness.

14. Areas for Improvement

- **Tool Familiarity:**
  - Initial difficulties configuring Autopsy and Hydra delayed forensic and brute-force testing.
  - *Improvement:* More pre-configured lab practice and tool walkthroughs.
- **Forensic Analysis Speed:**
  - Time-consuming to locate relevant files within .dd image.
  - *Improvement:* Develop custom keyword lists and improve Autopsy filtering.
- **Data Overload in Scans:**
  - Greenbone generated many low-severity findings, overwhelming focus.
  - *Improvement:* Automate report filtering based on CVSS thresholds.
- **Realistic Exploitation Scenarios:**
  - Some attacks were conducted in lab conditions (examples being DVWA XSS), not on actual services.
  - *Improvement:* Set up more realistic test environments for better simulation.

15. Conclusion

Through this project, we successfully conducted a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) along with a foundational digital forensic analysis. Using tools such as Greenbone, Nmap, Hydra, and Autopsy, we identified multiple critical vulnerabilities including a backdoor service, OS end-of-life systems, and exploitable web application flaws such as XSS. Forensic analysis of a compromised disk image revealed suspicious files that could indicate prior malicious activity. These findings demonstrate the real-world risks organizations face if security best practices are not followed. The project highlights the importance of continuous vulnerability management, regular system upgrades, and forensic readiness. By implementing the outlined recommendations, TechShield and its clients can significantly enhance their security posture and minimize the risk of future incidents

Thank you!