ESERCITAZIONE W11D1(2)

EPICODE

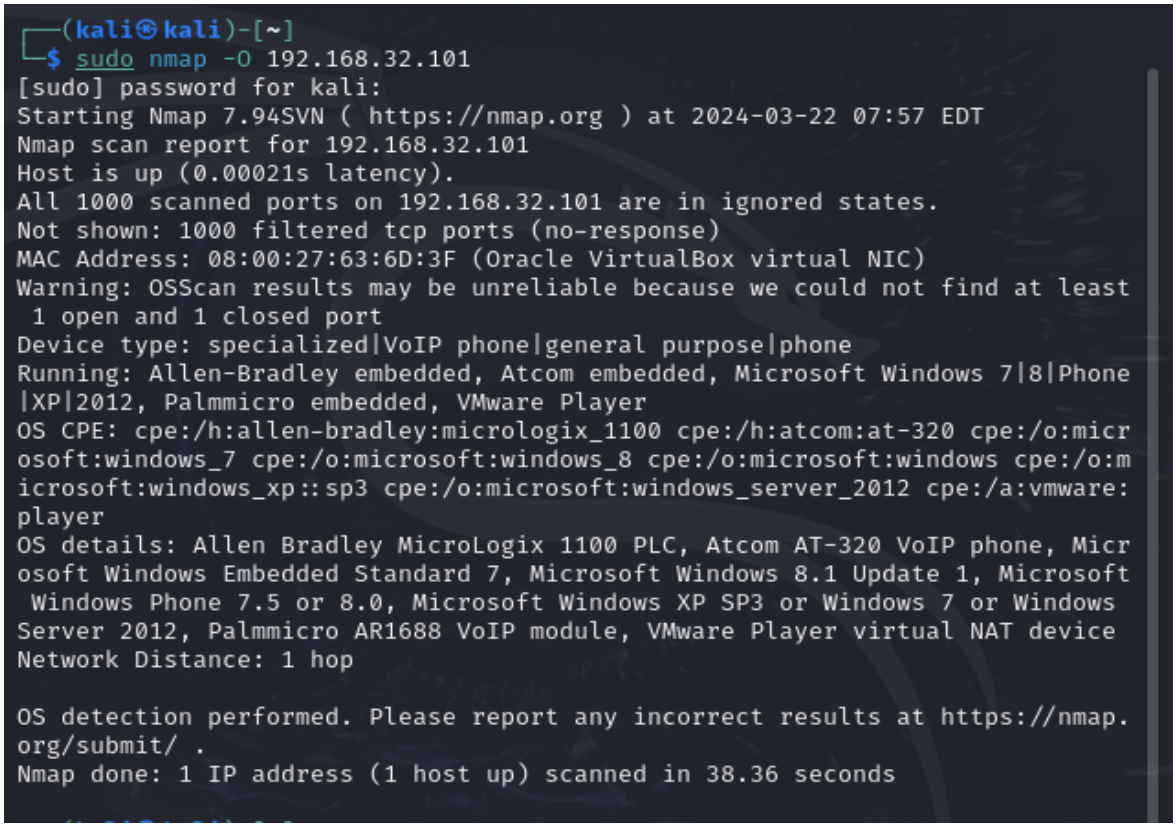
Esercizio
Scansione dei servizi

Traccia: Tecniche di scansione con Nmap

Si richiede allo studente di effettuare le seguenti scansioni sul target **Windows 7**:

- OS fingerprint
- Syn Scan
- Version detection

SCANSIONE OS FINGERPRINT SU WINDOWS 7



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.32.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-22 07:57 EDT
Nmap scan report for 192.168.32.101
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:63:6D:3F (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 Player
OS CPE: cpe:/h:allen-bradley:micrologix_1100 cpe:/h:atcom:at-320 cpe:/o:micr
osoft:windows_7 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:m
icrosoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2012 cpe:/a:vmware:
player
OS details: Allen Bradley MicroLogix 1100 PLC, Atcom AT-320 VoIP phone, Micr
osoft Windows Embedded Standard 7, Microsoft Windows 8.1 Update 1, Microsoft
 Windows Phone 7.5 or 8.0, Microsoft Windows XP SP3 or Windows 7 or Windows
Server 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 38.36 seconds
```

Da questa scansione possiamo notare che 999 porte TCP non hanno prodotto risposte durante i test eseguiti con Nmap, indicandole quindi come "filtrate". Questa situazione potrebbe derivare dalla presenza di un dispositivo di sicurezza che impedisce l'accesso alle richieste in entrata. In un contesto reale, le strategie utilizzabili potrebbero includere tecniche di elusione dei firewall e dei sistemi di prevenzione delle intrusioni (IPS).