ESERCIZIO S5L3

TRACCIA: 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 la seguente sul target Windows 7: OS fingerprint.
A valle delle scansioni è prevista la produzione di un report contenente le seguenti info (dove disponibili): ● IP. ● Sistema Operativo. ● Porte Aperte. ● Servizi in ascolto con versione.

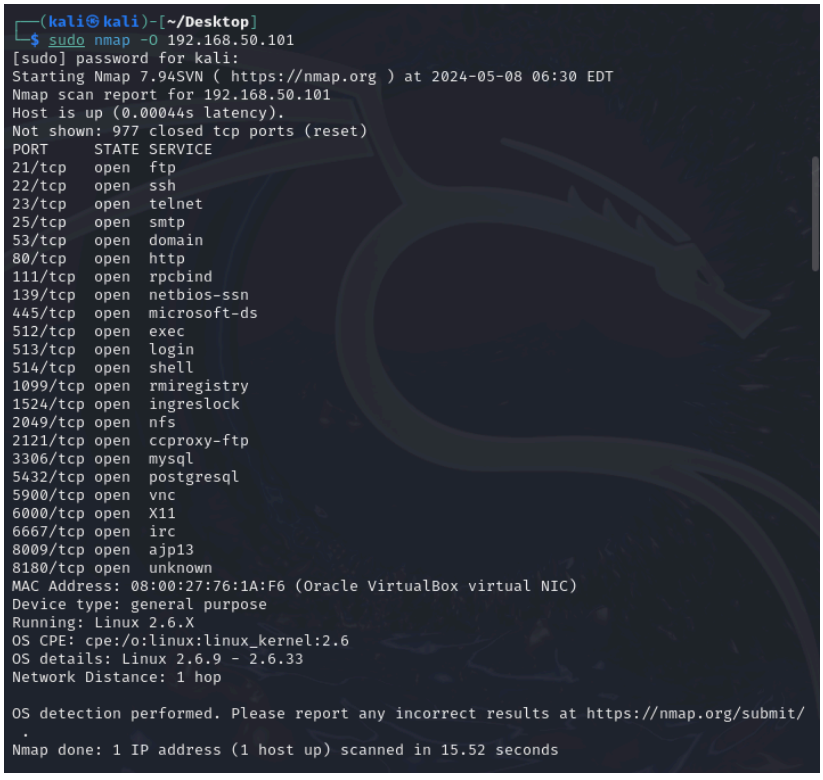
Quesito extra (al completamento dei quesiti sopra): Quale potrebbe essere una valida ragione per spiegare il risultato ottenuto dalla scansione sulla macchina Windows 7? Che tipo di soluzione potreste proporre per continuare le scansioni?

SVOLGIMENTO

TARGET: Metasploitable 2

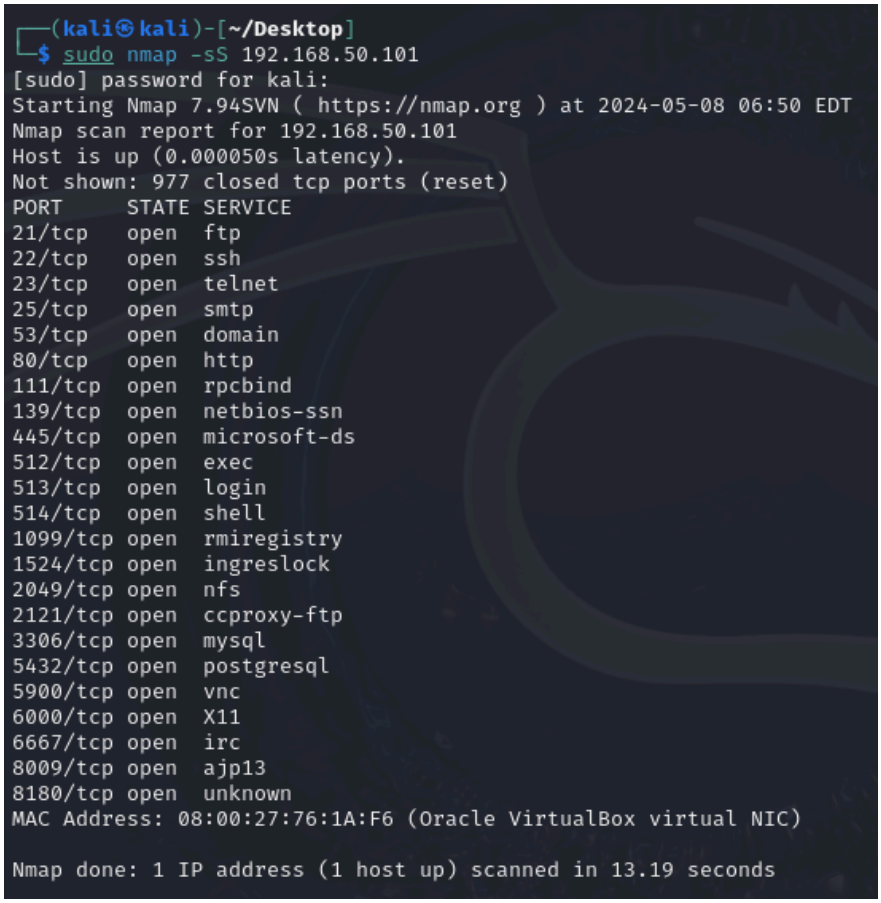
> sudo nmap -O *indirizzo_ip*

Con questo comando si effettua una scansione **OS fingerprint**: questa funzionalità stima il sistema operativo target ispezionando i pacchetti di risposta ricevuti. Tali pacchetti sono leggermente differenti per ogni sistema operativo (Windows, Linux, macOS), quindi confrontandoli con un database di risposte conosciute per i differenti SO si arriva a capire quasi sia il SO target. Il comando “sudo” viene messo per ottenere i permessi di root.



> sudo nmap -sS *inidirizzo_ip*

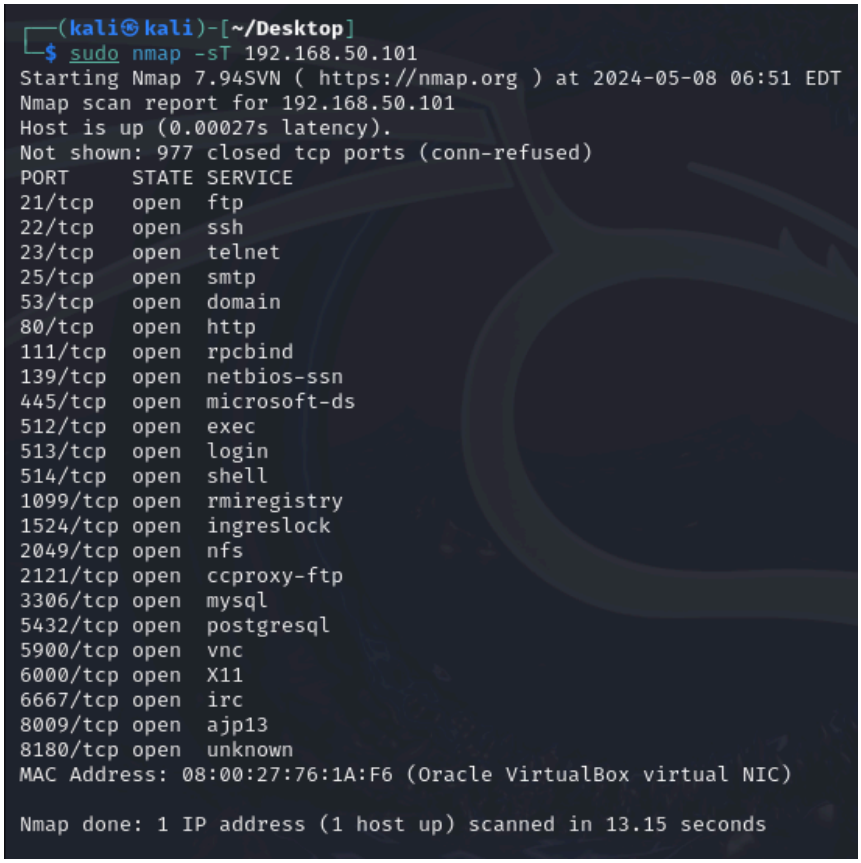
Con questo comando si esegue una scansione delle porte, in particolare lo switch ‘-sS’ indica il cosiddetto **SYN scan**. Questo metodo di scansione sfrutta il 3-way-handshake: il modo in cui TCP lavora per stabilire una comunicazione. In questo caso viene sfruttato per capire se una porta è attiva o meno, infatti se dopo una richiesta SYN si riceve in risposta un SYN-ACK questo vuol dire che la porta è aperta. In questo caso, il SYN scan non conclude il 3-way-handshake con una risposta ma, avendo capito che la porta è aperta, chiude la comunicazione inviando un pacchetto RST (reset).



> sudo nmap -sT *indirizzo_ip*

Con questo comando si esegue una scansione delle porte simile a quella descritta sopra nello SYN scan. A differenza del SYN scan, questo metodo è molto più invasivo poiché conclude il

3-way-handshake, stabilendo di fatto un canale di comunicazione. In questo modo si crea più “rumore” a livello network e si rischia di essere più identificabili.



> sudo nmap -sV -sS *indirizzo_ip*

Questo comando avvia una scansione con privilegi elevati utilizzando una combinazione di SYN scan e rilevazione delle versioni dei servizi, per identificare le porte aperte e i servizi eseguiti su un indirizzo IP specifico.
Lo switch ‘-sV’ permette di effettuare il "Service Version Detection" (rilevazione delle versioni dei servizi). Nmap tenta di determinare quali servizi stanno girando sulle porte aperte e, se possibile, di identificare la versione specifica di quei servizi. Questo può includere informazioni come il tipo di servizio (es. HTTP, FTP, SSH), il software esatto in esecuzione (es. Apache, OpenSSH), e la versione.
Questo tipo di scansione è utile per capire la configurazione di un sistema e identificare potenziali punti deboli, ma dovrebbe essere eseguita solo su sistemi su cui si ha il permesso di fare test di sicurezza o analisi di rete.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV -sS 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 06:52 EDT
Nmap scan report for 192.168.50.101
Host is up (0.000057s 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: 08:00:27:76:1A:F6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Li
nux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.60 seconds
```

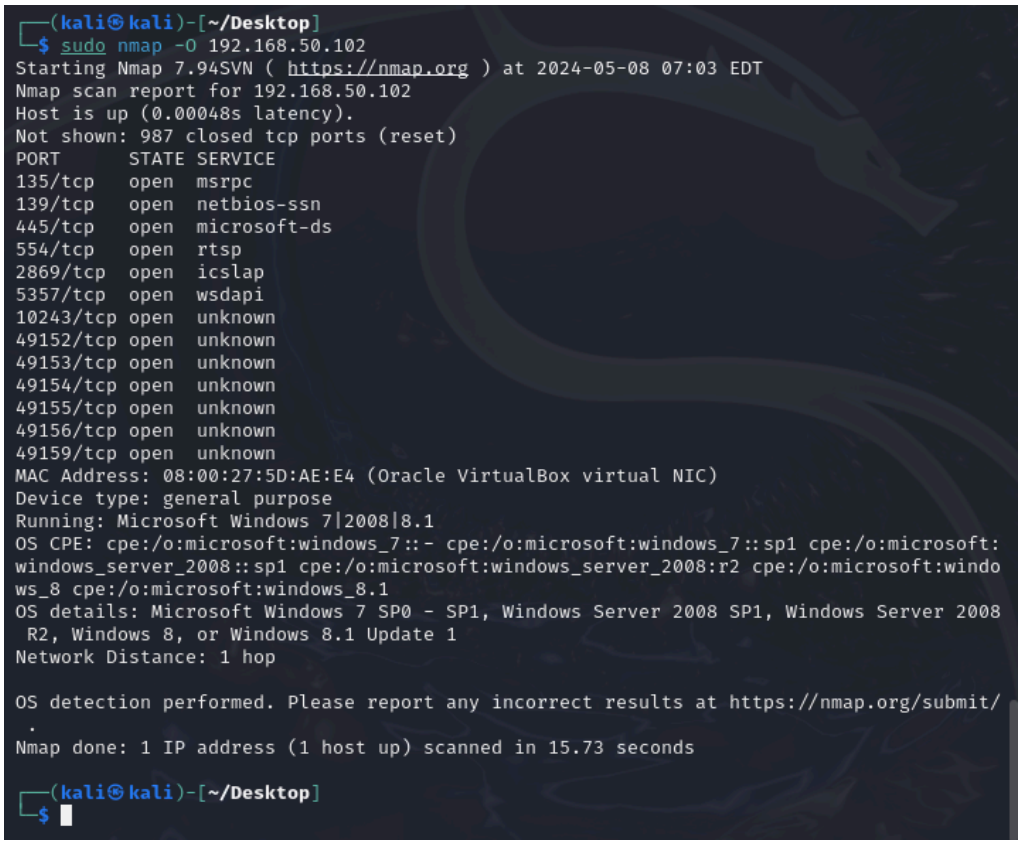
TARGET: WINDOWS 7

Usando come target Windows 7 è stata fatta una scansione OS fingerprint. In questo caso si nota una risposta diversa da quella ottenuta da Meta, così come mostrato in figura. Lo scan delle porte non è avvenuto correttamente in quanto non siamo riusciti ad ottenere il loro stato.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -O 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 07:00 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00019s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:5D:AE:E4 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
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 38.57 seconds
```

Per risolvere questa situazione si è disattivato il firewall di Windows 7. In questo modo si è riuscito ad ottenere uno scan delle porte come ottenuto prima con Meta. La figura in basso mostra gli output della scansione OS fingerprint.



RISPOSTA AL QUESITO EXTRA

Si è visto prima che l'output ottenuto da Windows per la scansione OS fingerprint non ha portato un buon risultato per la presenza del firewall attivo di Win7. Disattivandolo è andata buon fine la scansione. Questo però si può fare perchè stiamo lavorando in un laboratorio virtuale.