



ESERCIZIO W10D4

INFO GATHERING

Mungiovì Fabio

TASKS

<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

Facoltativo:

Utilizzare tutti i tool proposti ed approfondire lo studio dei metodi di evasione firewall con Nmap:

<https://nmap.org/book/firewall-subversion.html>

<https://nmap.org/book/man-bypass-firewalls-ids.html>

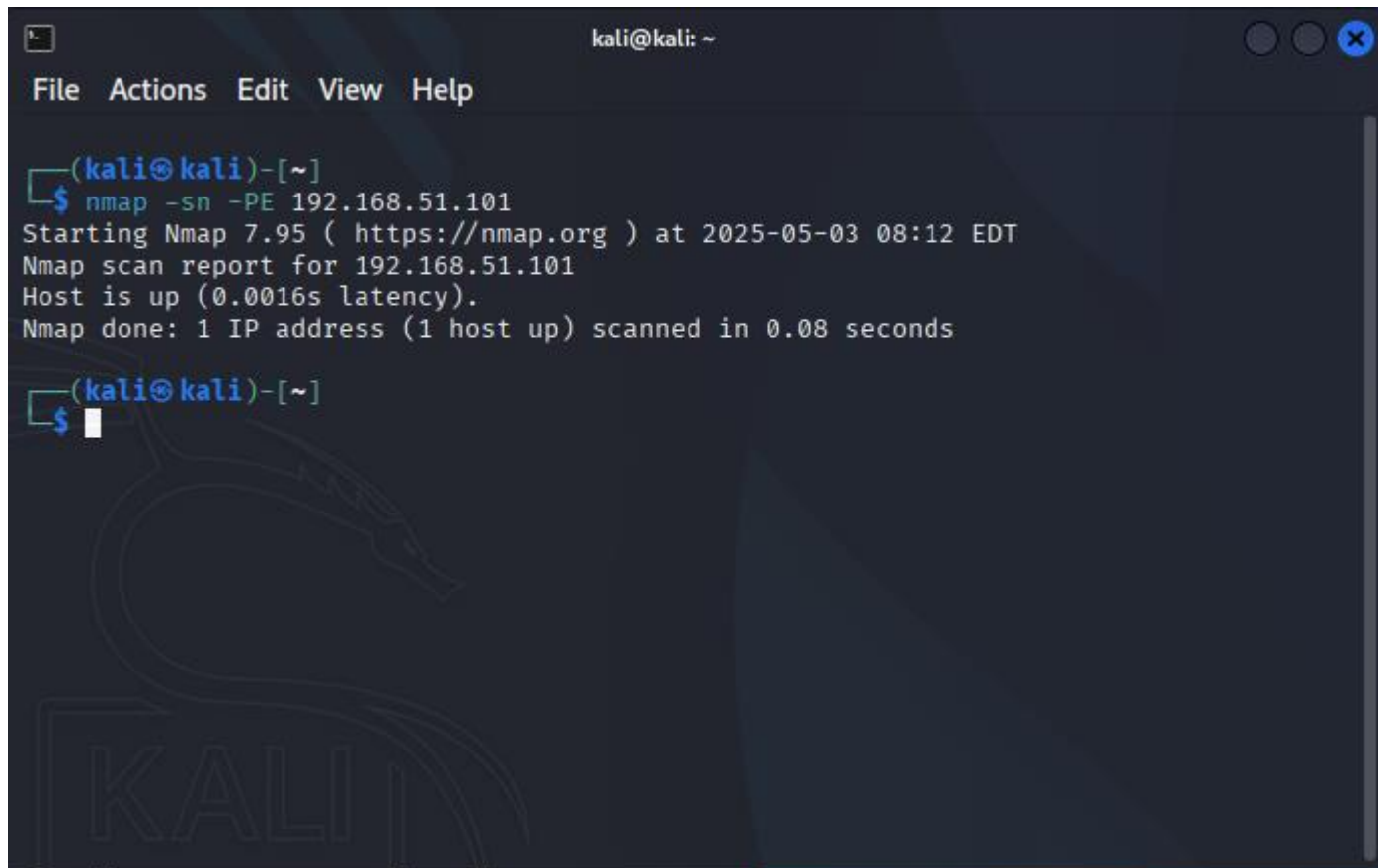
#1 `nmap -sn -PE <target>`

Questo comando utilizza nmap per effettuare una scansione di tipo "ping" su un target, verificando se l'host è attivo senza effettuare una scansione delle porte.

- `-sn` Esegue solo una scansione di tipo "host discovery" (ping scan), senza controllare le porte aperte. Serve per identificare quali host sono attivi nella rete.
- `-PE` Invia pacchetti ICMP Echo Request (simili a quelli usati dal comando ping) per verificare se il target risponde.

Utilizzo:

Questo comando è utile per identificare dispositivi attivi in una rete senza attirare troppa attenzione. È una scansione leggera che non genera traffico invasivo.



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sn -PE 192.168.51.101  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 08:12 EDT  
Nmap scan report for 192.168.51.101  
Host is up (0.0016s latency).  
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds  
(kali@kali)-[~]  
$
```

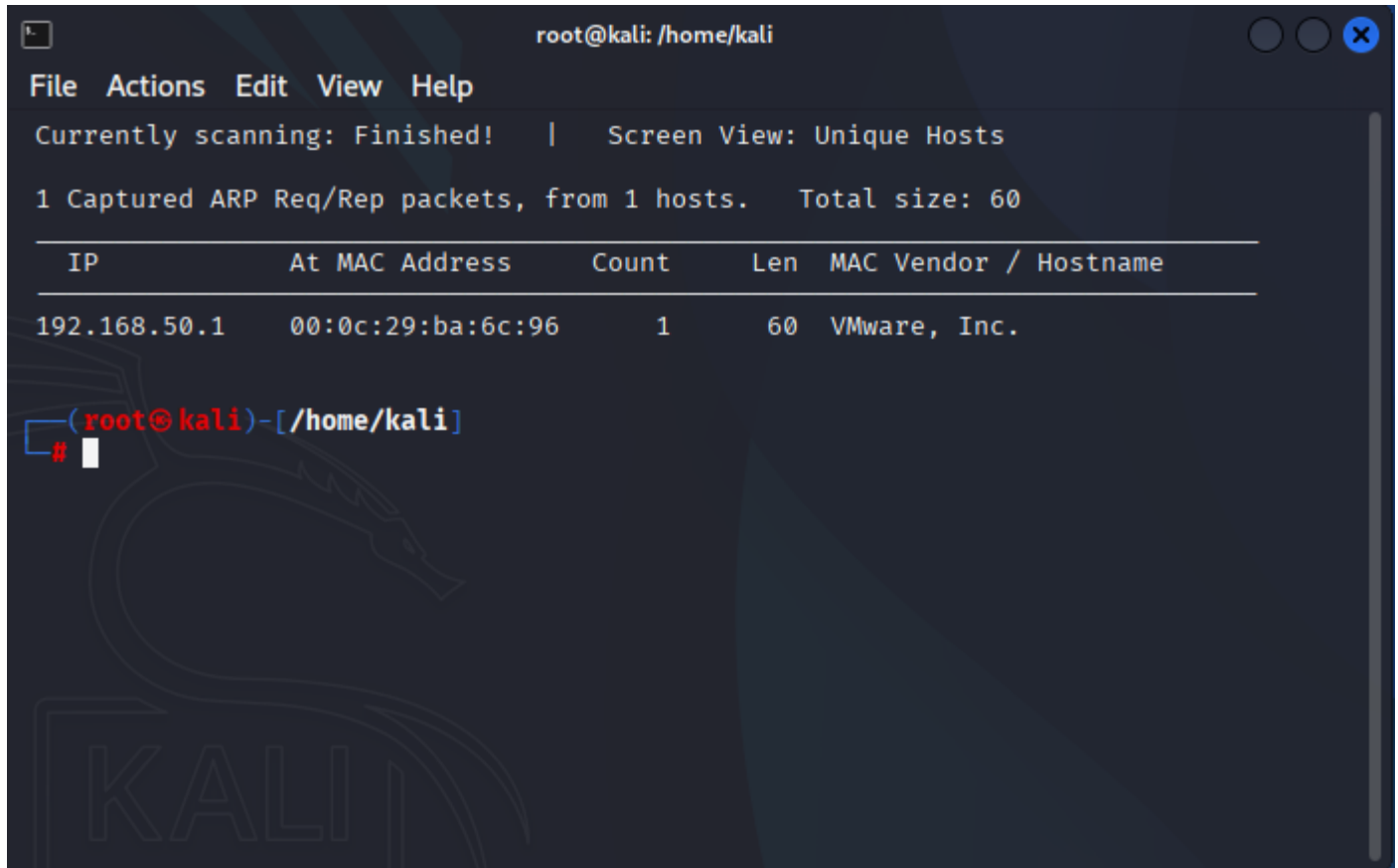
#2 netdiscover -r <target>

Netdiscover è uno strumento di analisi della rete che rileva dispositivi attivi e i loro indirizzi MAC.

-r Specifica l'intervallo di rete da scansione, ad esempio 192.168.1.0/24.

Utilizzo:

Questo comando è utile per scoprire dispositivi attivi in una rete locale e ottenere informazioni sugli indirizzi IP e MAC. È spesso usato per il riconoscimento iniziale di una rete.



```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+
| 192.168.50.1 | 00:0c:29:ba:6c:96 | 1     | 60  | VMware, Inc.          |
+-----+-----+-----+-----+-----+
(root@kali)-[/home/kali]
#
```

#3 crackmapexec <target>

CrackMapExec è uno strumento versatile per test di sicurezza sulle reti Windows.

<target>: Specifica l'indirizzo IP o l'intervallo di rete su cui eseguire il test.

Utilizzo:

Usato per verificare credenziali di autenticazione, enumerare utenti, condivisioni di rete e vulnerabilità su sistemi Windows. Non ci sono opzioni specificate, quindi il comando esegue un'analisi di base.

```
root@kali: /home/kali
File Actions Edit View Help
me
Version : 5.4.0
Codename: Indestructible G0thm0g

options:
-h, --help          show this help message and exit
-t THREADS          set how many concurrent threads to use (default: 100)
--timeout TIMEOUT   max timeout in seconds of each thread (default: None)
--jitter INTERVAL   sets a random delay between each connection (default: None)
--darrell           give Darrell a hand
--verbose           enable verbose output

protocols:
available protocols
{winrm,smb,ldap,rdp,mssql,ssh,ftp}
winrm      own stuff using WINRM
smb        own stuff using SMB
ldap       own stuff using LDAP
rdp        own stuff using RDP
mssql      own stuff using MSSQL
ssh        own stuff using SSH
ftp        own stuff using FTP

(root@kali)-[/home/kali]
# crackmapexec smb 192.168.51.101
SMB 192.168.51.101 445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signin
g:False) (SMBv1:True)

(root@kali)-[/home/kali]
#
```

#4 `nmap <target> --top-ports 10 --open`

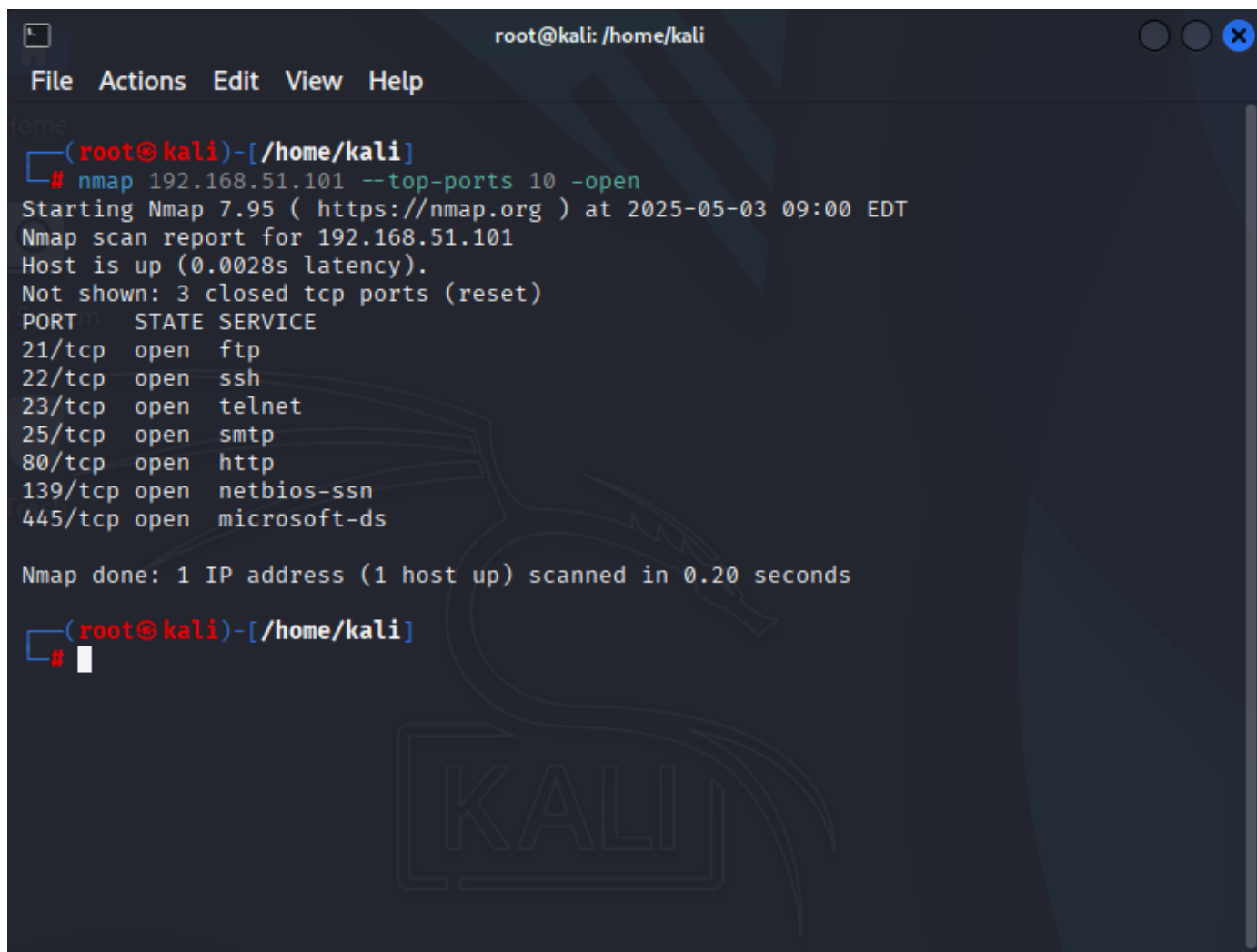
Questo comando utilizza nmap per scansionare le 10 porte più comuni su un target e mostra solo quelle aperte.

`--top-ports 10` Scansiona le 10 porte più frequentemente utilizzate (basato su statistiche di utilizzo globale).

`--open` Mostra solo le porte che risultano aperte.

Utilizzo:

È utile per una scansione rapida delle porte più comuni, ad esempio per identificare servizi come HTTP (porta 80) o SSH (porta 22).

A terminal window titled 'root@kali: /home/kali' showing the execution of an nmap command. The command is '# nmap 192.168.51.101 --top-ports 10 -open'. The output shows the scan starting at 2025-05-03 09:00 EDT, reporting that the host is up with a latency of 0.0028s. It lists 10 open ports with their corresponding services: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 80/tcp (http), 139/tcp (netbios-ssn), and 445/tcp (microsoft-ds). The scan took 0.20 seconds to complete. The terminal has a dark background with a faint 'KALI' logo watermark.

```
root@kali: /home/kali
File Actions Edit View Help
root@kali)~[/home/kali]
# nmap 192.168.51.101 --top-ports 10 -open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 09:00 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0028s 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

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali)~[/home/kali]
#
```

#5 `nmap <target> -p- -sV --reason --dns-server ns`

Questo comando esegue una scansione completa su tutte le porte e raccoglie informazioni dettagliate sui servizi.

<code>-p-</code>	Scansiona tutte le 65535 porte (dalla 1 alla 65535).
<code>-sV</code>	Identifica i servizi in esecuzione e le loro versioni.
<code>--reason</code>	Mostra il motivo per cui nmap classifica una porta come aperta, chiusa o filtrata (ad esempio, in base alla risposta ricevuta).
<code>--dns-server ns</code>	Specifica un server DNS personalizzato da utilizzare per le richieste di risoluzione dei nomi.

Utilizzo:

Questo comando è utile per un'analisi approfondita di un host, inclusa la scoperta di servizi in esecuzione e la raccolta di informazioni DNS.

```
root@kali: /home/kali
File Actions Edit View Help
ome
(root@kali)-[/home/kali]
# nmap 192.168.51.101 -p- -sV --reason --dns-server ns
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 09:18 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
using --system-dns or specify valid servers with --dns-servers
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 20.00% done; ETC: 09:19 (0:00:24 remaining)
Nmap scan report for 192.168.51.101
Host is up, received echo-reply ttl 63 (0.0047s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 63  vsftpd 2.3.4
22/tcp    open  ssh          syn-ack ttl 63  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2
.0)
23/tcp    open  telnet       syn-ack ttl 63  Linux telnetd
25/tcp    open  smtp         syn-ack ttl 63  Postfix smtpd
53/tcp    open  domain       syn-ack ttl 63  ISC BIND 9.4.2
80/tcp    open  http         syn-ack ttl 63  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      syn-ack ttl 63  2 (RPC #100000)
139/tcp   open  netbios-ssn  syn-ack ttl 63  Samba smbd 3.X - 4.X (workgroup: WORKGROU
P)
445/tcp   open  netbios-ssn  syn-ack ttl 63  Samba smbd 3.X - 4.X (workgroup: WORKGROU
P)
512/tcp   open  exec         syn-ack ttl 63  netkit-rsh rexecd
513/tcp   open  login?       syn-ack ttl 63
514/tcp   open  shell        syn-ack ttl 63  Netkit rshd
1099/tcp  open  java-rmi     syn-ack ttl 63  GNU Classpath grmiregistry
1524/tcp  open  bindshell    syn-ack ttl 63  Metasploitable root shell
2049/tcp  open  nfs          syn-ack ttl 63  2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp? syn-ack ttl 63
3306/tcp  open  mysql        syn-ack ttl 63  MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd      syn-ack ttl 63  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ub
untu4))
5432/tcp  open  postgresql   syn-ack ttl 63  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          syn-ack ttl 63  VNC (protocol 3.3)
6000/tcp  open  X11          syn-ack ttl 63  (access denied)
6667/tcp  open  irc          syn-ack ttl 63  UnrealIRCd
6697/tcp  open  irc          syn-ack ttl 63  UnrealIRCd
8009/tcp  open  ajp13        syn-ack ttl 63  Apache Jserv (Protocol v1.3)
8180/tcp  open  http         syn-ack ttl 63  Apache Tomcat/Coyote JSP engine 1.1
```

#6 `us -mT -Iv <target>:a -r 3000 -R 3 && us -mU -Iv<target>:a -r 3000`

Unicornsscan è un nuovo motore di raccolta e correlazione delle informazioni costruito per e da membri delle comunità di ricerca e test sulla sicurezza.

È stato progettato per fornire un motore scalabile, accurato, flessibile ed efficiente.

Unicornsscan per impostazione predefinita esegue una scansione TCP/UDP, a differenza di nmap.

Supponiamo di voler scansionare il nostro IP cercando tutte le porte e inviando 3000 pacchetti al secondo; potremmo scrivere

- mU Specifica un test UDP.
- Iv Modalità verbose (dettagliata).
- r 3000 Imposta la velocità di invio dei pacchetti a 3000 al secondo.
- R 3 Ripete il test tre volte.
- && Esegue il secondo comando solo se il primo ha successo.

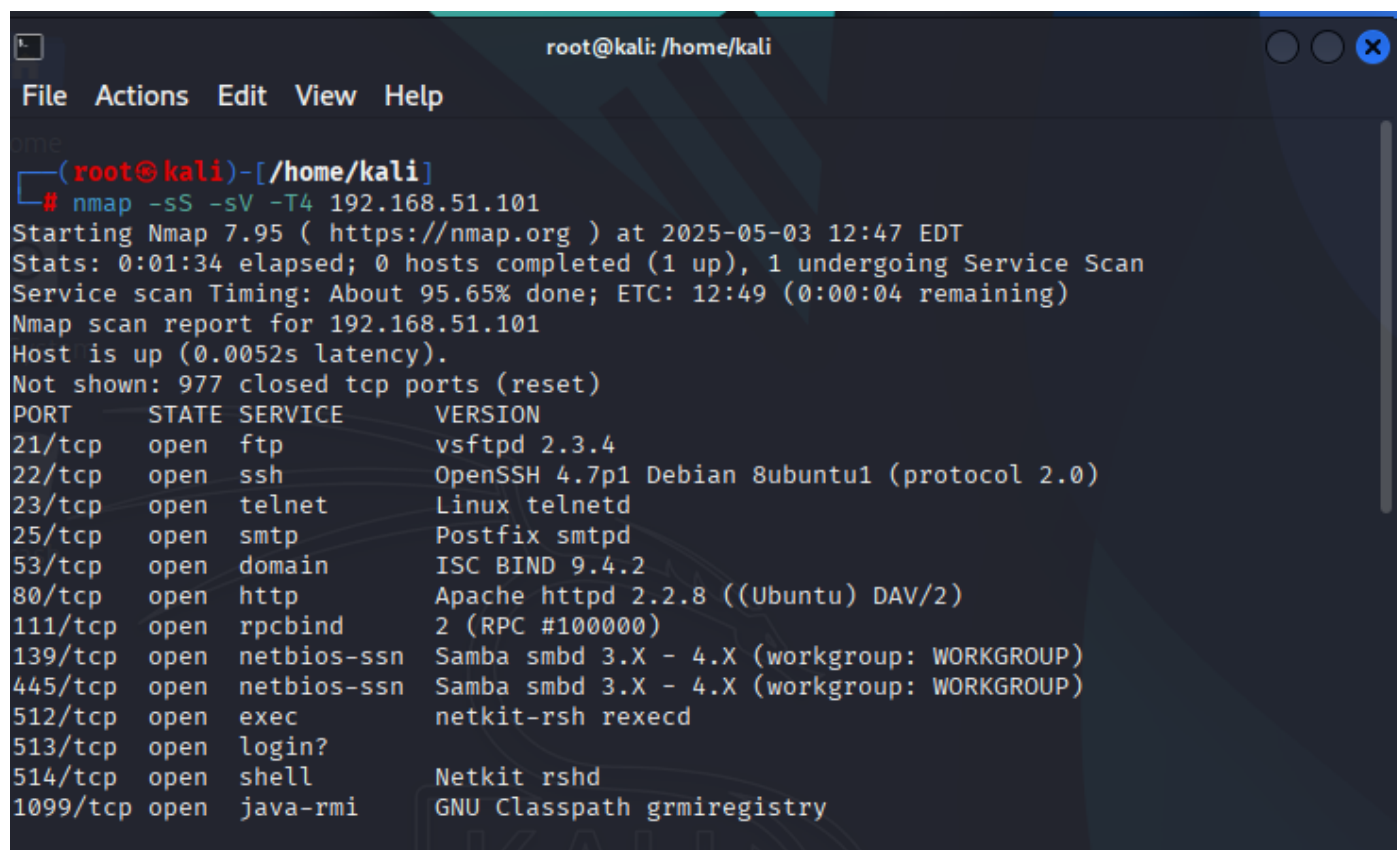
#7 `nmap -sS -sV -T4 <target>`

Questo comando utilizza nmap per una scansione SYN rapida e dettagliata.

- `-sS` Effettua una scansione SYN (stealth), che invia pacchetti SYN senza completare la connessione TCP. È più veloce e meno rilevabile rispetto a una scansione completa.
- `-sV` Identifica i servizi in esecuzione e le loro versioni.
- `-T4` Imposta un livello di velocità elevato (T4 è "aggressivo", bilanciando velocità e accuratezza).

Utilizzo:

Ideale per una scansione rapida e dettagliata di un target, utile per ottenere informazioni sui servizi in esecuzione.



```
root@kali: /home/kali
File Actions Edit View Help
me
(root@kali)-[/home/kali]
# nmap -sS -sV -T4 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 12:47 EDT
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 12:49 (0:00:04 remaining)
Nmap scan report for 192.168.51.101
Host is up (0.0052s 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
```


#8 hping3 --scan known <target>

Hping3 è uno strumento per l'invio di pacchetti TCP/IP personalizzati.

`--scan known` Scansiona le porte conosciute (cioè le porte più comuni) sul target.

Utilizzo:

Questo comando è utile per una scansione mirata delle porte più utilizzate, con maggiore personalizzazione rispetto a nmap.

```
root@kali: /home/kali
File Actions Edit View Help
ome
(root@kali)-[/home/kali]
# hping3 --scan known 192.168.51.101
Scanning 192.168.51.101 (192.168.51.101), port known
266 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 systa
) (13 daytime) (15 netstat) (17 qotd) (19 chargen) (20 ftp-data) (21 ftp) (22 ssh) (23 t
lnet) (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 netbi
s-ns) (138 netbios-dgm) (139 netbios-ssn) (143 imap2) (161 snmp) (162 snmp-trap) (163 cm
p-man) (164 cmip-agent) (174 mailq) (177 xdmcp) (179 bgp) (199 smux) (209 qmtp) (210 z39
0) (213 ipx) (319 ptp-event) (320 ptp-general) (345 pawserv) (346 zserv) (369 rpc2portma
) (370 codauth2) (371 clearcase) (389 ldap) (427 svrloc) (443 https) (444 snpp) (445 mi
rosoft-d) (464 kpasswd) (465 submissions) (487 saft) (500 isakmp) (512 exec) (513 login)
(514 shell) (515 printer) (517 talk) (518 ntalk) (520 route) (538 gdomap) (540 uucp) (54
klogin) (544 kshell) (546 dhcpv6-clie) (547 dhcpv6-serv) (548 afpovertcp) (554 rtsp) (5
3 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 pass
d-serv) (754 krb-prop) (775 moira-db) (777 moira-updat) (779 moira-ureg) (783 spamd) (85
domain-s) (871 supfilesrv) (873 rsync) (989 ftps-data) (990 ftps) (992 telnets) (993 im
ps) (995 pop3s) (1080 socks) (1093 proofd) (1094 rootd) (1099 rmiregistry) (1127 supfile
bg) (1178 skkserv) (1194 openvpn) (1210 predict) (1236 rmtcfg) (1313 xtel) (1314 xtelw)
```

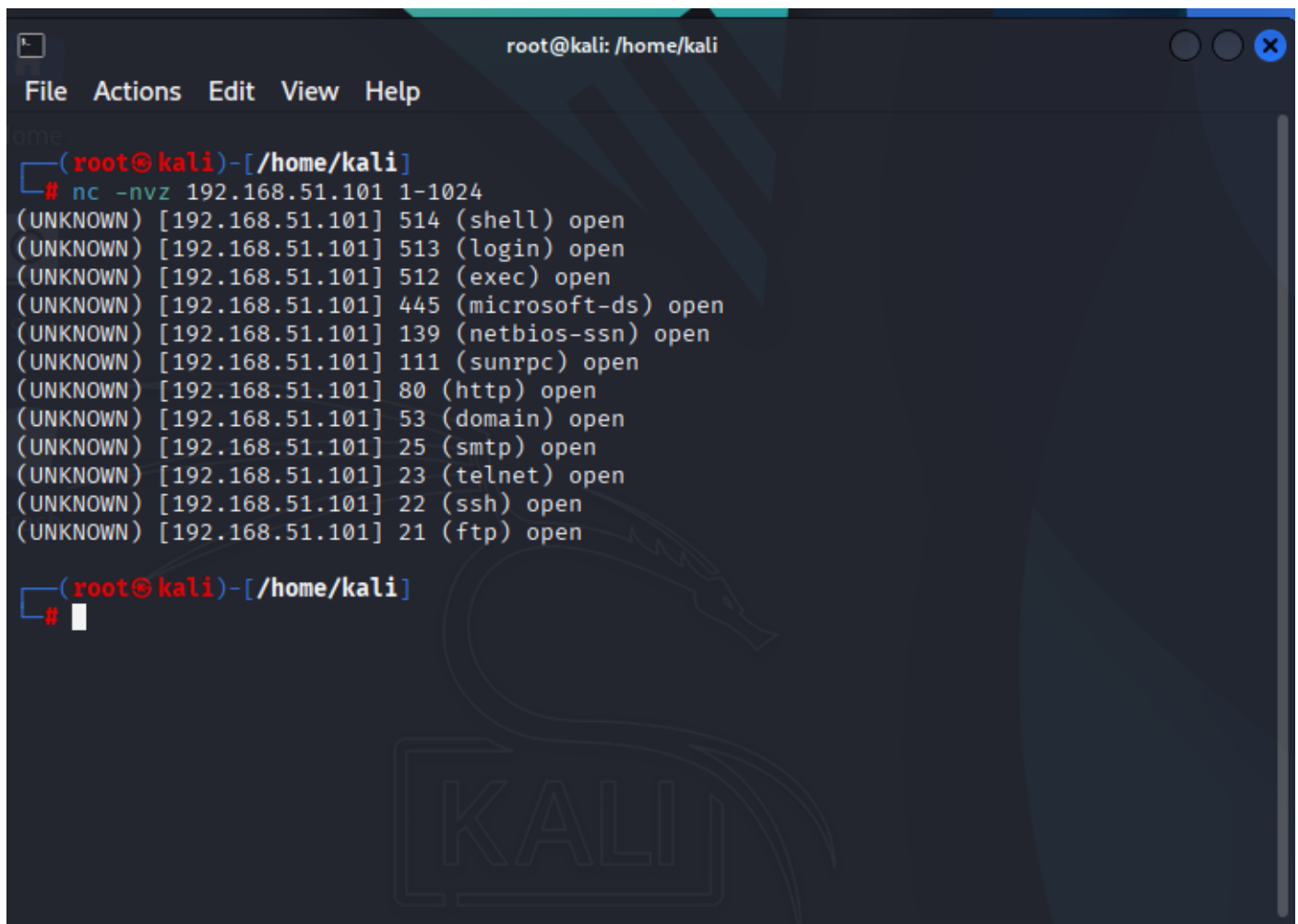
#9 `nc -nvz <target> 1-1024`

Netcat è uno strumento per la scansione e la comunicazione di rete.

- n: Non risolve i nomi DNS (usa solo indirizzi IP).
- v: Modalità verbose (mostra più dettagli).
- z: Modalità "zero I/O", verifica solo se le porte sono aperte senza inviare dati.
- 1-1024: Specifica l'intervallo di porte da scansionare (dalla 1 alla 1024).

Utilizzo:

È utile per una scansione rapida delle porte più comuni (1-1024), spesso utilizzate da servizi standard.



```
root@kali: /home/kali
File Actions Edit View Help
me
(root@kali)-[/home/kali]
# nc -nvz 192.168.51.101 1-1024
(UNKNOWN) [192.168.51.101] 514 (shell) open
(UNKNOWN) [192.168.51.101] 513 (login) open
(UNKNOWN) [192.168.51.101] 512 (exec) open
(UNKNOWN) [192.168.51.101] 445 (microsoft-ds) open
(UNKNOWN) [192.168.51.101] 139 (netbios-ssn) open
(UNKNOWN) [192.168.51.101] 111 (sunrpc) open
(UNKNOWN) [192.168.51.101] 80 (http) open
(UNKNOWN) [192.168.51.101] 53 (domain) open
(UNKNOWN) [192.168.51.101] 25 (smtp) open
(UNKNOWN) [192.168.51.101] 23 (telnet) open
(UNKNOWN) [192.168.51.101] 22 (ssh) open
(UNKNOWN) [192.168.51.101] 21 (ftp) open
(root@kali)-[/home/kali]
#
```

#10 `nc -nv <target> 22`

Questo comando utilizza netcat per testare una connessione alla porta 22 (SSH).

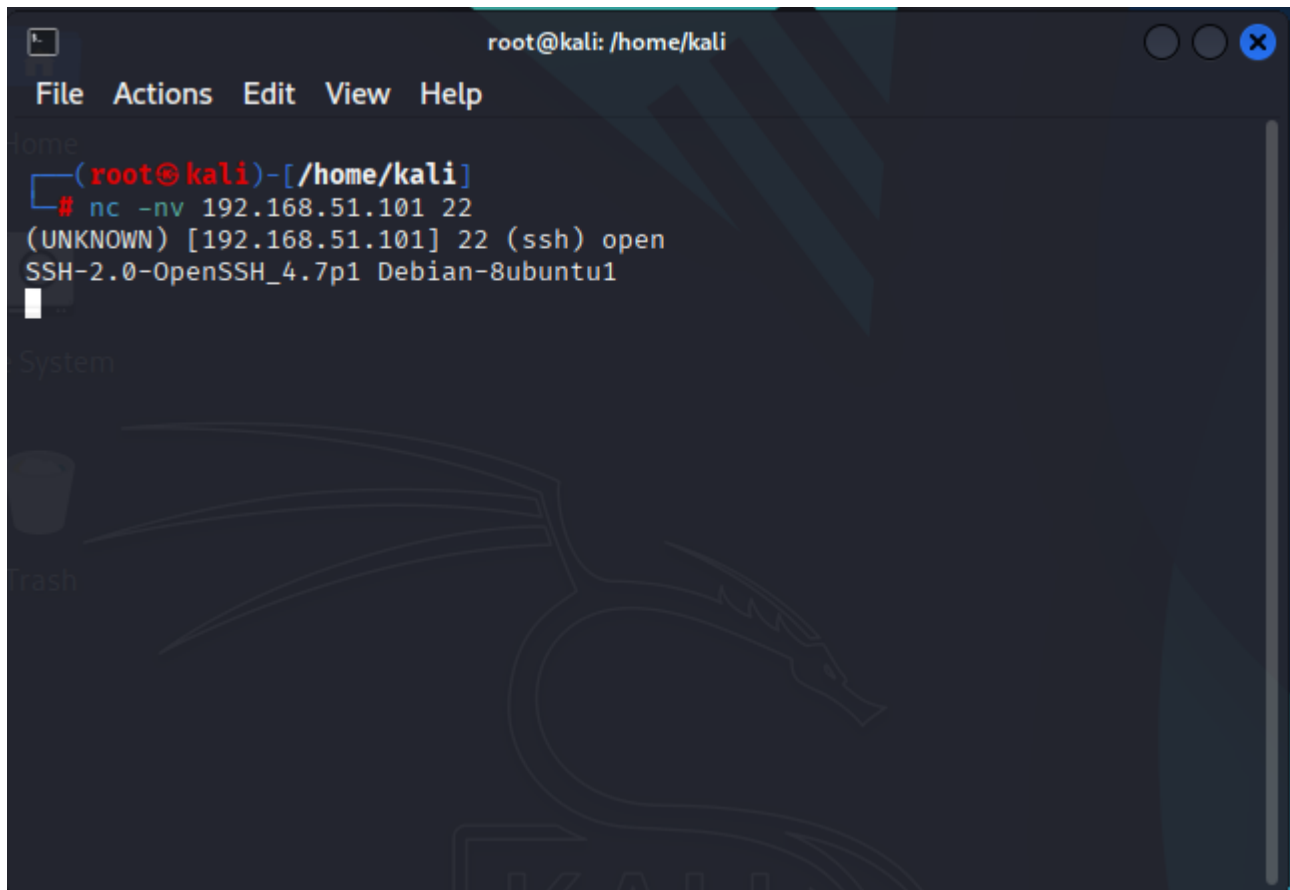
-n Non risolve i nomi DNS.

-v Modalità verbose.

22 Specifica la porta da testare (SSH).

Utilizzo:

È utile per verificare se un servizio SSH è attivo su un target.



The screenshot shows a terminal window titled "root@kali: /home/kali". The terminal output is as follows:

```
(root@kali)-[/home/kali]
# nc -nv 192.168.51.101 22
(UNKNOWN) [192.168.51.101] 22 (ssh) open
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

The terminal window has a menu bar with "File", "Actions", "Edit", "View", and "Help". The background of the terminal window features a faint, stylized dragon logo.

#11 `nmap -sV <target>`

Questo comando utilizza nmap per identificare i servizi in esecuzione.

`-sV` Rileva i servizi in esecuzione e le loro versioni.

Utilizzo:

Ideale per ottenere informazioni dettagliate sui servizi in esecuzione su un target.

```
root@kali: /home/kali
File Actions Edit View Help
ome
(root@kali)-[/home/kali]
# nmap -sV 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 13:01 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0061s 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 rshd
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)
```

#12 db_import <file.xml>

Questo comando importa un file XML (ad esempio, risultati di nmap) nel database di Metasploit Framework.

Utilizzo:

Permette di analizzare i risultati delle scansioni direttamente in Metasploit per pianificare exploit o attacchi successivi.

#13 nmap -f -mtu=512 <target>

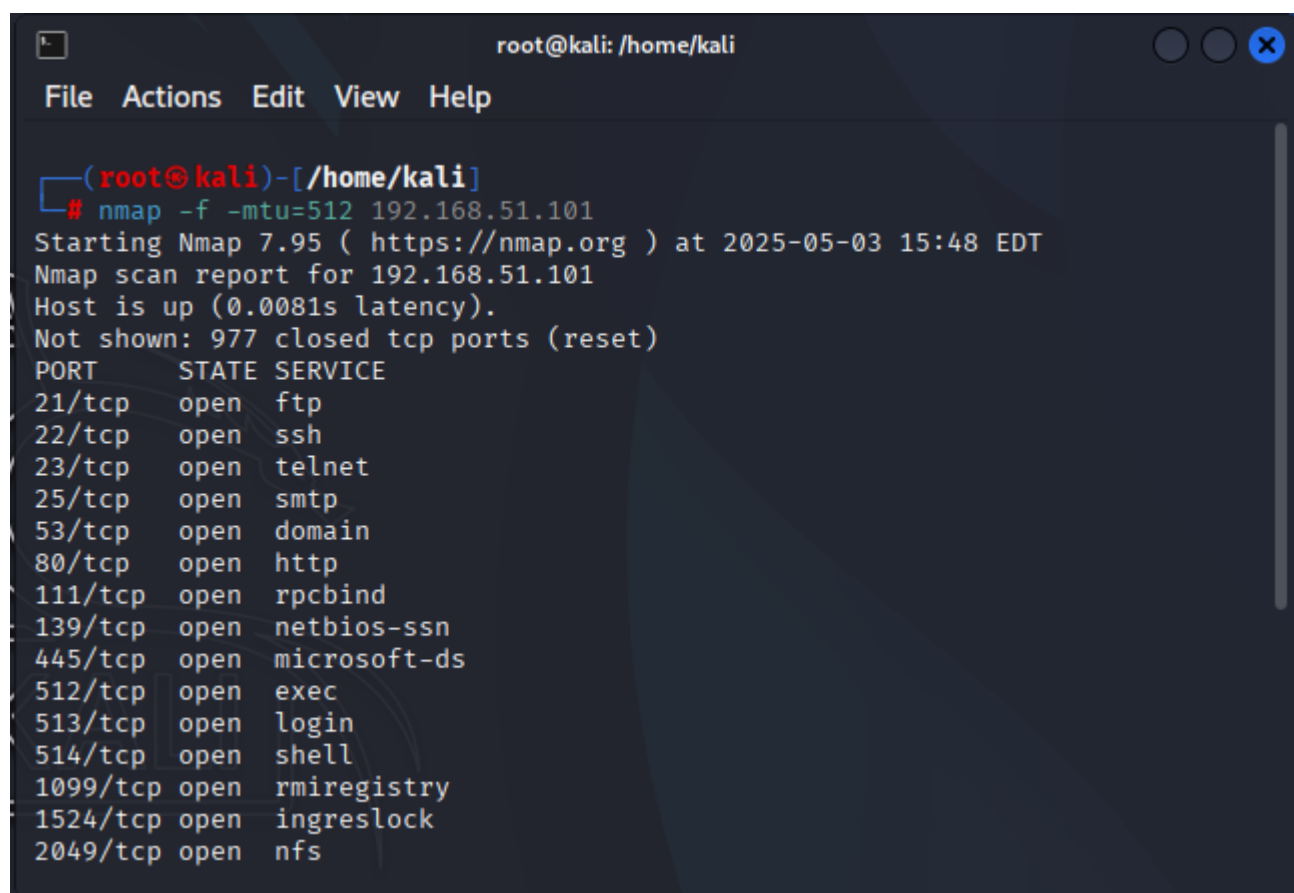
Questo comando utilizza nmap per eseguire una scansione frammentata.

-f Frammenta i pacchetti in segmenti più piccoli per aggirare firewall o IDS.

-mtu=512 Imposta la dimensione massima del pacchetto a 512 byte.

Utilizzo:

È utile per eludere sistemi di rilevamento o firewall che analizzano pacchetti di dimensioni standard.



The screenshot shows a terminal window titled 'root@kali: /home/kali'. The terminal displays the command `# nmap -f -mtu=512 192.168.51.101` and its output. The output indicates that the host is up and lists several open ports with their corresponding services.

```
(root@kali)-[/home/kali]
# nmap -f -mtu=512 192.168.51.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 15:48 EDT
Nmap scan report for 192.168.51.101
Host is up (0.0081s 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
```

#14 `masscan <network> -p80 --banners --source-ip <target>`

Masscan è uno strumento estremamente veloce per la scansione delle porte.

`<network>` Specifica la rete da scansionare (es. 192.168.1.0/24).

`-p80` Scansiona la porta 80 (HTTP).

`--banners` Raccoglie i banner dei servizi, fornendo informazioni sui software in esecuzione.

`--source-ip <target>` Specifica un indirizzo IP sorgente personalizzato.

Utilizzo:

Ideale per una scansione rapida di grandi reti, raccogliendo informazioni sui servizi in esecuzione.

Bypassing Firewall Rules

<https://nmap.org/book/firewall-subversion.html>

L'articolo analizza diverse tecniche avanzate per bypassare firewall e sistemi di rilevamento delle intrusioni utilizzando **Nmap**, uno strumento di scansione delle reti.

Viene spiegato come sfruttare configurazioni errate nei sistemi di sicurezza e come utilizzare scansioni specializzate per ottenere informazioni sulle reti protette. Di seguito, vengono descritte le principali tecniche e i comandi associati.

Tecniche di scansione avanzate

Nmap offre diversi tipi di scansione per aggirare i firewall:

- Scansione FIN
Invio di pacchetti FIN per superare regole che bloccano i pacchetti SYN. Ad esempio:

```
nmap -sF -p1-100 -T4 <target>
```

Questo comando invia pacchetti FIN per individuare porte aperte o filtrate.

- Manipolazione delle porte sorgente
Alcuni firewall si fidano del traffico basandosi solo sul numero di porta sorgente. È possibile sfruttare questa vulnerabilità con il comando:

```
nmap -sS -Pn -g 88 <target>
```

Qui, Nmap invia pacchetti con porta sorgente 88, sfruttando una configurazione errata nei filtri di Windows IPsec.

Scansioni IPv6

Molti sistemi non configurano correttamente i filtri per IPv6. Utilizzando l'opzione `-6`, è possibile effettuare scansioni IPv6:

```
nmap -6 www.target.com
```

Questo comando può rivelare servizi accessibili via IPv6 che potrebbero essere bloccati su IPv4.

Idle Scan (scansione stealth)

La scansione *Idle IP ID* permette di dedurre porte aperte senza inviare pacchetti direttamente dall'indirizzo reale dell'attaccante. Si utilizza un host "zombie" per generare pacchetti:

```
nmap -sI zombie_ip:port -p target_port <target>
```

Questa tecnica è utile per rimanere invisibili, ma richiede zombie con sequenze IP ID prevedibili.

Frammentazione dei pacchetti

Alcuni firewall non gestiscono correttamente i pacchetti frammentati. Con Nmap è possibile frammentare i pacchetti per aggirare i filtri:

```
nmap -f <target>
```

Ogni opzione `-f` aggiunge 8 byte ai frammenti, oppure si può specificare la dimensione con `--mtu`.

Routing sorgente

Il routing sorgente consente di specificare percorsi personalizzati per aggirare router che bloccano il traffico. Ad esempio:

```
nmap -n -sn -PE --ip-options "L hop_ip" <target>
```

Questo comando invia pacchetti instradati attraverso un hop specifico per raggiungere reti altrimenti inaccessibili.

Proxy e spoofing MAC

- Proxy
I proxy mal configurati possono essere sfruttati per accedere anonimamente a risorse interne. Sebbene Nmap non supporti direttamente la scansione tramite proxy, esistono strumenti dedicati.
- Spoofing MAC
Per ingannare i sistemi di autenticazione basati su MAC, si può usare l'opzione:

```
nmap --spoof-mac vendor <target>
```

Ad esempio, `--spoof-mac Apple` utilizza un MAC casuale con prefisso Apple.

Scansione FTP Bounce

La tecnica FTP Bounce sfrutta server FTP vulnerabili per scansionare altre reti:

```
nmap -p 22,25,135 -Pn -v -b ftp_server <target>
```

Questa tecnica è utile per superare firewall e accedere a reti interne.

Caso reale

Un esempio pratico descritto nell'articolo mostra come un team di penetration testing abbia combinato diverse tecniche per accedere a una rete protetta. Dopo aver trovato un file server con porta 445 aperta, hanno utilizzato il routing sorgente per raggiungere una subnet bloccata. Successivamente, hanno eseguito una scansione SYN:

```
nmap -vv -n -sS -Pn --ip-options "L hop_ip" target
```

Questo ha permesso loro di identificare porte aperte e accedere alla rete protetta.

Conclusione

L'articolo sottolinea l'importanza di provare diverse tecniche per bypassare firewall e sistemi di sicurezza. Ogni configurazione errata rappresenta una potenziale vulnerabilità, e strumenti come Nmap offrono un'ampia gamma di opzioni per individuarle e sfruttarle.

Firewall/IDS Evasion and Spoofing

<https://nmap.org/book/man-bypass-firewalls-ids.html>

L'articolo affronta le funzionalità avanzate di Nmap che permettono di aggirare firewall e sistemi di rilevamento delle intrusioni (IDS).

L'obiettivo principale è comprendere e testare la sicurezza delle reti, simulando le tecniche che un attaccante potrebbe adottare.

Si sottolinea come, con l'introduzione dei firewall negli anni '90, la visione di una rete globale e connessa sia stata limitata da filtri e restrizioni, rendendo più complessa la mappatura delle reti. Tuttavia, Nmap offre una serie di strumenti per analizzare e superare queste difese.

Tra le tecniche discusse, troviamo:

Frammentazione dei pacchetti (-f):

questa opzione divide i pacchetti in frammenti molto piccoli, rendendo più difficile per i firewall e gli IDS identificarli. Tuttavia, può creare problemi con alcuni programmi o reti che non gestiscono correttamente i frammenti.

Uso di esche (decoys):

con l'opzione -D, Nmap permette di mascherare l'origine della scansione, facendo sembrare che provenga da più indirizzi IP. Questo confonde i sistemi di rilevamento, che registrano più IP come potenziali responsabili della scansione.

Spoofing dell'indirizzo IP (-S):

Consente di falsificare l'indirizzo sorgente, simulando che un'altra entità stia effettuando la scansione. Questa tecnica, però, rende difficile ricevere risposte utili, poiché i pacchetti di ritorno saranno inviati all'IP falsificato.

Manipolazione delle porte sorgente (--source-port):

sfrutta configurazioni errate nei firewall che si fidano del traffico proveniente da porte specifiche (ad esempio, porta 53 per DNS o porta 20 per FTP).

Aggiunta di dati personalizzati ai pacchetti (--data):

permette di includere stringhe o dati binari nei pacchetti inviati, utili per testare la reazione di sistemi di sicurezza.

Uso di proxy (--proxies):

consente di instradare le connessioni TCP attraverso una catena di proxy, utile per nascondere l'origine della scansione, anche se questa tecnica può rallentare l'operazione.

L'articolo evidenzia anche come gli IDS e i sistemi di prevenzione delle intrusioni (IPS) siano progettati per rilevare scansioni come quelle effettuate da Nmap, poiché spesso rappresentano un preludio a un attacco.

Tuttavia, con pazienza e abilità, un attaccante può eludere questi sistemi, sfruttando le opzioni avanzate offerte da Nmap.

Infine, viene discusso il dibattito sull'uso di tali funzionalità.

Alcuni ritengono che Nmap non dovrebbe includere strumenti per eludere firewall e IDS, ma l'articolo sostiene che queste tecniche sono fondamentali per gli amministratori di rete, che possono usarle per testare e migliorare la sicurezza delle proprie infrastrutture.