Identificazione Servizi e scansione

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 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):

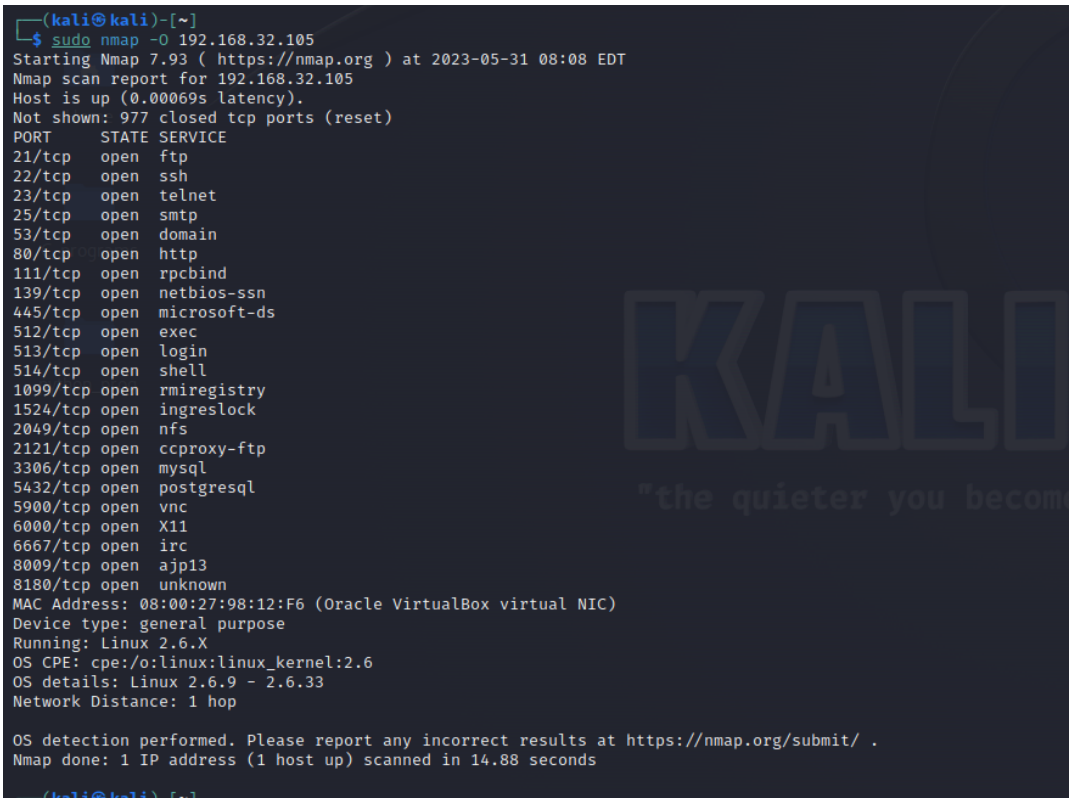
- IP
- Sistema Operativo
- Porte Aperte
- Servizi in ascolto con versione

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:

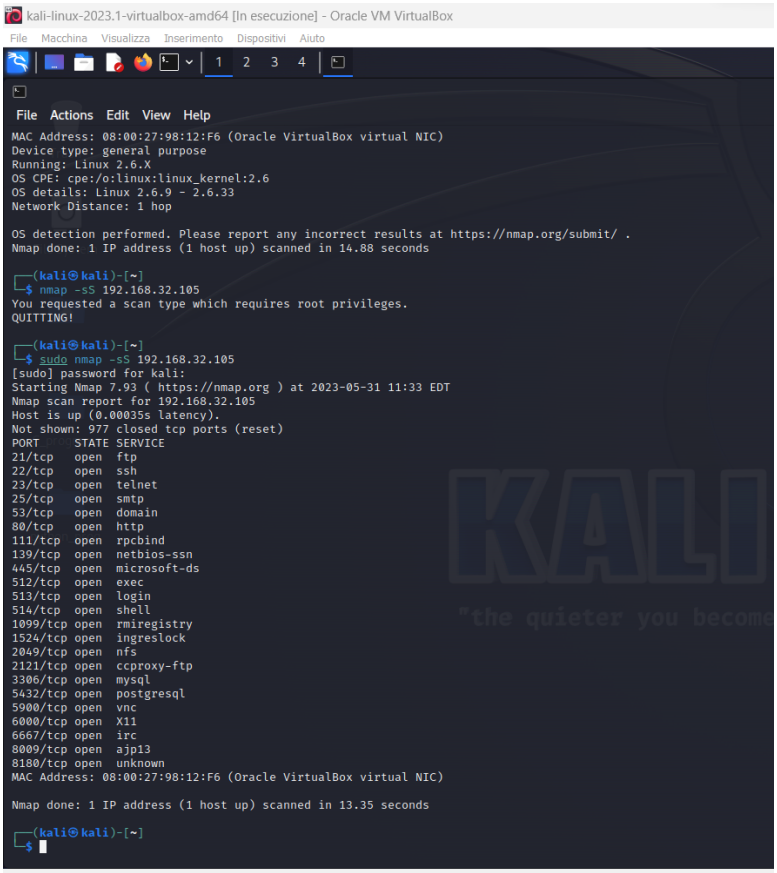
Dopo aver riportato le macchine sulla stessa rete impostando su Meta l'indirizzo IP 192.168.32.105, procedo allo svolgimento della traccia iniziando le mie scansioni con Nmap. Nel caso specifico, considerando che conosciamo l'IP, salto la fase di Host discovery già presentata in un precedente report e inizio con l'analisi di riconoscimento del Sistema Operativo:

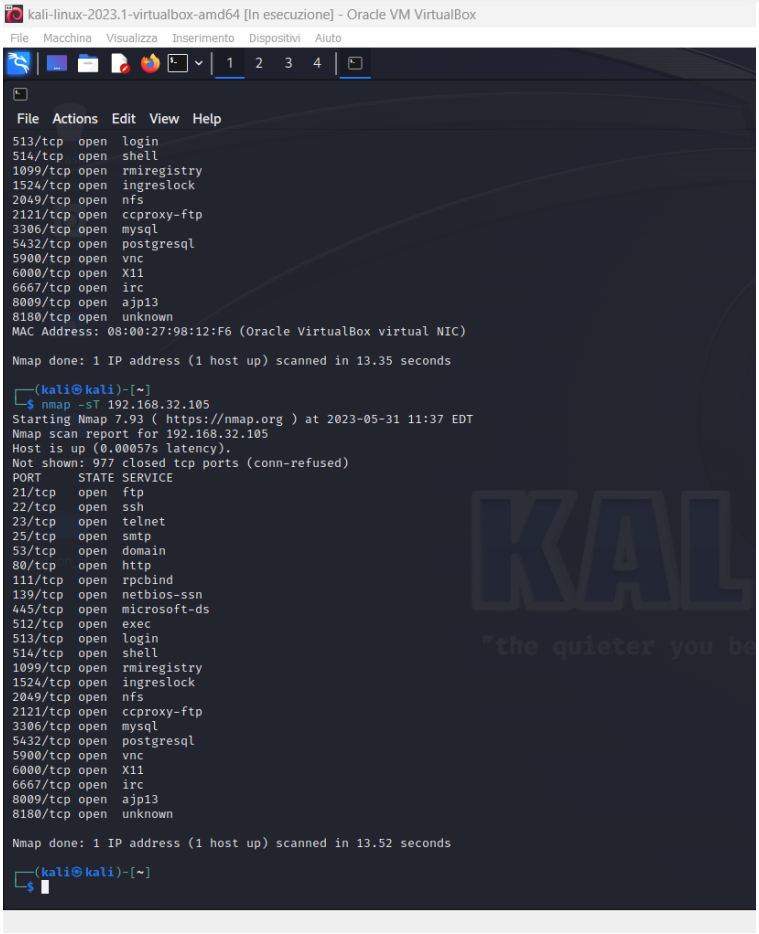


Già questo comando permette di ottenere un'enorme quantità di informazioni, si notino dallo screenshot:

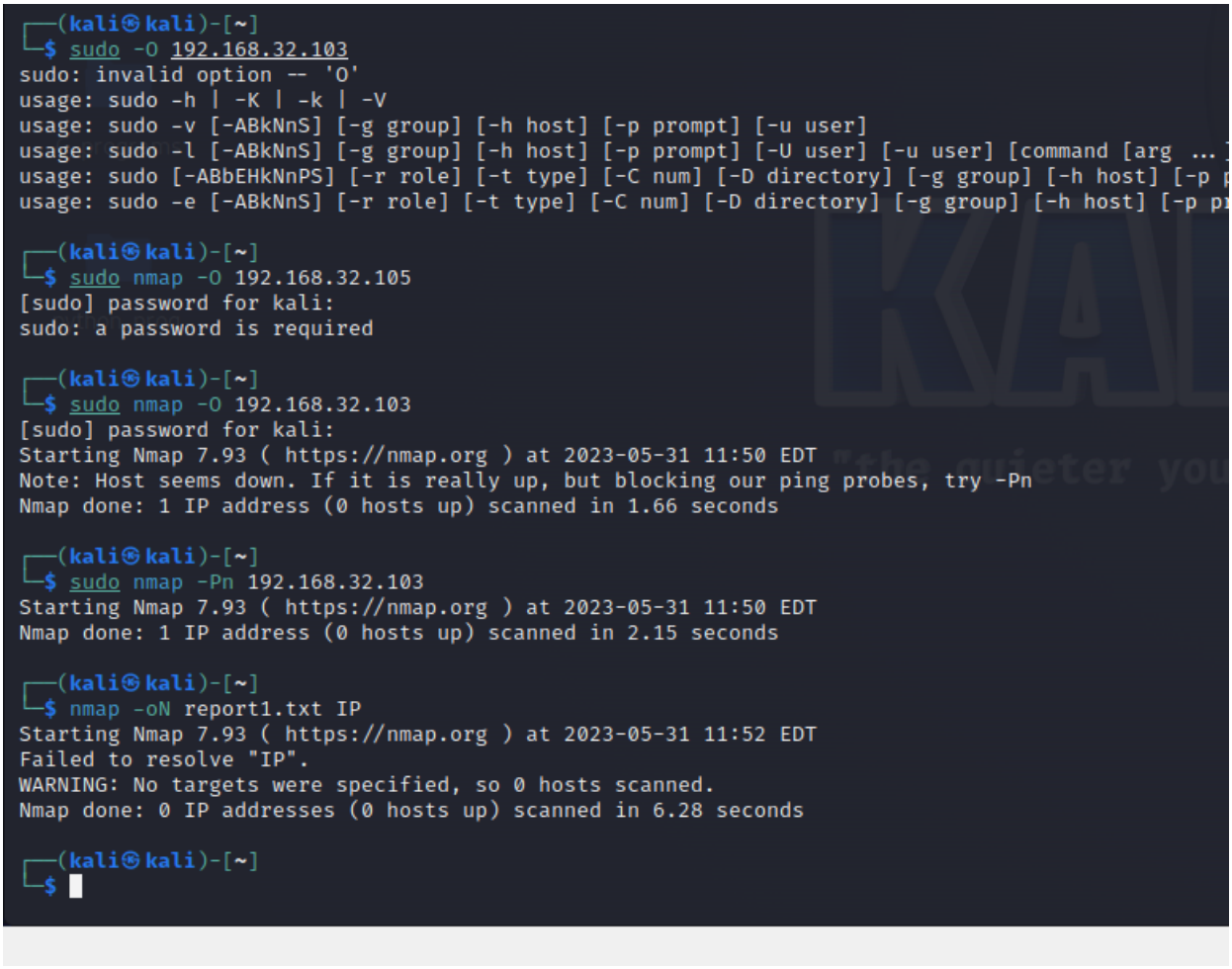
- **L'indirizzo IP target**
- **Il S.O. con relativa versione**
- **Le porte aperte**
- **I servizi relativi alle porte in questione**
- **L'indirizzo MAC**

Si possono inoltre utilizzare strumenti meno invadenti per la scansione del target, come il comando "nmap –sS", che esegue la scansione senza completare il Three-way-handshake, e "nmap –sT", che fornisce informazioni appena più affidabili a valle di una scansione un po' più invasiva, che completa il "TWH". Le informazioni ottenute sono decisamente coerenti tra loro.


kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
MAC Address: 08:00:27:98:12:F6 (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 14.88 seconds
(kali㉿kali)-[~]
$ nmap -sS 192.168.32.105
You requested a scan type which requires root privileges.
QUITTING!
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.32.105
[sudo] password for kali:
Starting Nmap 7.93 (https://nmap.org) at 2023-05-31 11:33 EDT
Nmap scan report for 192.168.32.105
Host is up (0.00035s 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: 08:00:27:98:12:F6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
(kali㉿kali)-[~]
$


kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
File Actions Edit View Help
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: 08:00:27:98:12:F6 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.35 seconds
(kali㉿kali)-[~]
$ nmap -sT 192.168.32.105
Starting Nmap 7.93 (https://nmap.org) at 2023-05-31 11:37 EDT
Nmap scan report for 192.168.32.105
Host is up (0.00057s 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
Nmap done: 1 IP address (1 host up) scanned in 13.52 seconds
(kali㉿kali)-[~]
$

Passo ora all'analisi della macchina Windows 7.
Come per Metasploitable, iniziamo con l'host discovery e il riconoscimento del S.O.
La prima cosa che si può notare, e la mancata riuscita dello scan con il firewall attivo:



Una volta spento, esamino di nuovo i risultati:

Anche in questo caso, possiamo enumerare la stessa quantità di informazioni già ottenute su Meta, come :

- L'indirizzo IP target
- Il S.O. con relativa versione
- Le porte aperte
- I servizi relativi alle porte in questione
- L'indirizzo MAC

Si può usare inoltre, in entrambi i casi, il comando "sudo nmap –nO report.txt IP_target" che preparerà un pratico e chiaro report con tutte le informazioni in questione. Va inoltre sottolineato, che tutti gli altri comandi (quali –sS, -sT, etc), funzionano altrettanto bene anche nell'approccio con S.O. windows.