

Esercizio W18D1 - Security Operation: azioni preventive

RICHIESTA

L'esercizio W18D1 - Security Operation: azioni preventive verte, appunto, sulle azioni preventive che puntano a ridurre la possibilità di attacchi provenienti dall'esterno. Nello specifico, è richiesto all'allievo di una scansione con **nmap** sulla macchina target Windows 7, prima con firewall disattivato e poi con firewall attivato. Lo scopo dell'esercizio è quello di evidenziare e motivare le differenze nei risultati

~~~

## SOLUZIONE

Per ottemperare alle richieste dell'esercizio W18D1 ho approntato, nel mio laboratorio, due macchine virtuali. La macchina attaccante è una VM Debian (**indirizzo IP 192.168.1.5**), la macchina target è una VM Windows 7 (**indirizzo IP 192.168.1.16**).

Ho innanzitutto disabilitato il firewall della macchina Windows 7 dal pannello di configurazione di Windows, poi ho utilizzato il tool **nmap** (dalla macchina Debian) per scansionare le porte della macchina target. Come lecito aspettarsi, la mancanza di ogni forma di difesa ha esposto diversi servizi di rete, comprese le porte dinamiche utilizzate da diversi servizi Windows.

Discorso completamente diverso con il firewall attivato: la prima scansione con **nmap** infatti non giunge a compimento, grazie al blocco completo delle richieste di ping. Questo comportamento mi ha costretto ad utilizzare un comando più aggressivo del tool **nmap**, che bypassa la prima fase di Ping.

L'esecuzione del secondo comando ha portato al completamento della scansione, con l'evidenziazione di diversi servizi di rete. A differenza della prima scansione, però, **nmap** non ha potuto rilevare le porte dinamiche utilizzate dai servizi Windows.

Questo comportamento evidenzia quindi l'importanza del firewall di Windows, nonostante sia una versione basica di firewall. Come ho potuto appurare, l'abilitazione del firewall ha **ridotto significativamente** la visibilità della macchina Windows 7 dall'esterno.

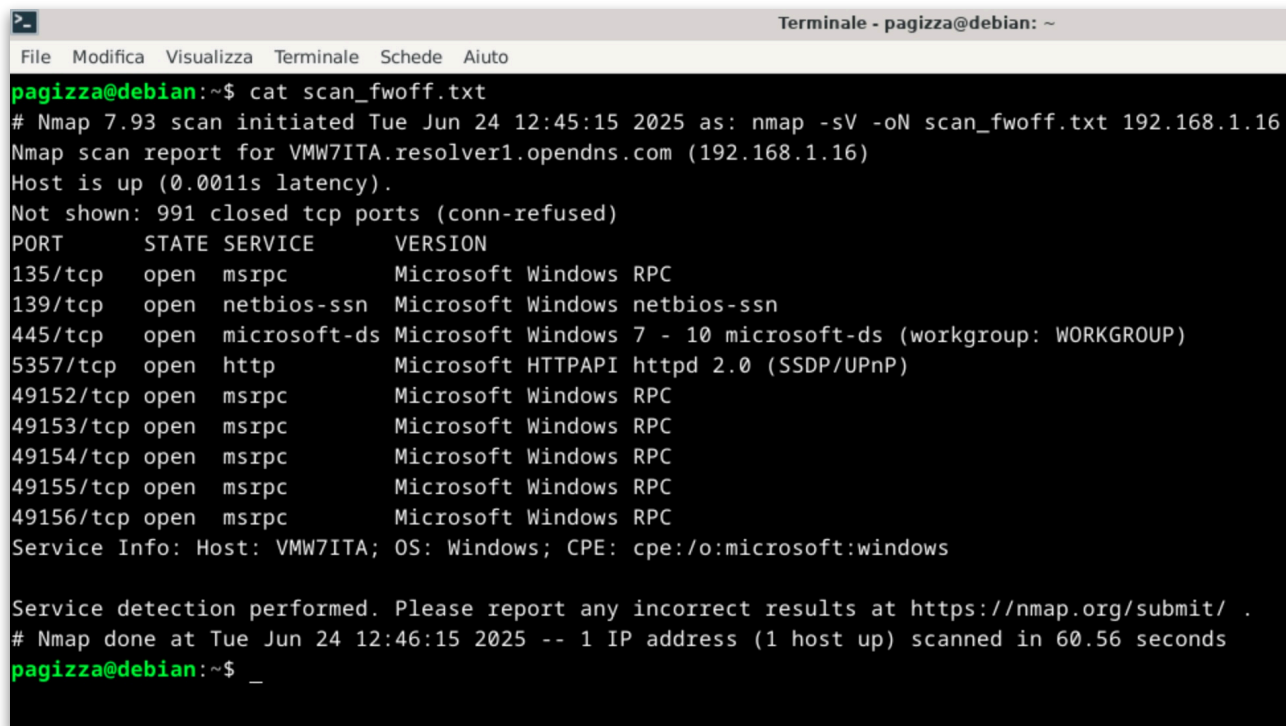
~~~

ANNOTAZIONI TECNICHE

Il primo passo dell'esercizio W18D1 prevede la disattivazione del Firewall sulla VM Windows 7 (**indirizzo IP 192.168.1.16**). Sono due le strade percorribili per ottenere questo risultato: si può disattivare il Firewall sia dalle impostazioni del pannello di controllo (la via che ho scelto), sia disattivando l'apposito servizio (MpsSvc). Una volta disattivato il Firewall, ho effettuato la prima scansione con il tool **nmap** dalla mia VM attaccante Debian. Il comando utilizzato è:

nmap -sV -oN nmap_scan_fwoff.txt 192.168.1.16

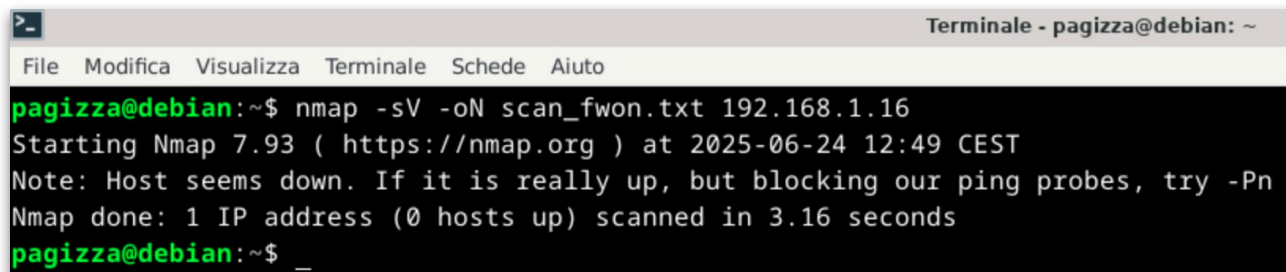
Il comando, oltre a scansionare le porte aperte della macchina target, si occupa anche di creare un file TXT con il risultato della scansione. Come si può vedere dall'immagine allegata, la scansione ha evidenziato diverse porte TCP aperte, come la 135, la 139, la 445 e la 5357. Particolarmente interessante il fatto che la scansione è riuscita anche a individuare alcune **porte dinamiche aperte** (dalla 49152 alla 49156), utilizzate dal sistema per l'esecuzione di vari servizi Windows che si appoggiano a RPC (Remote Procedure Call).



```
pagizza@debian:~$ cat scan_fwoff.txt
# Nmap 7.93 scan initiated Tue Jun 24 12:45:15 2025 as: nmap -sV -oN scan_fwoff.txt 192.168.1.16
Nmap scan report for VMW7ITA.resolver1.opendns.com (192.168.1.16)
Host is up (0.0011s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
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
Service Info: Host: VMW7ITA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 24 12:46:15 2025 -- 1 IP address (1 host up) scanned in 60.56 seconds
pagizza@debian:~$ _
```

Come anticipato nel capitolo relativo alla Soluzione, l'attivazione del Firewall nella VM target Windows 7 ha cambiato completamente il risultato della scansione. Riprovando lo stesso comando (**nmap -sV -oN nmap_scan_fwon.txt 192.168.1.16**) la scansione infatti non è nemmeno partita. Questo si spiega con il fatto che **nmap** esegue una fase preliminare di scoperta dell'host prima ancora di scansionare le porte, e parte di questa procedura di scoperta è affidata all'invio di pacchetti di ping. Il firewall di Windows 7 impedisce alla macchina di rispondere ai ping, stoppando dunque l'esecuzione di **nmap**.



```
pagizza@debian:~$ nmap -sV -oN scan_fwon.txt 192.168.1.16
Starting Nmap 7.93 ( https://nmap.org ) at 2025-06-24 12:49 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
pagizza@debian:~$ _
```

Come suggerito dal programma stesso, è possibile bypassare questa procedura di sicurezza inserendo l'opzione **-Pn** all'interno del comando di nmap. La sintassi si modifica in questo modo:

nmap -sV -Pn -oN nmap_scan_fwon_pn.txt 192.168.1.16

Con l'ausilio di questa opzione, la scansione si conclude con esito positivo. La differenza più grande che è possibile notare è il fatto che, nonostante la scansione si concluda con successo, non riesce però a rilevare nessuna delle **porte dinamiche aperte**.

```
pagizza@debian:~$ cat scan_fwon_pn.txt
# Nmap 7.93 scan initiated Tue Jun 24 12:51:29 2025 as: nmap -sV -Pn -oN scan_fwon_pn.txt 192.168.1.16
Nmap scan report for VMW7ITA.resolver1.opendns.com (192.168.1.16)
Host is up (0.0052s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
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)
Service Info: Host: VMW7ITA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jun 24 12:51:46 2025 -- 1 IP address (1 host up) scanned in 16.31 seconds
pagizza@debian:~$ _
```