W18D1 - TULLI ROBERTO
SECURITY OPERATION: AZIONI PREVENTIVE

ROMA 09/11/2025

Traccia:

Le azioni preventive mirano a ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

La macchina Windows, che abbiamo utilizzato, ha di **default il Firewall disabilitato.**

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

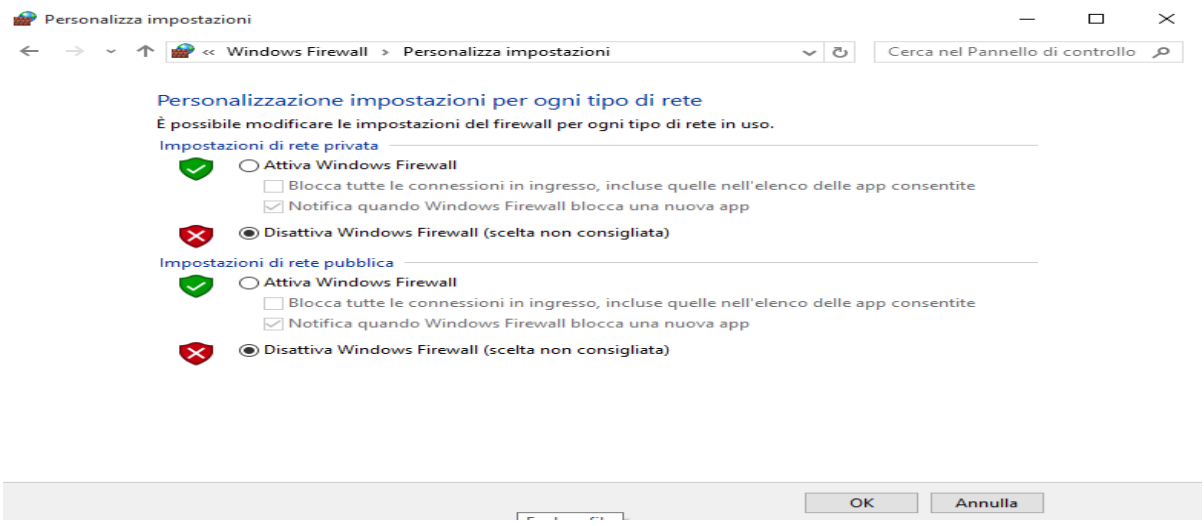
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

SVOLGIMENTO:

Prima di tutto, dopo aver acceso le due macchine, proviamo a vedere se le due macchine comunichino tra loro con un ping:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=2.44 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.32 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=2.47 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.983 ms
^C64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.64 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.49 ms
```

Successivamente andiamo a disattivare i firewall sulla macchina windows, aprendo le impostazioni dei firewall:



Dopo aver disattivato i firewall, andiamo a lanciare la scansione con nmap -sV (per la service detection) -o (per salvare la scansione effettuata su un file chiamato nmap.txt):

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o nmap.txt 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 14:36 EST
Nmap scan report for 192.168.50.102
Host is up (0.0013s latency).
Not shown: 982 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
7/tcp    open  echo
9/tcp    open  discard?
13/tcp   open  daytime       Microsoft Windows International daytime
17/tcp   open  qotd          Windows qotd (English)
19/tcp   open  chargen
80/tcp   open  http          Microsoft IIS httpd 10.0
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)
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5432/tcp open  postgresql?
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:64:42:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: DESKTOP-9K1O4BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 159.32 seconds
```

Andiamo ora a effettuare una nuova scansione nmap, ma stavolta andando ad attivare il firewall sulla macchina Windows:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -o nmapfirewallattivo.txt 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 14:41 EST
Nmap scan report for 192.168.50.102
Host is up (0.0012s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
8443/tcp open  ssl/https-alt
MAC Address: 08:00:27:64:42:74 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.58 seconds
```

Possiamo vedere la sostanziale differenza con firewall disattivo prima ed attivo poi, dove quando quest'ultimo è attivo abbiamo molte meno porte aperte visibili (la scansione con il firewall attivo impiegherà anche molto più tempo). Quando effettuiamo la scansione con il firewall attivo molte porte quindi risultano chiuse o filtrate.
Questo dimostra che il firewall è efficace nel limitare la visibilità dei servizi e nel ridurre la superficie d'attacco dall'esterno.

Facoltativo:

Monitorare i log di Windows durante queste operazioni:

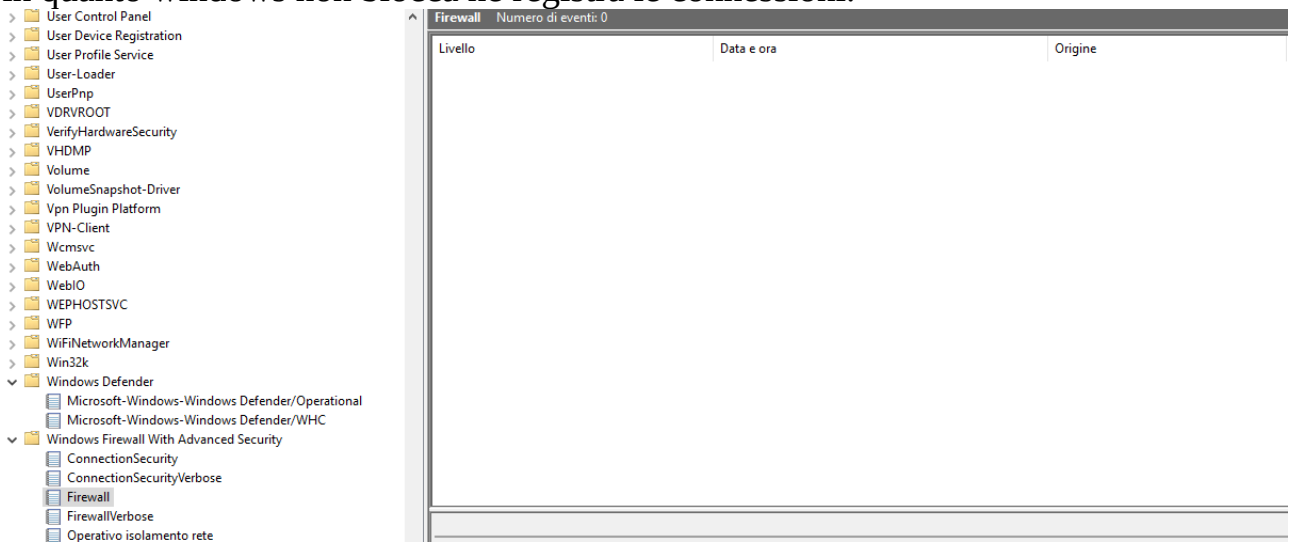
1. Quali log vengono modificati? (se vengono modificati)
2. Cosa si riesce a trovare?

SVOLGIMENTO:

Per effettuare questa parte dell’esercizio andiamo come prima cosa a cancellare il registro degli eventi per monitorare al meglio i log.

Poi lanciamo una nuova scansione (con firewall disattivo) e andiamo a controllare i log nella sezione Registri applicazioni e servizi → Microsoft → Windows → Windows firewall with advanced security → firewall.

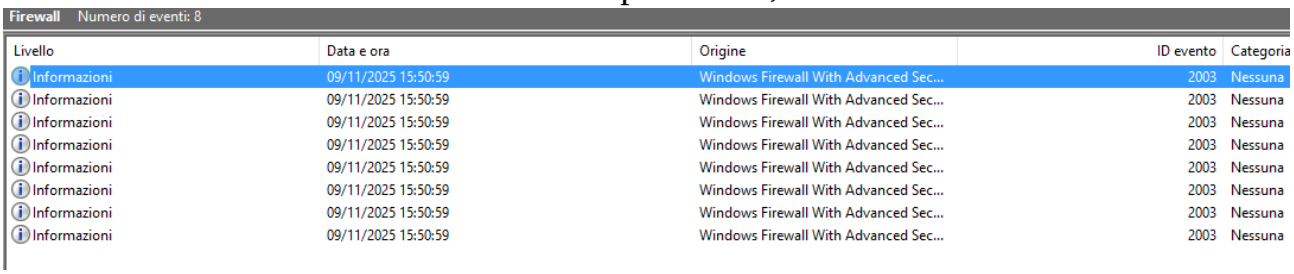
Dato che abbiamo effettuato la scansione disattivando il firewall non troviamo nulla in quanto windows non blocca ne registra le connessioni.



Firewall Numero di eventi: 0

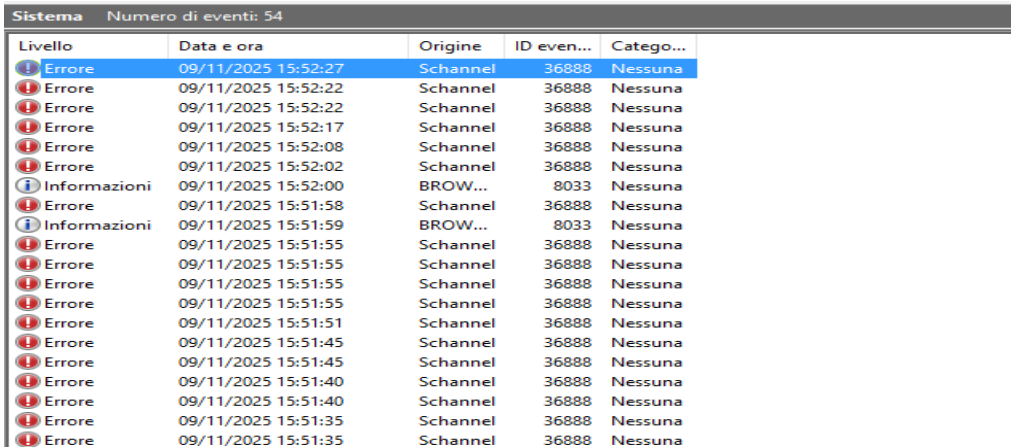
Livello	Data e ora	Origine

Discorso diverso se effettuiamo la stessa procedura, ma attivando i firewall:



Firewall Numero di eventi: 8

Livello	Data e ora	Origine	ID evento	Categoria
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna
Informazioni	09/11/2025 15:50:59	Windows Firewall With Advanced Sec...	2003	Nessuna



Sistema Numero di eventi: 54

Livello	Data e ora	Origine	ID even...	Catego...
Errore	09/11/2025 15:52:27	Schannel	36888	Nessuna
Errore	09/11/2025 15:52:22	Schannel	36888	Nessuna
Errore	09/11/2025 15:52:22	Schannel	36888	Nessuna
Errore	09/11/2025 15:52:17	Schannel	36888	Nessuna
Errore	09/11/2025 15:52:08	Schannel	36888	Nessuna
Errore	09/11/2025 15:52:02	Schannel	36888	Nessuna
Informazioni	09/11/2025 15:52:00	BROW...	8033	Nessuna
Errore	09/11/2025 15:51:58	Schannel	36888	Nessuna
Informazioni	09/11/2025 15:51:59	BROW...	8033	Nessuna
Errore	09/11/2025 15:51:55	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:55	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:55	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:55	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:51	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:45	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:45	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:40	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:40	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:35	Schannel	36888	Nessuna
Errore	09/11/2025 15:51:35	Schannel	36888	Nessuna

Conclusione:
Durante la scansione con firewall disattivato, nessun log rilevante viene modificato perche Windows non blocca il traffico.
Con il firewall attivo, si registrano numerosi eventi nel registro Windows Firewall, che indicano il blocco dei pacchetti provenienti dall’IP della macchina Kali.
Questi log dimostrano che il firewall rileva e registra i tentativi di connessione bloccati.