EPICODE

ESERCIZIO W11D4

SCANSIONE DEI SERVIZI CON NMAP PT. 2

Mungiovì Fabio

TASK

Si richiede allo studente di effettuare le scansioni dell'esercizio precedente con Nmap sul target Windows con Windows Firewall abilitato e disabilitato.

Elencare tutti i passaggi compiuti ed i tipi di scansione, con i relativi risultati, durante la fase di scrittura report.

Facoltativo:
Spostare il target Windows nella stessa rete dell'attaccante e ripetere le scansioni con Windows Firewall abilitato e disabilitato.

Comandi da eseguire:

- `nmap -O <target>`
  Tenta di identificare il sistema operativo dell'host.

- `nmap -sS <target>`
  Esegue una scansione TCP SYN (stealth scan) per verificare lo stato delle porte TCP. È meno probabile che venga loggata.

- `nmap -sT <target>`
  segue una scansione TCP Connect, che completa la connessione TCP per verificare lo stato delle porte. È più rumorosa della -sS.

- `nmap -sV <target>`
  Tenta di determinare la versione dei servizi in esecuzione sulle porte aperte/filtrate.

ESECUZIONE

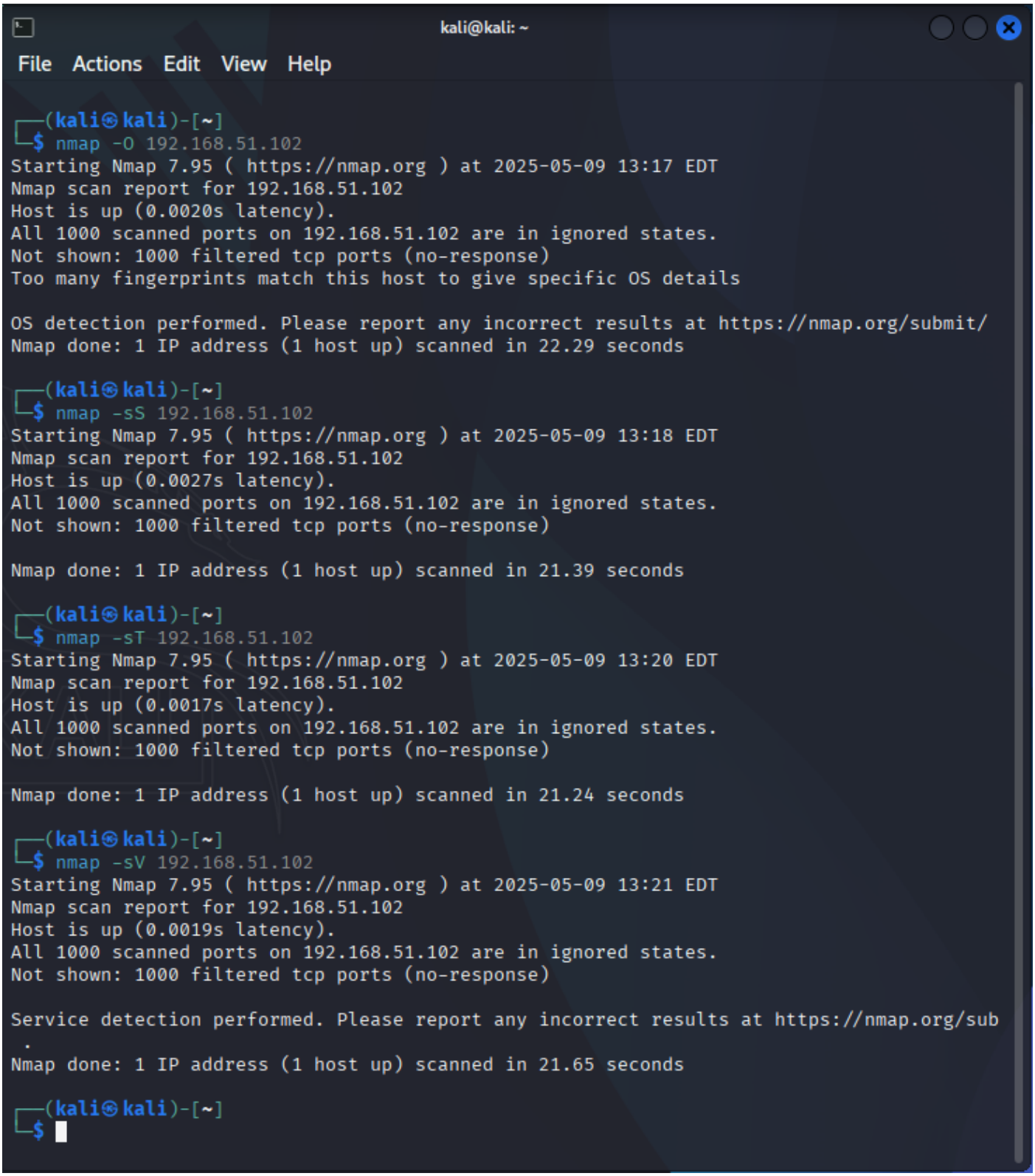
- Report Scansioni Nmap per 192.168.51.102 con Firewall ATTIVO

Comando Nmap	Data/Ora Inizio (EDT)	Latenza	Risultato Porte Scansionate	Note Aggiuntive	Durata Scansione
nmap -O 192.168.51.102	2025-05-09 13:17	0.0020s	1000 porte filtrate (no-response)	"Too many fingerprints match this host to give specific OS details" (Rilevamento OS eseguito)	22.29 secondi
nmap -sS 192.168.51.102	2025-05-09 13:18	0.0027s	1000 porte filtrate (no-response)	-	21.39 secondi
nmap -sT 192.168.51.102	2025-05-09 13:20	0.0017s	1000 porte filtrate (no-response)	-	21.24 secondi
nmap -sV 192.168.51.102	2025-05-09 13:21	0.0019s	1000 porte filtrate (no-response)	"Service detection performed." (Rilevamento dei servizi eseguito)	21.65 secondi

CONCLUSIONI

In tutte le scansioni l'host 192.168.51.102 risulta attivo ("Host is up"), ma tutte le 1000 porte TCP scansionate sono indicate come "filtered" (filtrate), il che significa che Nmap non è riuscito a determinare se fossero aperte o chiuse, a causa del firewall.

Nella seguente immagine i risultati visualizzati dal terminale:



❖ Report Scansione Nmap per 192.168.51.102 con Firewall DISATTIVATO

Informazioni sulla Scansione:

- Host Target: 192.168.51.102
- Comando Nmap: `nmap -sV -O -sT 192.168.51.102`
- Data e Ora Inizio Scansione: 2025-05-11 01:35 CEST
- Durata Scansione: 62.80 secondi

Porta	Stato	Servizio	Versione
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC

Note: 990 porte TCP chiuse (conn-refused) non sono mostrate.

Informazioni sul Sistema Operativo e Dispositivo:

Categoria	Dettaglio
Tipo Dispositivo	General purpose
Sistema Operativo	Microsoft Windows 2008 | 7 | Vista
Dettagli OS	Microsoft Windows 7 or Windows Server 2008 R2, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
OS CPE	cpe:/o:microsoft:windows_server_2008:r2, cpe:/o:microsoft:windows_7, cpe:/o:microsoft:windows_vista::-, cpe:/o:microsoft:windows_vista::sp1
Info Servizio	Host: PC; OS: Windows; CPE: cpe:/o:microsoft:windows
Distanza di Rete	2 hops

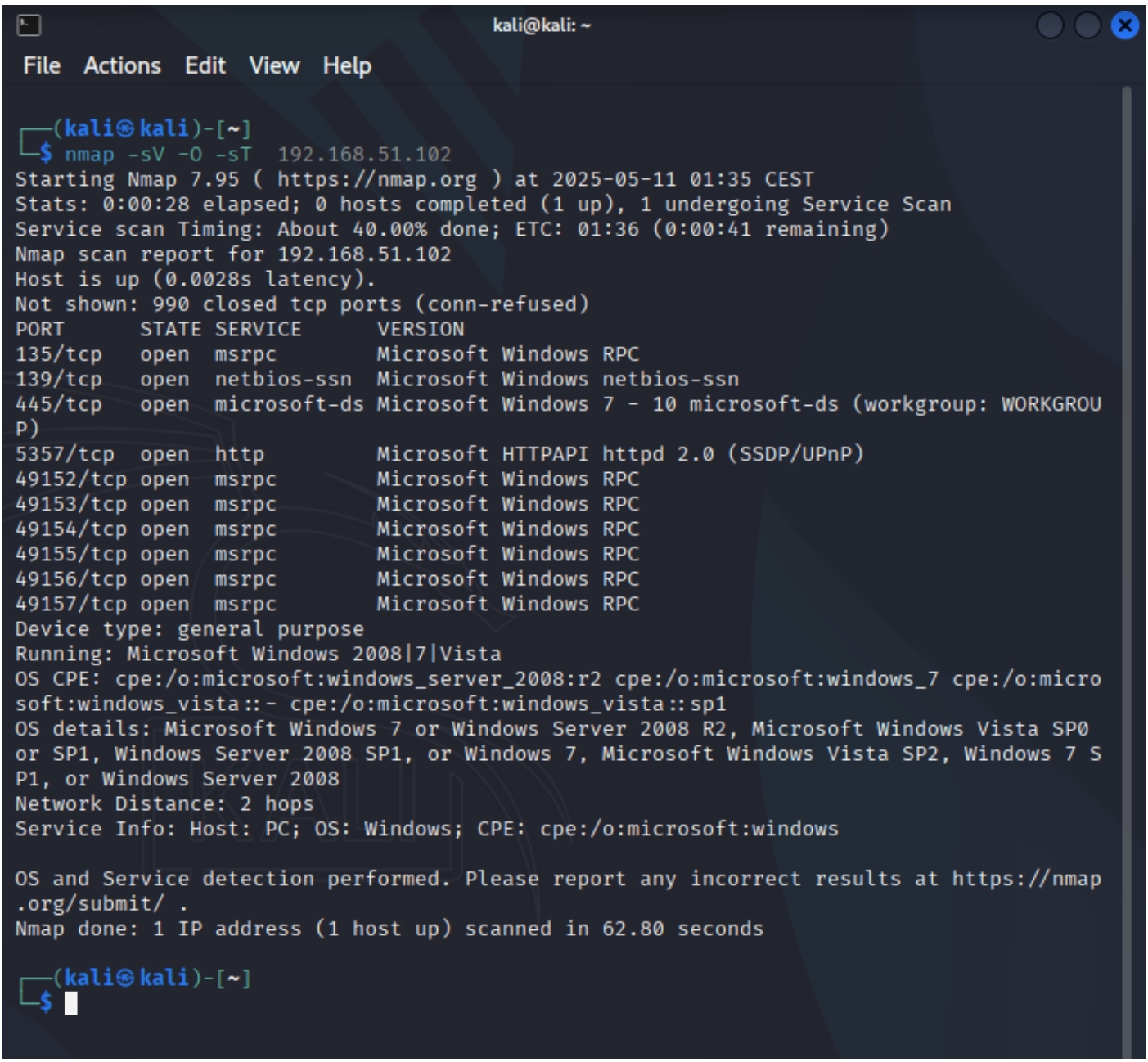
CONCLUSIONI

Disattivando il firewall di Windows riusciamo ad ottenere molte più informazioni sul sistema operativo, sulle porte aperte e sui servizi annessi ad esse, che potrebbero rappresentare delle criticità di sicurezza.

La scansione indica anche che l'host si trova a 2 "hop" di distanza, il che fornisce un'idea della sua posizione nella rete rispetto alla macchina che ha eseguito la scansione.

La maggior parte delle altre porte TCP (990) sono risultate chiuse.

Nella seguente immagine i risultati visualizzati dal terminale:



FACOLTATIVO

Spostando la macchina Windows 7 sotto la stessa subnet di Kali Linux, ripetiamo le scansioni precedenti con firewall attivo e disattivato, e analizziamo le differenze

- ❖ Riepilogo Scansioni Nmap per 192.168.50.102 con Firewall ATTIVO

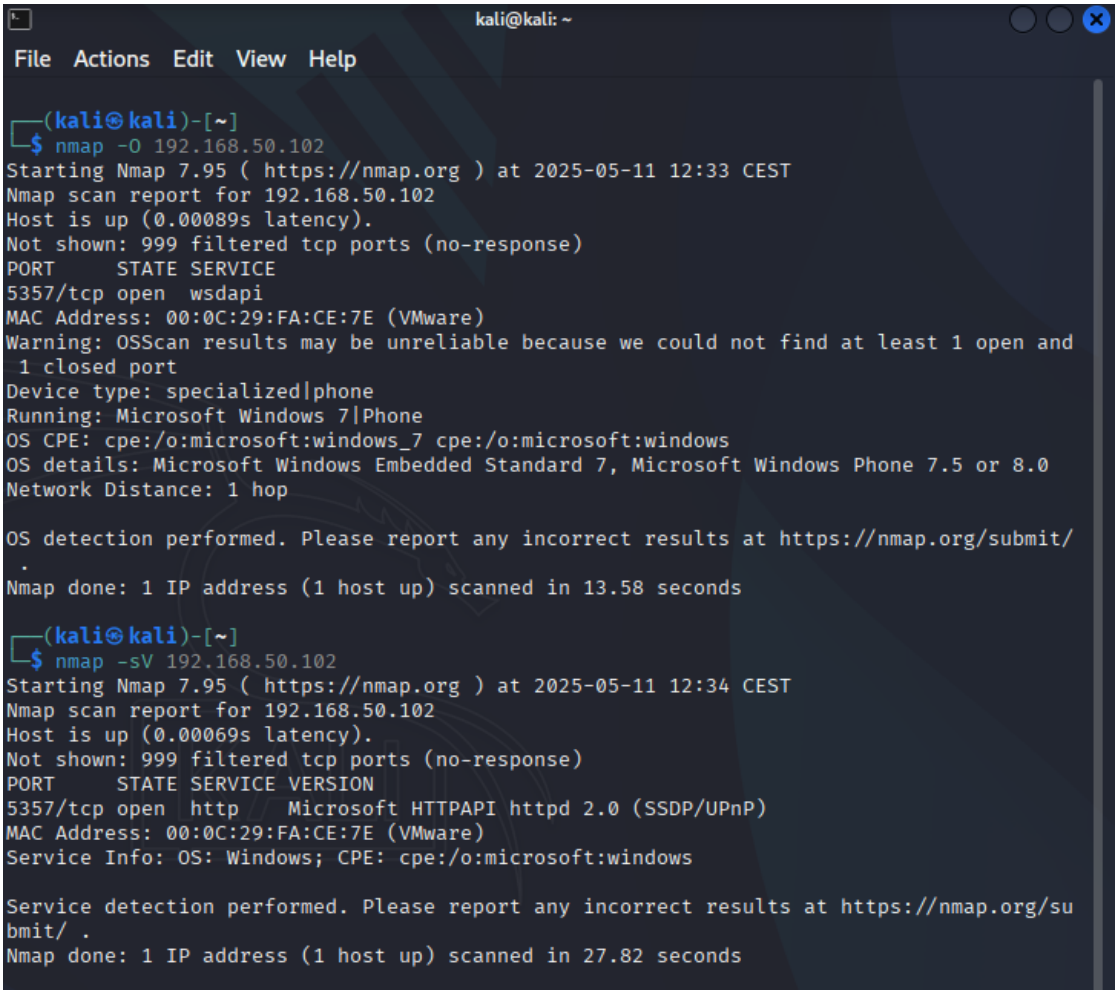
Informazioni sulla scansione

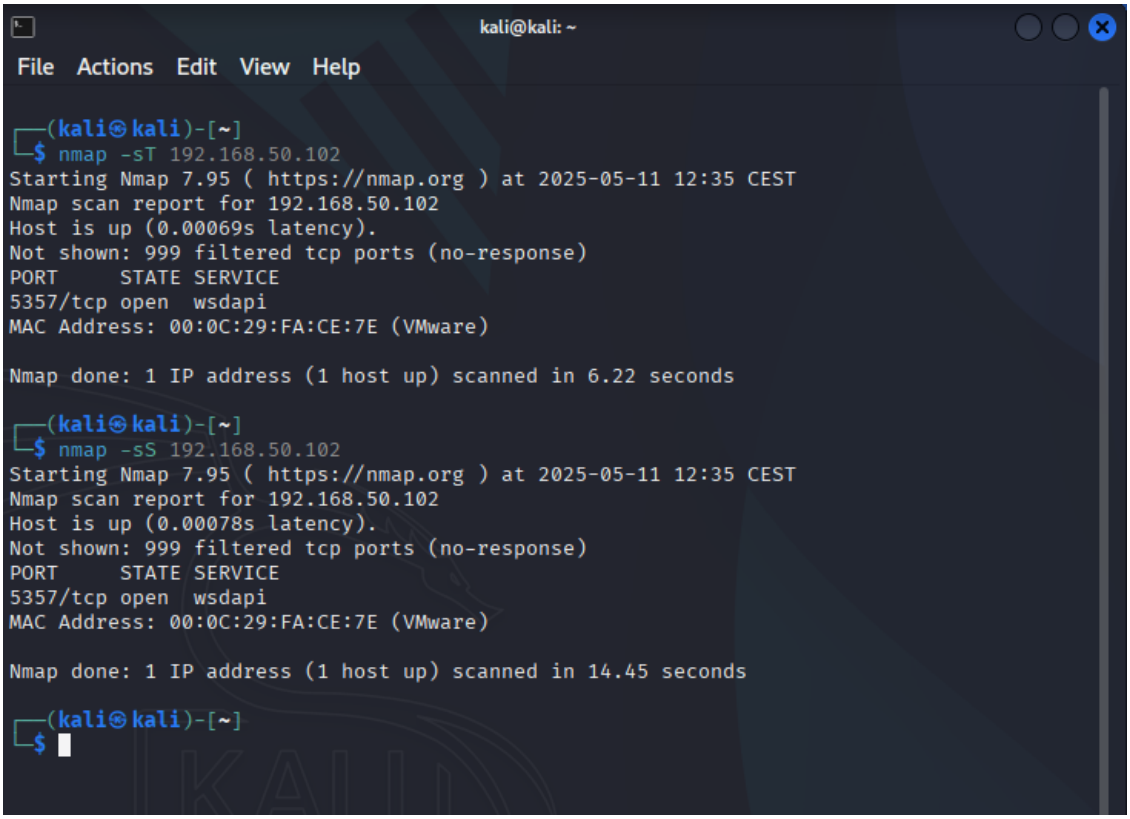
- Porte Aperte:
  Identificata 1 porta aperta: 5357/tcp (Microsoft HTTPAPI httpd 2.0, SSDP/UPnP).
- Stato delle Altre Porte:
  999 porte TCP risultano filtrate (no-response), indicando che il firewall dell'host blocca attivamente la maggior parte dei tentativi di connessione.
- Rilevazione OS:
  Nmap fornisce un'ipotesi sul sistema operativo (Windows 7/Phone, Windows Embedded), sebbene con un avviso di possibili inaffidabilità a causa della mancanza di una porta chiusa tra quelle testate per l'OS fingerprinting.
- MAC Address: Rilevato
- Network Distance: 1 hop.

CONCLUSIONI

In sintesi, con questa configurazione il firewall dell'host permette una minima visibilità (porta 5357), mentre con l'host su una subnet differente si ha un ulteriore livello di filtraggio (probabilmente a livello di rete) che blocca completamente i tentativi di scansione.

Nelle seguenti immagini i risultati visualizzati dal terminale:





❖ Report Scansioni Nmap per 192.168.50.102 con Firewall DISATTIVATO

Informazioni sulla scansione

- Comando Nmap: nmap -sV -O -sT 192.168.50.102 (o variazione simile)
- Indirizzo IP Target: 192.168.50.102
- Host: Raggiungibile (latenza 0.00095s)
- Porte Aperte (10 porte):
  L'elenco delle porte aperte, i servizi e le versioni sono identici a quelli dello scenario precedente.
- Porte Non Mostrate:
  990 closed tcp ports (conn-refused).
- MAC Address: 00:0C:29:FA:CE:7E (VMware). Rilevato, poiché l'host è sulla stessa subnet.
- Device Type: general purpose
- Sistema Operativo Rilevato:
  Running: Microsoft Windows 2008|7|Vista|8.1 (notare l'aggiunta di 8.1)
  OS Details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1 (leggermente più specifico, include Windows 8.1)
- Network Distance: 1 hop. Indica una connessione più diretta all'interno della stessa subnet.
- Tempo Scansione: 61.40 secondi.

CONCLUSIONI

Entrambi gli scenari di topologia della rete mostrano per la maggiori gli stessi risultati.

Le differenze che si possono notare sono nella differenza di hop, che nel secondo scenario è sceso a 1, e nella rilevazione del MAC address, che con macchine su subnet diverse non veniva identificato.

Nella seguente immagine i risultati visualizzati dal terminale: