S5 L3

Svolgimento Progetto

Giulia Salani

Consegna

Si richiede allo studente di effettuare le seguenti scansioni sul target Metasploitable:
OS fingerprint
Syn Scan
TCP connect - trovate differenze tra i risultati della scansioni TCP connect e SYN?
Version detection

E le seguenti sul target Windows 7:
OS fingerprint

Modificate le impostazioni di rete delle macchine virtuali per fare in modo che i due target siano sulla stessa rete.

A valle delle scansioni, per entrambi gli IP, è prevista la produzione di un report contenente le seguenti info (dove disponibili):
IP
Sistema Operativo
Porte Aperte
Servizi in ascolto con versione

Consegna

Quesito extra (al completamento dei quesiti sopra):

Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

Svolgimento

Kali, Meta, Windows 7 sono tutte sulla stessa rete.

IP Kali: 192.168.32.100

IP Meta: 192.168.32.102

IP Windows 7: 192.168.32.101

L'**OS fingerprinting** è un metodo utilizzato per identificare il sistema operativo in esecuzione su un determinato host di rete. Attraverso l'analisi delle risposte di un dispositivo alle specifiche richieste di rete, come pacchetti di sondaggio, un attaccante o un analista di sicurezza può tentare di determinare il tipo e la versione del sistema operativo del target.

Eseguiamo il comando «nmap -Pn -O 192.168.32.102» da Kali verso Meta.

Questo comando utilizza Nmap per eseguire una scansione OS fingerprinting dell'indirizzo IP 192.168.32.102, saltando la fase di ping e cercando di identificare il sistema operativo del dispositivo.

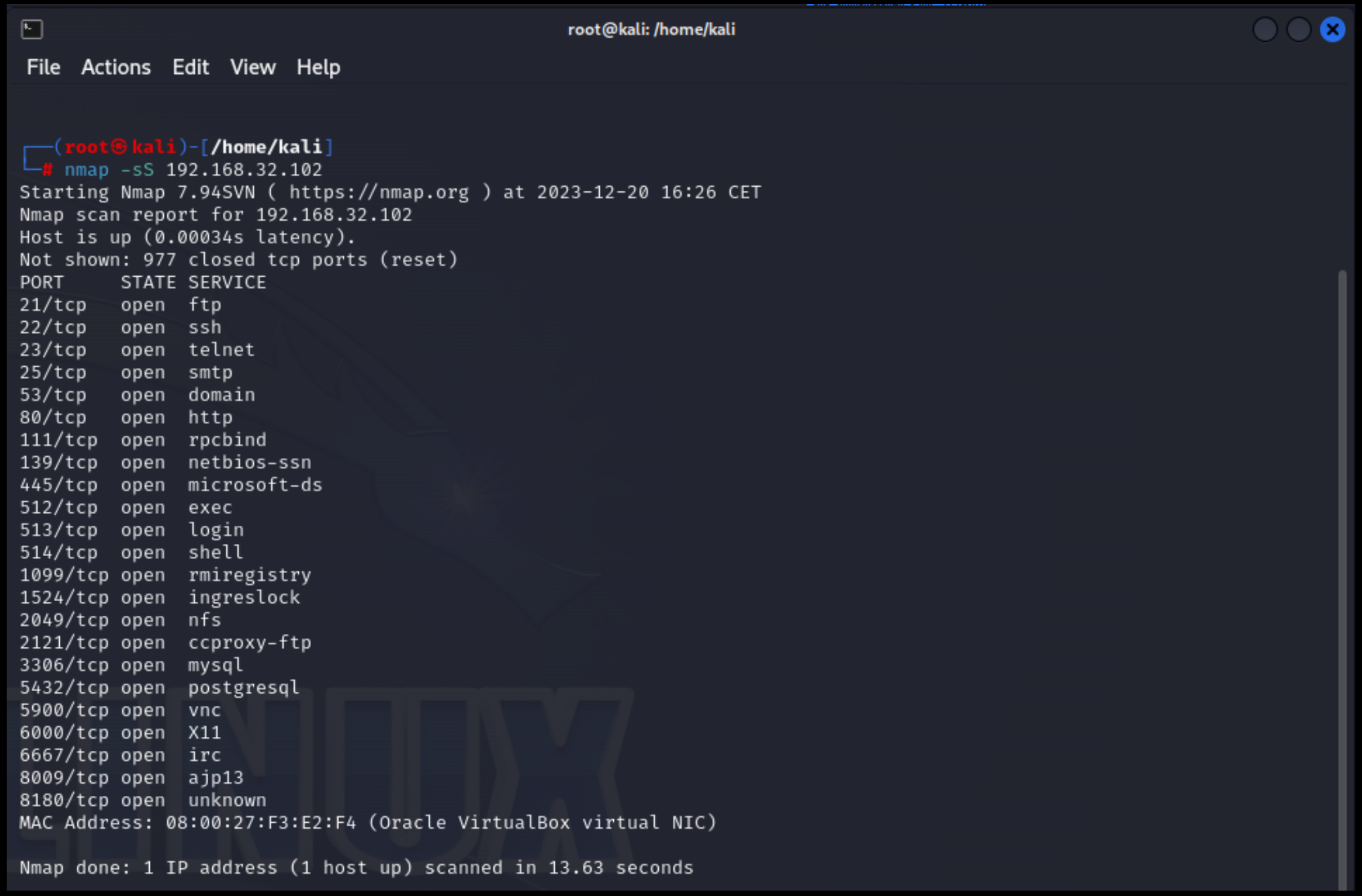
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -O 192.168.32.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 17:35 CET
Nmap scan report for 192.168.32.102
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   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: 08:00:27:F3:E2:F4 (Oracle VirtualBox virtual NIC)
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.05 seconds
```

Una scansione **SYN stealth**, spesso nota come "scansione SYN", è una tecnica di scansione delle porte in cui l'attaccante invia pacchetti SYN ai porti target senza completare la connessione TCP. Questo metodo mira a identificare le porte aperte senza stabilire una connessione completa, rendendo l'approccio più discreto e meno rilevabile rispetto ad altre tecniche di scansione.

Eseguiamo il comando «nmap -sS 192.168.32.102» da Kali verso Meta.

Questo comando utilizza Nmap per eseguire una scansione SYN stealth delle porte sul dispositivo con indirizzo IP 192.168.32.102, cercando di determinare le porte aperte senza completare la connessione TCP.


root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.32.102
Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:26 CET
Nmap scan report for 192.168.32.102
Host is up (0.00034s 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: 08:00:27:F3:E2:F4 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.63 seconds

La scansione TCP Connect è una tecnica di scansione delle porte utilizzata da Nmap e altri strumenti di rete. In questa tecnica, l'attaccante (o l'analista) tenta di stabilire una connessione TCP completa con la porta target. Se la connessione è stabilita con successo, la porta viene considerata aperta; altrimenti, viene considerata chiusa o filtrata, a seconda della risposta ricevuta. Questo metodo è meno discreto rispetto alle tecniche di scansione stealth come la scansione SYN, poiché stabilisce effettivamente una connessione con le porte target.

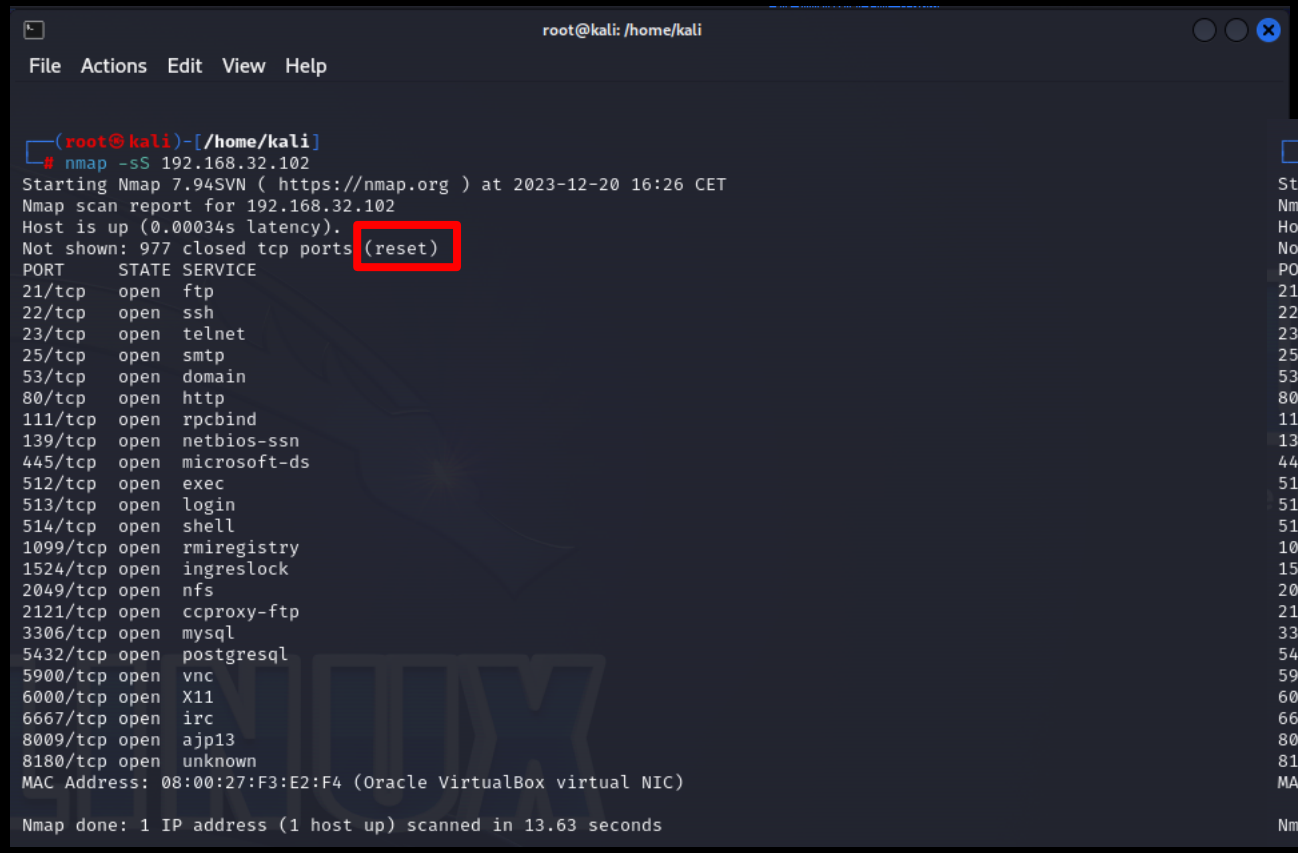
Eseguiamo il comando «nmap –sT 192.168.32.102» da Kali verso Meta.

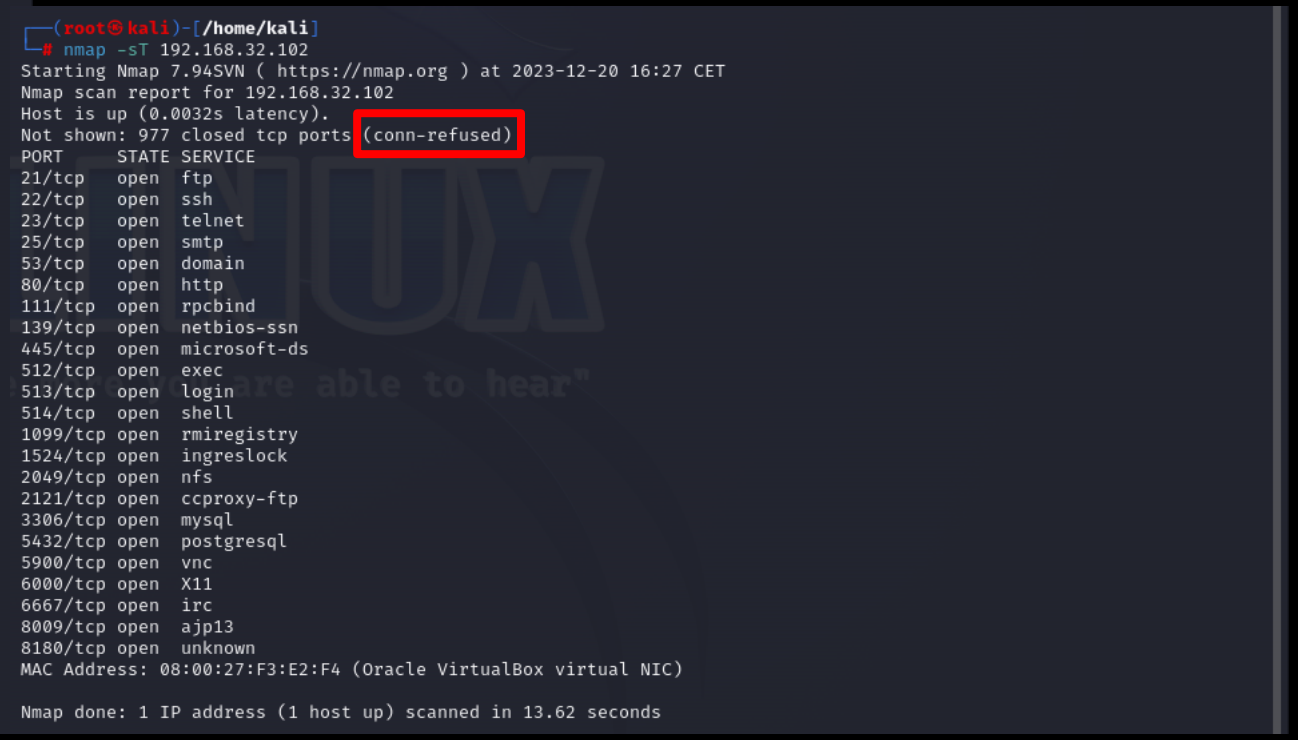
Questo comando utilizza Nmap per eseguire una scansione delle porte utilizzando la tecnica di scansione TCP connect, dove Nmap tenta di stabilire una connessione TCP completa con le porte target per determinare se sono aperte, chiuse o filtrate.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sT 192.168.32.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 16:27 CET
Nmap scan report for 192.168.32.102
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (conn-refused)
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: 08:00:27:F3:E2:F4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds
```

Differenze tra i risultati della scansioni TCP connect e SYN:

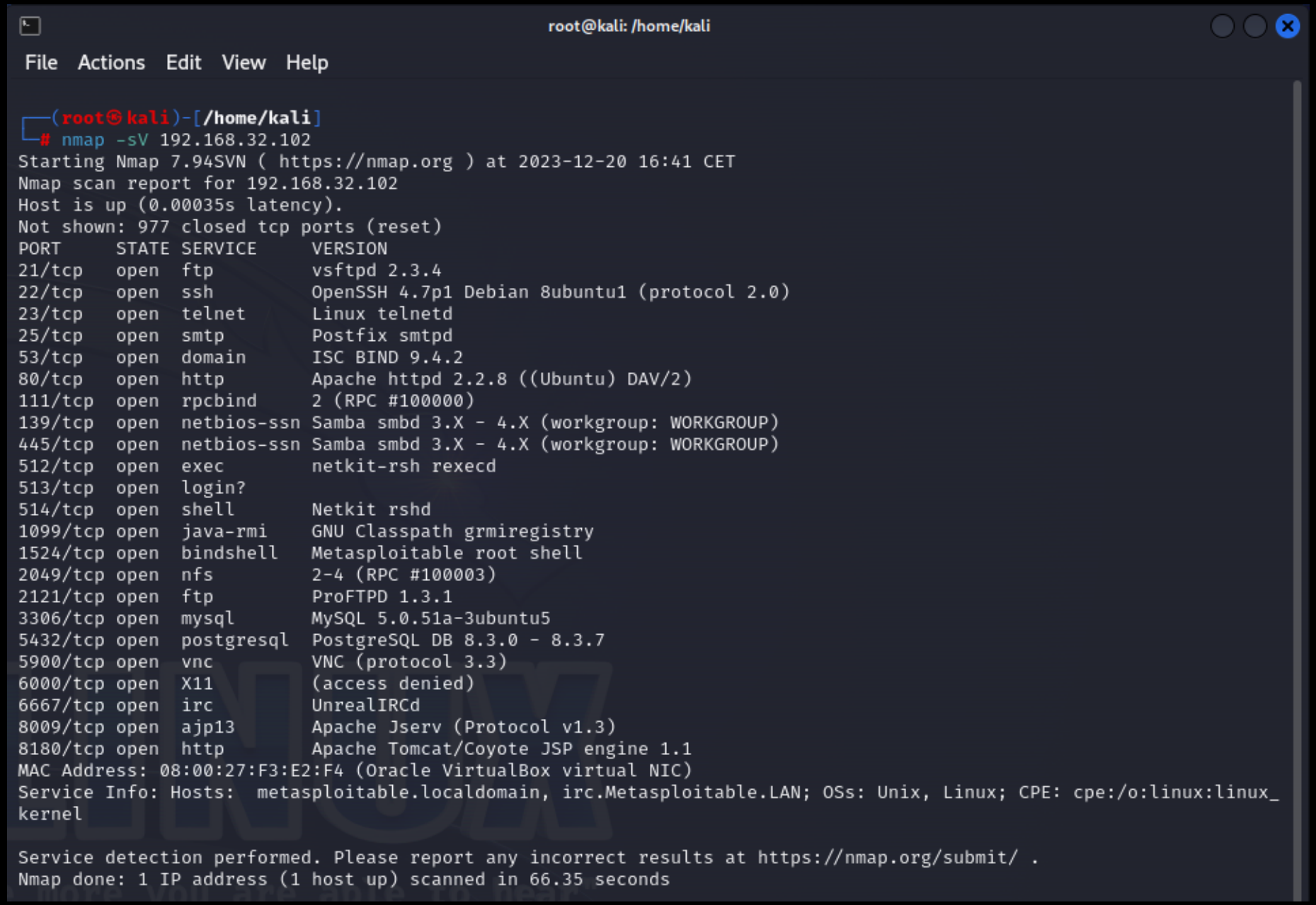




La "version detection" è una funzione di Nmap e di altri strumenti di scansione di rete che cerca di identificare le versioni specifiche dei servizi in esecuzione su porte target. Invece di limitarsi a determinare se una porta è aperta o chiusa, la version detection analizza le risposte dei servizi per cercare di determinare la versione esatta del software (come web server, database, servizi di file, ecc.) in esecuzione su quella porta. Questa informazione può essere utile per valutare la sicurezza, pianificare potenziali vulnerabilità o comprendere meglio la configurazione e le capacità di un sistema target.

Eseguiamo il comando «nmap –sV 192.168.32.102» da Kali verso Meta.

Il comando nmap -sV 192.168.32.102 utilizza Nmap per eseguire una scansione delle porte e tenta di determinare le versioni dei servizi in esecuzione su tali porte. In pratica, Nmap cercherà di identificare le versioni specifiche dei servizi (ad esempio, versioni di web server, database, ecc.) che stanno eseguendo su quelle porte specifiche sull'host 192.168.32.102.


root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.32.102
Starting Nmap 7.94SVN (https://nmap.org) at 2023-12-20 16:41 CET
Nmap scan report for 192.168.32.102
Host is up (0.00035s 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:F3:E2:F4 (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 66.35 seconds

Eseguiamo ora il comando «nmap -Pn -O 192.168.32.101» da Kali verso Windows 7.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-20 16:32 CET
Nmap scan report for 192.168.32.101
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:2C:73:DD (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|general purpose|phone
Running: Allen-Bradley embedded, Atcom embedded, Microsoft Windows 7|8|Phone|XP|2012, Palmmicro embedded, VMware Pla
yer
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows
_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:play
er
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Microsoft Windows Embedded Standard 7, Micro
soft Windows 8.1 Update 1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows Serv
er 2012, Palmmicro AR1688 VoIP module, VMware Player virtual NAT device
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.12 seconds
```

Si tratta molto probabilmente dell'impostazione del Firewall di Windows che costringe Nmap ad ignorare le porte.

Per poterle scansionare, occorrerebbe intervenire sul Firewall o bypassarlo.