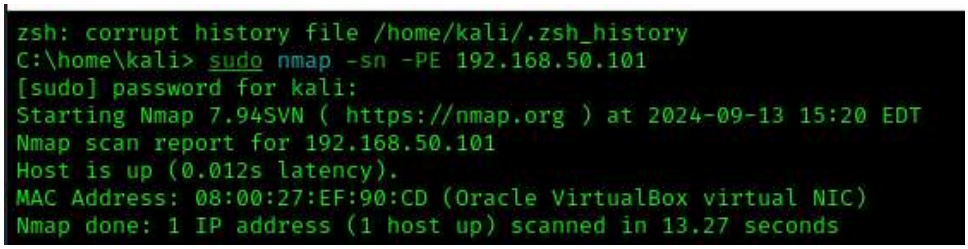
sabato 14 settembre 2024 19:24

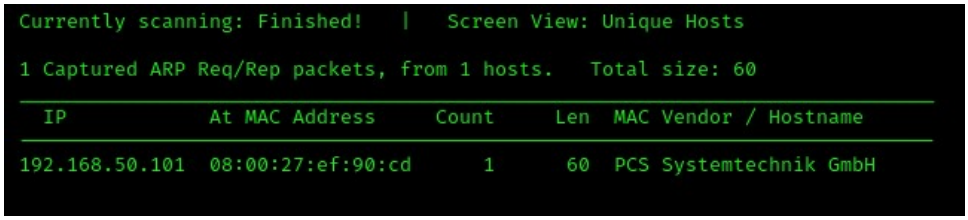
Traccia:
https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/
Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report.
Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate

nmap -sn -PE <IP target>



- **Nmap** è uno strumento utilizzato per la scansione delle reti.
- Il flag **-sn** significa che verrà eseguita un "ping scan", ovvero Nmap verifica se gli host sono attivi senza eseguire una scansione delle porte.
- Il flag **-PE** invia pacchetti ICMP Echo Request (ping standard) per rilevare se il bersaglio (**<target>**) è attivo.

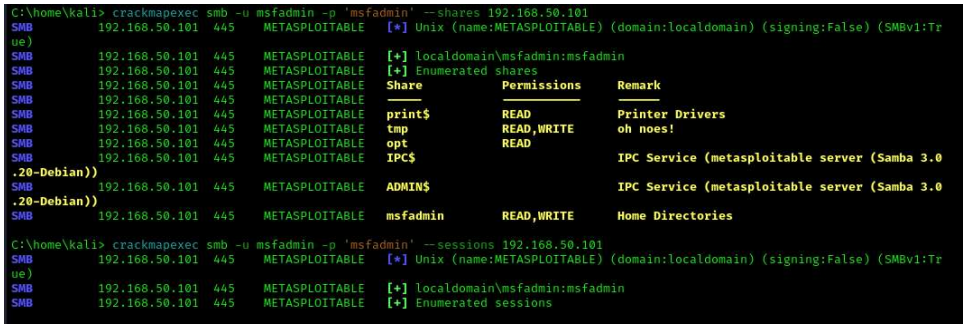
netdiscover -r <IP target>



Netdiscover è uno strumento per trovare host in una rete locale.

- Il flag **-r** specifica l'intervallo di indirizzi IP da scansionare (ad esempio, una sottorete come 192.168.50.101/24).

crackmapexec <IP target>



CrackMapExec è uno strumento di post-exploitation utilizzato durante test di penetrazione, verifiche di sicurezza e audit delle reti.
CrackMapExec può enumerare informazioni cruciali all'interno di una rete, come:

- Gli utenti che hanno accesso a una determinata macchina.
- I gruppi a cui appartengono gli utenti.
- I servizi attivi su un determinato host.

Queste informazioni sono fondamentali per un attaccante per capire la struttura e le vulnerabilità di una rete.

nmap <IP target> –top-ports 10 –open

Esegue una scansione Nmap su **<target>**.

- **--top-ports 10** significa che Nmap controllerà le 10 porte più comuni (quelle più usate dai servizi).
- **--open** limita i risultati alle porte che risultano aperte.

nmap <IP target> -p- -sV –reason –dns-server ns

```
C:\home\kali> sudo nmap 192.168.50.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 14:25 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid serve
h --dns-servers
Nmap scan report for 192.168.50.101
Host is up, received arp-response (0.037s 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 netkit-rsh rexecd
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell       syn-ack ttl 64 Netkit rshd
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)
35714/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
36779/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
46405/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
60594/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:EF:90:CD (Oracle VirtualBox virtual NIC)
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 168.55 seconds
```

- **-p-** significa che verranno scansionate tutte le porte (1-65535).
- **-sV** cerca di identificare la versione dei servizi in esecuzione sulle porte aperte.
- **--reason** mostra il motivo per cui una porta è stata classificata come aperta, chiusa o filtrata.
- **--dns-server ns** permette di specificare un server DNS personalizzato per risolvere i nomi di dominio (qui specificato come **ns**).

nmap -sS -sV -T4 <IP target>

```
C:\home\kali> sudo nmap -sS -sV -T4 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 15:26 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0090s 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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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: 08:00:27:EF:90:CD (Oracle VirtualBox virtual NIC)
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 69.54 seconds
```

Questo comando determina se la porta è in ascolta questa tecnica viene chiamata scansione semiaperta perché non viene stabilita una connessione TCP completa ma vene inviato solamente un pacchetto SYN e si attende la risposta. Se la ricevuta sarà SYN/ACK significa che la porta è in ascolto

- **-sS** esegue una "scansione SYN" (rapida e furtiva).

- **-sV** cerca di determinare la versione dei servizi in esecuzione sulle porte aperte.
- **-T4** aumenta la velocità della scansione, riducendo il tempo di attesa tra i pacchetti, utile su reti veloci.

hping3 –scan known <IP target>

```
zsh: corrupt history file /home/kali/.zsh_history
C:\home\kali> sudo hping3 --scan known 192.168.50.101
[sudo] password for kali:
Scanning 192.168.50.101 (192.168.50.101), 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 su
nrpc) (139 netbios-ssn) (445 microsoft-d) (512 exec) (513 login) (514 shell) (1099 rmiregis
try) (1524 ingreslock) (2049 nfs) (2121 iprop) (3306 mysql) (3632 distcc) (5432 postgresql)
 (6000 x11) (6667 ircd) (6697 ircs-u)
```

Hping3 è uno strumento avanzato per inviare pacchetti TCP/IP personalizzati. È simile a un "ping", ma molto più potente, permettendo di inviare oltre ai pacchetti TCP/IP anche pacchetti UDP e ICMP personalizzati.

- **--scan known** dice a Hping3 di scansionare solo le porte conosciute (standard) sul bersaglio **<target>**.

hping3 -V –scan known <IP target>

```
C:\home\kali> sudo hping3 -V --scan known 192.160.50.101
using eth0, addr: 192.168.50.100, MTU: 1500
Scanning 192.160.50.101 (192.160.50.101), 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: (1 tcpmux) (2 nbp) (4 echo) (6 zip) (7 echo) (9 discard) (11 systat)
(13 daytime) (15 netstat) (17 qotd) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 telnet
) (25 smtp) (37 time) (43 whois) (49 tacacs) (53 domain) (67 bootps) (68 bootpc) (69 tftp)
(70 gopher) (79 finger) (80 http) (88 kerberos) (102 iso-tsap) (104 acr-nema) (106 poppassd
) (110 pop3) (111 sunrpc) (113 auth) (119 nntp) (123 ntp) (135 epmap) (137 netbios-ns) (138
 netbios-dgm) (139 netbios-ssn) (143 imap2) (161 snmp) (162 snmp-trap) (163 cmip-man) (164
cmip-agent) (174 mailq) (177 xdmcp) (179 bgp) (199 smux) (209 qmtp) (210 z3950) (213 ipx) (
319 ptp-event) (320 ptp-general) (345 pawserv) (346 zserv) (369 rpc2portmap) (370 codaauth2
) (371 clearcase) (389 ldap) (427 svrloc) (443 https) (444 snpp) (445 microsoft-d) (464 kpa
sswd) (465 submissions) (487 saft) (500 isakmp) (512 exec) (513 login) (514 shell) (515 pri
nter) (517 talk) (518 ntalk) (520 route) (538 gdomap) (540 uucp) (543 klogin) (544 kshell)
(546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (554 rtsp) (563 nntps) (587 submission
) (607 nqs) (623 asf-rmcp) (628 qmqp) (631 ipp) (636 ldaps) (646 ldp) (655 tinc) (706 silc)
 (749 kerberos-ad) (750 kerberos4) (751 kerberos-ma) (752 passwd-serv) (754 krb-prop) (775
moira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (853 domain-s) (871 supfilesrv) (8
73 rsync) (989 ftps-data) (990 ftps) (992 telnets) (993 imaps) (995 pop3s) (1080 socks) (10
93 proofd) (1094 rootd) (1099 rmiregistry) (1127 supfiledbg) (1178 skkserv) (1194 openvpn)
(1210 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw) (1352 lotusnote) (1433 ms-sql-s) (143
4 ms-sql-m) (1524 ingreslock) (1645 datametrics) (1646 sa-msg-port) (1649 kermit) (1677 gro
upwise) (1701 l2f) (1812 radius) (1813 radius-acct) (2000 cisco-sccp) (2049 nfs) (2086 gnun
et) (2101 rtcm-sc104) (2102 zephyr-srv) (2103 zephyr-clt) (2104 zephyr-hm) (2119 gsigatekee
p) (2121 iprop) (2135 gris) (2401 cvspserver) (2430 venus) (2431 venus-se) (2432 codasrv) (
2433 codasrv-se) (2583 mon) (2600 zebrasrv) (2601 zebra) (2602 ripd) (2603 ripngd) (2604 os
pfd) (2605 bgpd) (2606 ospf6d) (2607 ospfapi) (2608 isisd) (2628 dict) (2792 f5-globalsi) (
2811 gsiftp) (2947 gpsd) (3050 gds-db) (3130 icpv2) (3205 isns) (3260 iscsi-targe) (3306 my
sql) (3389 ms-wbt-serv) (3493 nut) (3632 distcc) (3689 daap) (3690 svn) (4031 suucp) (4094
sysrqd) (4190 sieve) (4353 f5-iquery) (4369 epmd) (4373 remctl) (4460 ntske) (4500 ipsec-na
t-t) (4557 fax) (4559 hylafax) (4569 iax) (4691 mtn) (4899 radmin-port) (4949 munin) (5060
sip) (5061 sip-tls) (5222 xmpp-client) (5269 xmpp-server) (5308 cfengine) (5353 mdns) (5432
 postgresql) (5555 rplay) (5556 freeciv) (5666 nrpe) (5667 nsca) (5671 amqps) (5672 amqp) (
5680 canna) (6000 x11) (6001 x11-1) (6002 x11-2) (6003 x11-3) (6004 x11-4) (6005 x11-5) (60
06 x11-6) (6007 x11-7) (6346 gnutella-sv) (6347 gnutella-rt) (6379 redis) (6444 sge-qmaster
) (6445 sge-execd) (6446 mysql-proxy) (6514 syslog-tls) (6566 sane-port) (6667 ircd) (6696
babel) (6697 ircs-u) (7000 bbs) (7001 afs3-callba) (7002 afs3-prserv) (7003 afs3-vlserv) (7
004 afs3-kaserv) (7005 afs3-volser) (7007 afs3-bos) (7008 afs3-update) (7009 afs3-rmtsys) (
7100 font-servic) (8021 zope-ftp) (8080 http-alt) (8081 tproxy) (8088 omniorb) (8140 puppet
) (8990 clc-build-d) (9098 xinetd) (9101 bacula-dir) (9102 bacula-fd) (9103 bacula-sd) (941
8 git) (9667 xmms2) (9673 zope) (10000 webmin) (10050 zabbix-agen) (10051 zabbix-trap) (100
80 amanda) (10081 kamanda) (10082 amandaidx) (10083 amidxtape) (10809 nbd) (11112 dicom) (1
1371 hkp) (17001 sgi-cmsd) (17002 sgi-crsd) (17003 sgi-gcd) (17004 sgi-cad) (17500 db-lsp)
(22125 dcap) (22128 gsidcap) (22273 wnn6) (24554 binkp) (27374 asp) (30865 csync2) (57000 d
ircproxy) (60177 tfido) (60179 fido)
```

nc -nvz <IP target> 1-1024

```
C:\home\kali> sudo nc -nvz 192.168.50.101 1-1024
(UNKNOWN) [192.168.50.101] 514 (shell) open
(UNKNOWN) [192.168.50.101] 513 (login) open
(UNKNOWN) [192.168.50.101] 512 (exec) open
(UNKNOWN) [192.168.50.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.50.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.50.101] 111 (sunrpc) open
(UNKNOWN) [192.168.50.101] 80 (http) open
(UNKNOWN) [192.168.50.101] 53 (domain) open
(UNKNOWN) [192.168.50.101] 25 (smtp) open
(UNKNOWN) [192.168.50.101] 23 (telnet) open
(UNKNOWN) [192.168.50.101] 22 (ssh) open
(UNKNOWN) [192.168.50.101] 21 (ftp) open
```

netcat (nc), è uno strumento di rete usato per varie operazioni, come trasferimenti di dati o debug di reti.
1-1024 indica che netcat testerà le porte dalla 1 alla 1024 su **<target>**

nc -nv <IP target> <n. porta>

```
C:\home\kali> sudo nc -nv 192.168.50.101 22
[sudo] password for kali:
(UNKNOWN) [192.168.50.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

netcat (**nc**) in questo caso tenta di connettersi alla porta **22** su **<target>**, che di solito è utilizzata per il protocollo SSH che indica il nome e la versione del servizio

nmap -sV <IP target>

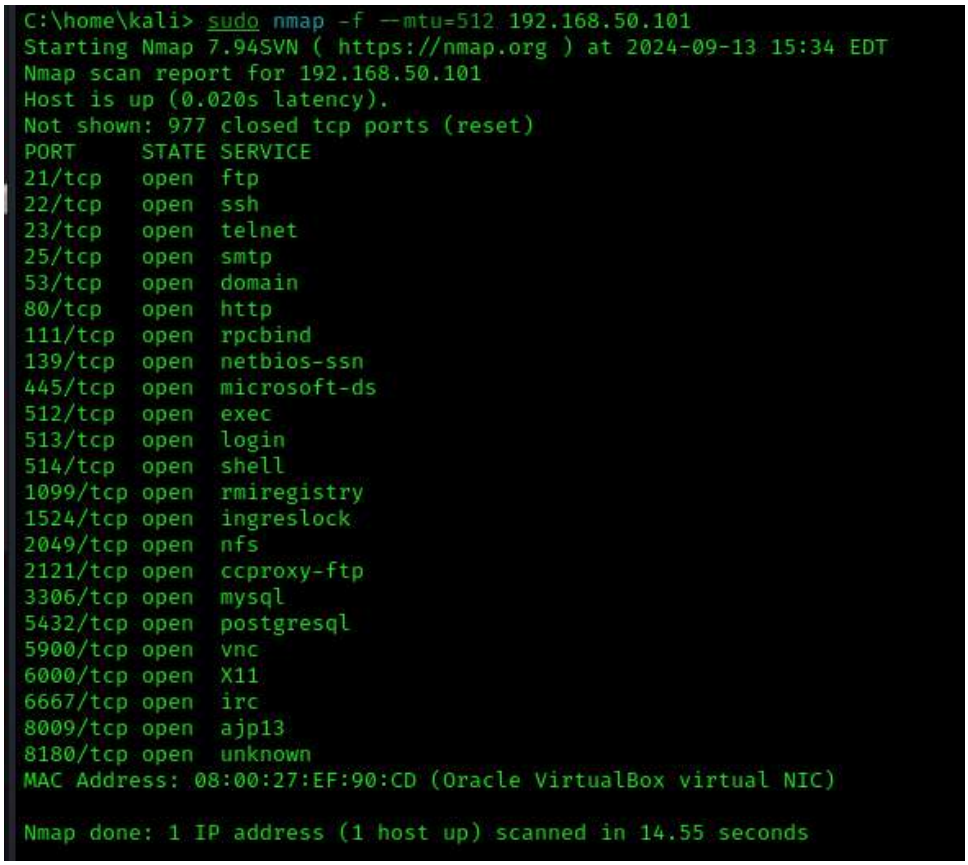
```
C:\home\kali> sudo nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 15:32 EDT
Nmap scan report for 192.168.50.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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: 08:00:27:EF:90:CD (Oracle VirtualBox virtual NIC)
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 67.86 seconds
```

Esegue una scansione delle porte aperte con Nmap.

- **-sV** cerca di determinare quale servizio (e la versione del software) è in esecuzione su una porta

aperta del bersaglio **<target>**.

nmap -f --mtu=512 <IP target>



- Con il flag **-f** Nmap l'header TCP viene suddiviso in piccoli frammenti su più pacchetti IP. Una tecnica usata a volte per eludere i firewall o i sistemi di rilevamento intrusioni.
- **--mtu=512** imposta la dimensione massima dell'unità di trasmissione a 512 byte per pacchetto. È un altro modo per manipolare la trasmissione dei pacchetti