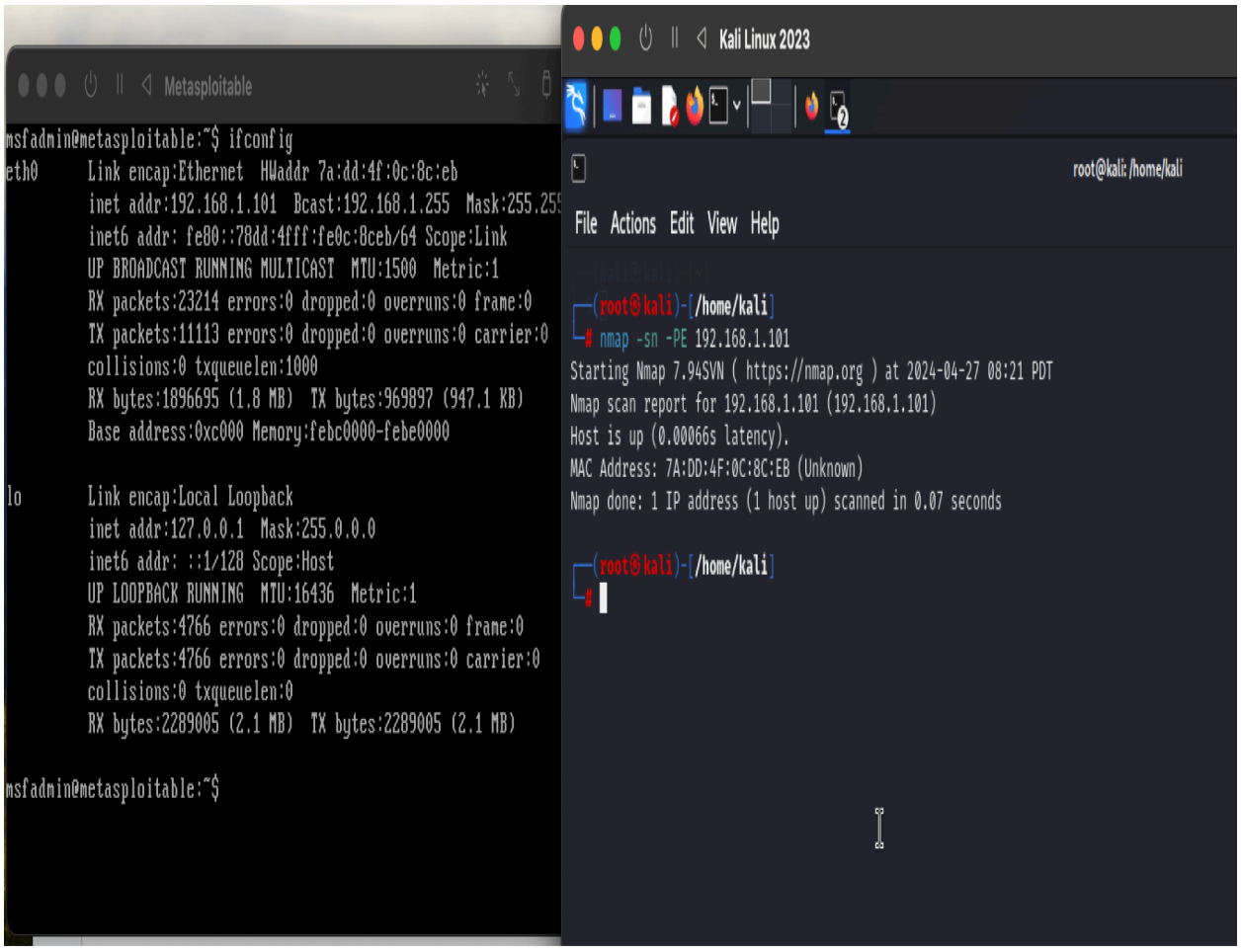
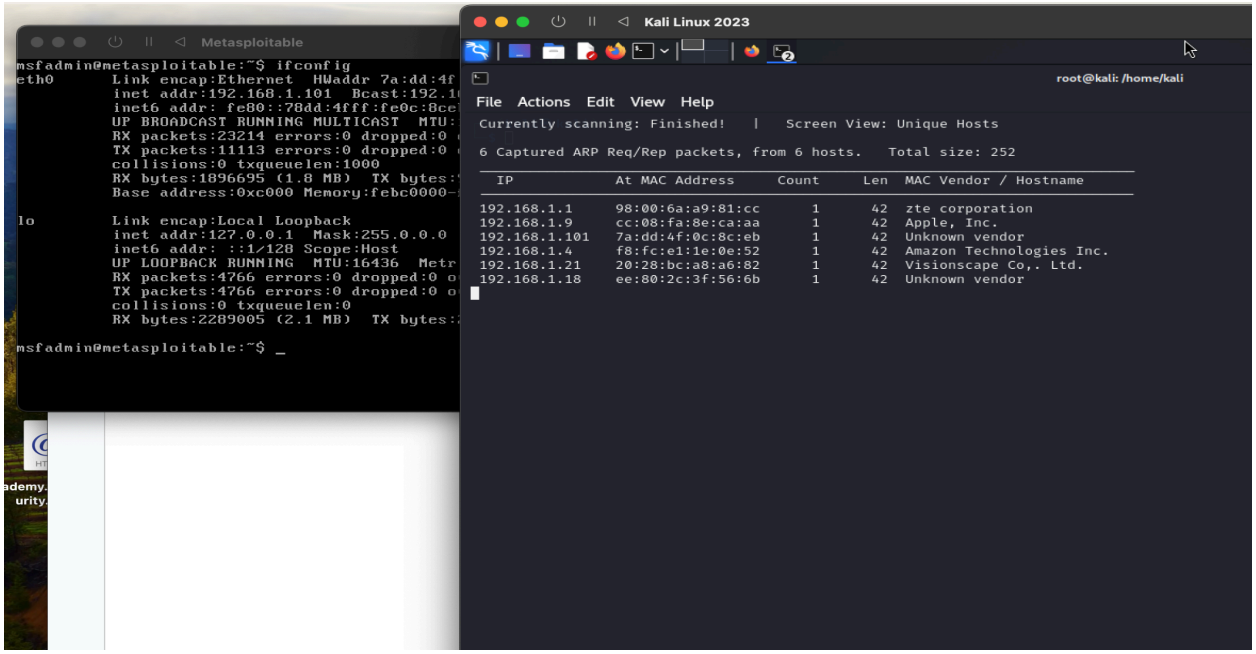
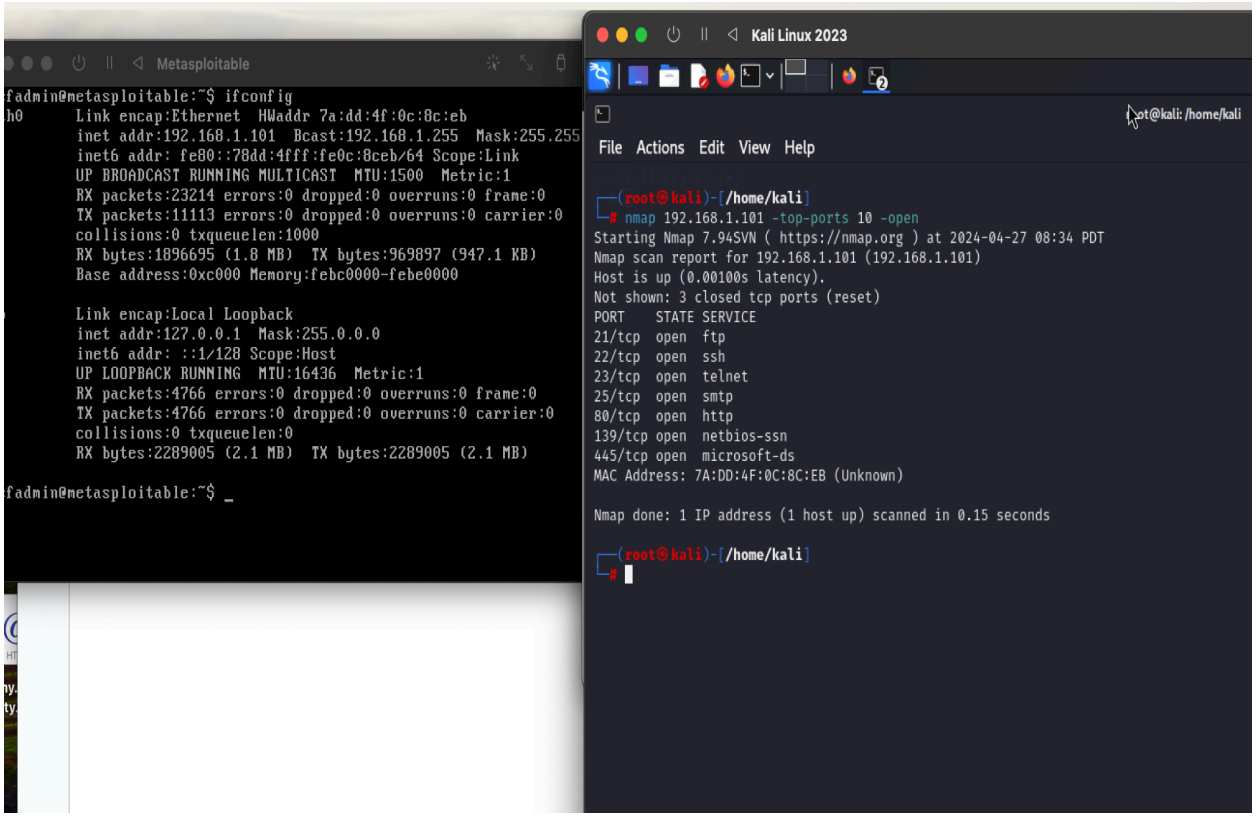
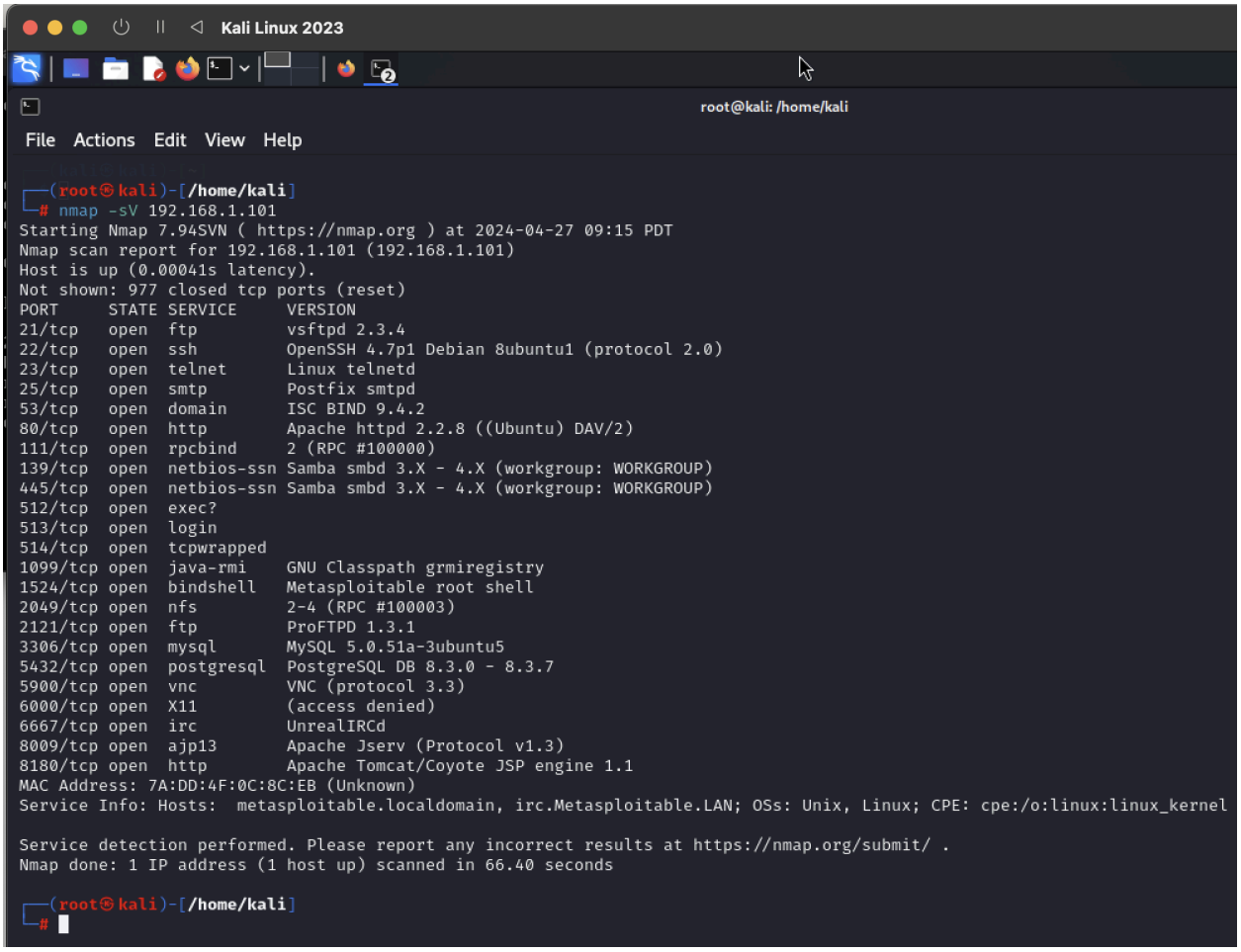
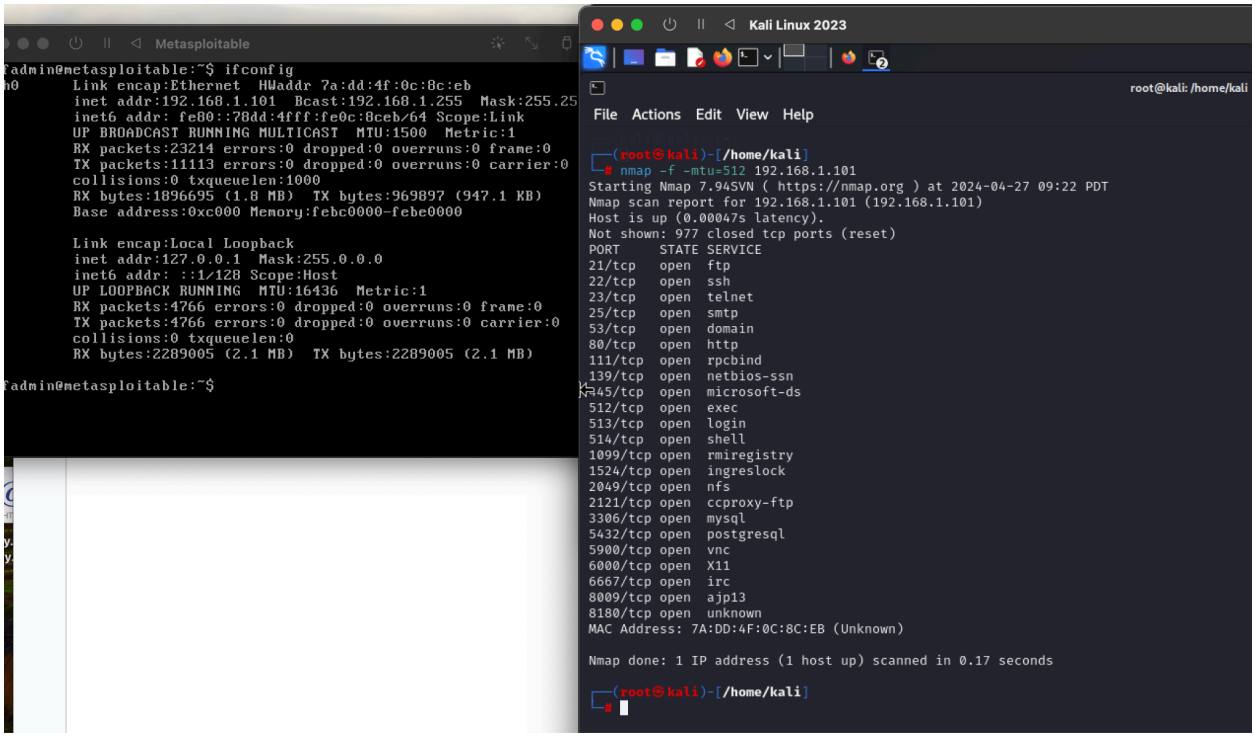
- 1. nmap -sn -PE <target>
- 2. netdiscover -r <target>
- 3. crackmapexec <target>
- 4. nmap <target> –top-ports 10 –open
- 5. nmap <target> -p- -sV –reason –dns-server ns
- 6. us -mT -lv <target>:a -r 3000 -R 3 && us -mU -lv <target>:a -r 3000 -R 3
- 7. nmap -sS -sV -T4 <target>
- 8. hping3 –scan known <target>
- 9. nc -nvz <target> 1-1024
- 10. nc -nv <target> 22
- 11. nmap -sV <target>
- 12. db_import <file.xml> (For Metasploit Framework)
- 13. nmap -f –mtu=512 <target>
- 14. masscan <network> -p80 –banners –source-ip <target>

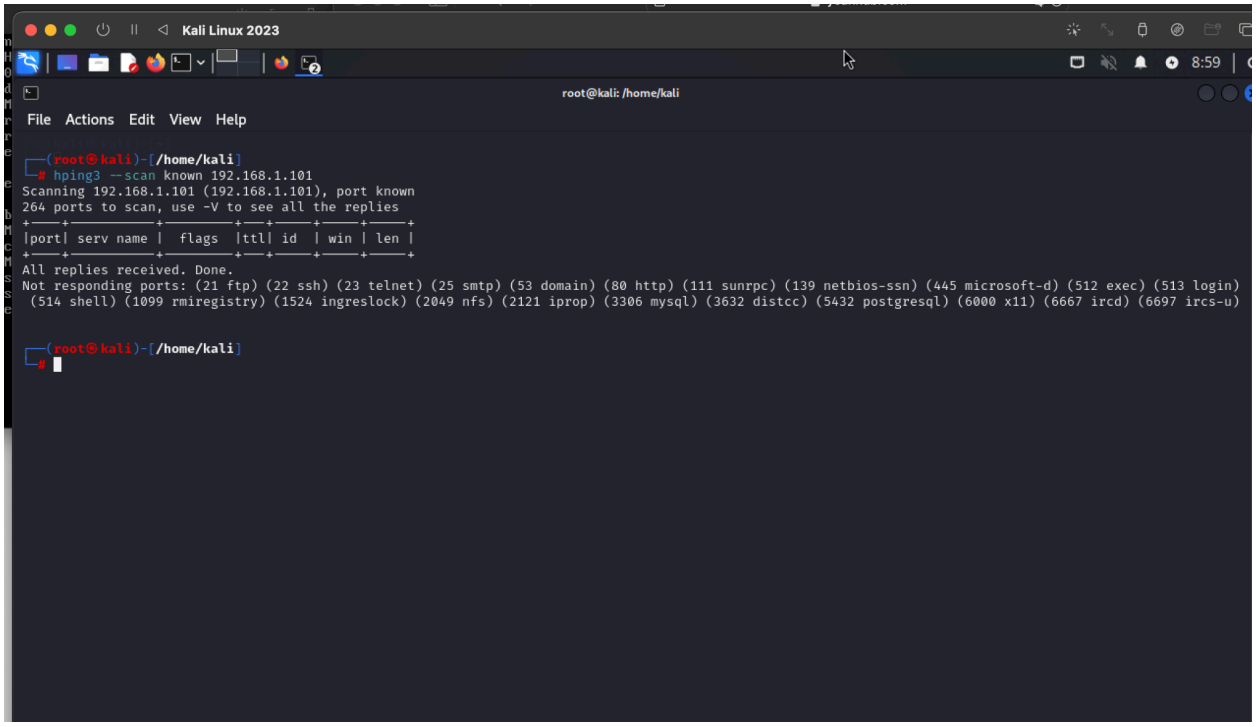


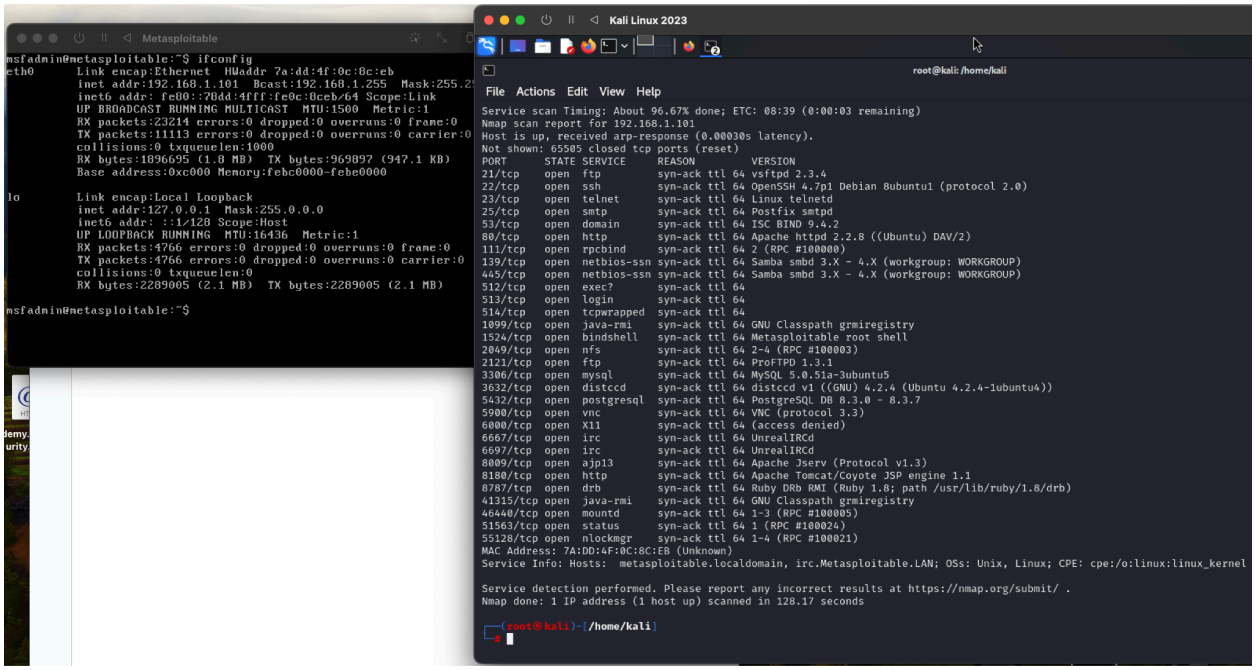

Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f
inet addr:192.168.1.101 Bcast:192.1
inet6 addr: fe80::78dd:4fff:fe0c:8ce
UP BROADCAST RUNNING MULTICAST MTU:
RX packets:23214 errors:0 dropped:0
TX packets:11113 errors:0 dropped:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:
Base address:0xc000 Memory:febc0000-
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 Metr
RX packets:4766 errors:0 dropped:0 o
TX packets:4766 errors:0 dropped:0 o
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:
msfadmin@metasploitable:~$ _
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
6 Captured ARP Req/Rep packets, from 6 hosts. Total size: 252
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.1.1 98:00:6a:a9:81:cc 1 42 zte corporation
192.168.1.9 cc:08:fa:8e:ca:aa 1 42 Apple, Inc.
192.168.1.101 7a:dd:4f:0c:8c:eb 1 42 Unknown vendor
192.168.1.4 f8:fc:e1:1e:0e:52 1 42 Amazon Technologies Inc.
192.168.1.21 20:28:bc:a8:a6:82 1 42 Visionscape Co,. Ltd.
192.168.1.18 ee:80:2c:3f:56:6b 1 42 Unknown vendor

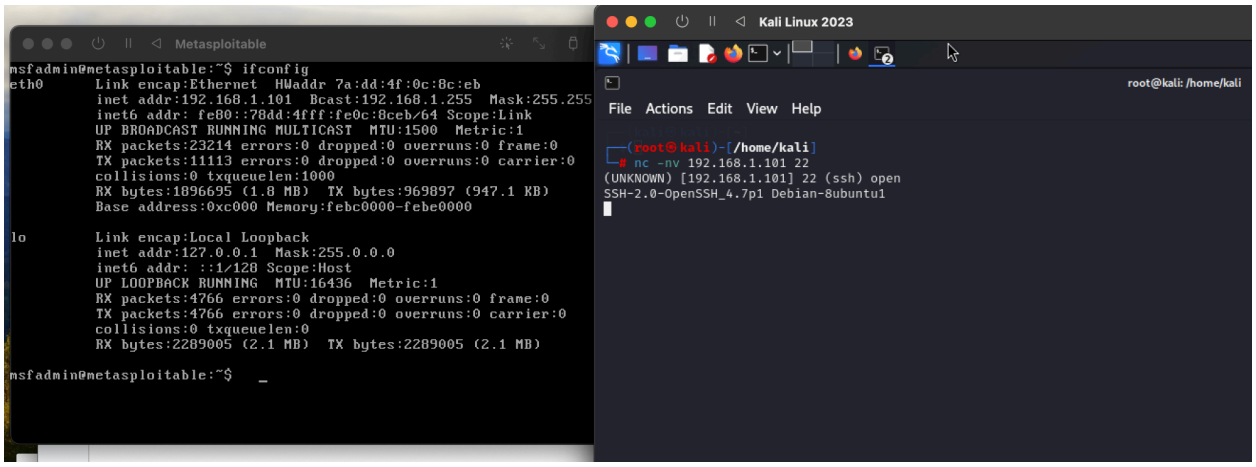

Metasploitable
fadmin@metasploitable:~$ ifconfig
h0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
fadmin@metasploitable:~$ _
Kali Linux 2023
ot@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
nmap 192.168.1.101 -top-ports 10 -open
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-27 08:34 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00100s latency).
Not shown: 3 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
(root@kali)-[/home/kali]
#

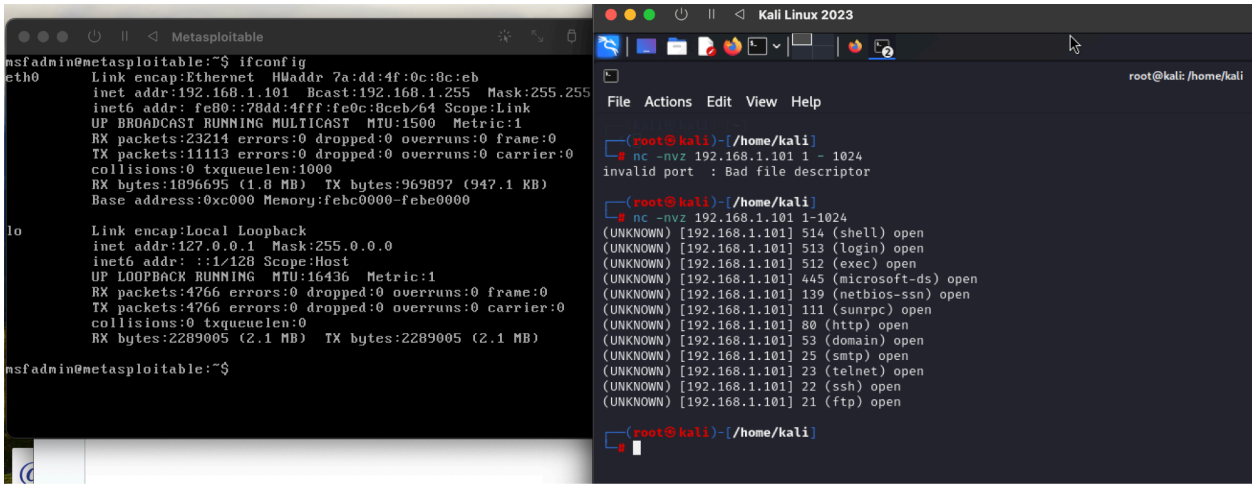

Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.1.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-27 09:15 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00041s latency).
Not shown: 977 closed tcp ports (reset)
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?
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: 7A:DD:4F:0C:8C:EB (Unknown)
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 66.40 seconds
┌──(root㉿kali)-[/home/kali]
└─#

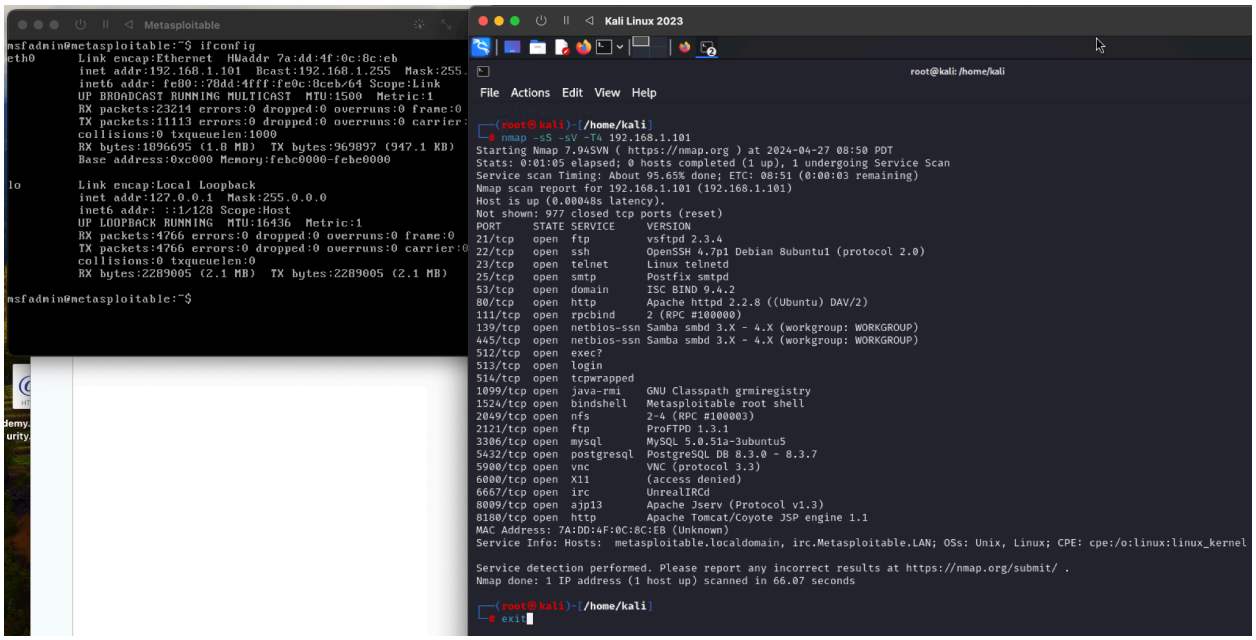

Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.25
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
msfadmin@metasploitable:~$
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -f -mtu=512 192.168.1.101
Starting Nmap 7.94SVN (https://nmap.org) at 2024-04-27 09:22 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00047s latency).
Not shown: 977 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
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
┌──(root㉿kali)-[/home/kali]
└─#


Kali Linux 2023
8:59
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# hping3 --scan known 192.168.1.101
Scanning 192.168.1.101 (192.168.1.101), port known
264 ports to scan, use -V to see all the replies
+----+-----------+--------+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+----+-----------+--------+---+-----+-----+-----+
All replies received. Done.
Not responding ports: (21 ftp) (22 ssh) (23 telnet) (25 smtp) (53 domain) (80 http) (111 sunrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login)
(514 shell) (1099 rmiregistry) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql) (6000 x11) (6667 ircd) (6697 ircs-u)
┌──(root㉿kali)-[/home/kali]
└─#


Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.2
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
msfadmin@metasploitable:~$
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
Service scan Timing: About 96.67% done; ETC: 08:39 (0:00:03 remaining)
Nmap scan report for 192.168.1.101
Host is up, received arp-response (0.00030s latency).
Not shown: 65505 closed tcp ports (reset)
PORT STATE SERVICE REASON VERSION
21/tcp open ftp syn-ack ttl 64 vsftpd 2.3.4
22/tcp open ssh syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet syn-ack ttl 64 Linux telnetd
25/tcp open smtp syn-ack ttl 64 Postfix smtpd
53/tcp open domain syn-ack ttl 64 ISC BIND 9.4.2
80/tcp open http syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec? syn-ack ttl 64
513/tcp open login syn-ack ttl 64
514/tcp open tcpwrapped syn-ack ttl 64
1099/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp open bindshell syn-ack ttl 64 Metasploitable root shell
2049/tcp open nfs syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp open ftp syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp open mysql syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp open distccd syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp open X11 syn-ack ttl 64 (access denied)
6667/tcp open irc syn-ack ttl 64 UnrealIRCd
6697/tcp open irc syn-ack ttl 64 UnrealIRCd
8009/tcp open ajp13 syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp open http syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open drb syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
41315/tcp open java-rmi syn-ack ttl 64 GNU Classpath grmiregistry
46440/tcp open mountd syn-ack ttl 64 1-3 (RPC #100005)
51563/tcp open status syn-ack ttl 64 1 (RPC #100024)
55128/tcp open nlockmgr syn-ack ttl 64 1-4 (RPC #100021)
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
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 128.17 seconds
(root@kali)-[/home/kali]
#


Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
msfadmin@metasploitable:~$
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
nc -nv 192.168.1.101 22
(UNKNOWN) [192.168.1.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1


Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.255
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
msfadmin@metasploitable:~$
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
nc -nvz 192.168.1.101 1 - 1024
invalid port : Bad file descriptor
(root㉿kali)-[/home/kali]
nc -nvz 192.168.1.101 1-1024
(UNKNOWN) [192.168.1.101] 514 (shell) open
(UNKNOWN) [192.168.1.101] 513 (login) open
(UNKNOWN) [192.168.1.101] 512 (exec) open
(UNKNOWN) [192.168.1.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.1.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.1.101] 111 (sunrpc) open
(UNKNOWN) [192.168.1.101] 80 (http) open
(UNKNOWN) [192.168.1.101] 53 (domain) open
(UNKNOWN) [192.168.1.101] 25 (smtp) open
(UNKNOWN) [192.168.1.101] 23 (telnet) open
(UNKNOWN) [192.168.1.101] 22 (ssh) open
(UNKNOWN) [192.168.1.101] 21 (ftp) open
(root㉿kali)-[/home/kali]
#


Metasploitable
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 Mask:255.
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:23214 errors:0 dropped:0 overruns:0 frame:0
TX packets:11113 errors:0 dropped:0 overruns:0 carrier:
collisions:0 txqueuelen:1000
RX bytes:1896695 (1.8 MB) TX bytes:969897 (947.1 KB)
Base address:0xc000 Memory:febc0000-febe0000
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:4766 errors:0 dropped:0 overruns:0 frame:0
TX packets:4766 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2289005 (2.1 MB) TX bytes:2289005 (2.1 MB)
msfadmin@metasploitable:~$
Kali Linux 2023
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
nmap -sS -sV -T4 192.168.1.101
Starting Nmap 7.945VN (https://nmap.org) at 2024-04-27 08:50 PDT
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 08:51 (0:00:03 remaining)
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00048s 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?
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: 7A:DD:4F:0C:8C:EB (Unknown)
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 66.07 seconds
(root㉿kali)-[/home/kali]
exit