W18D1 – Pratica

Epic Education Srl

Impatto firewall Windows, log, BC, DR e IRBC

Simone Giordano

06/11/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Impatto del firewall Windows su scansioni esterne

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.

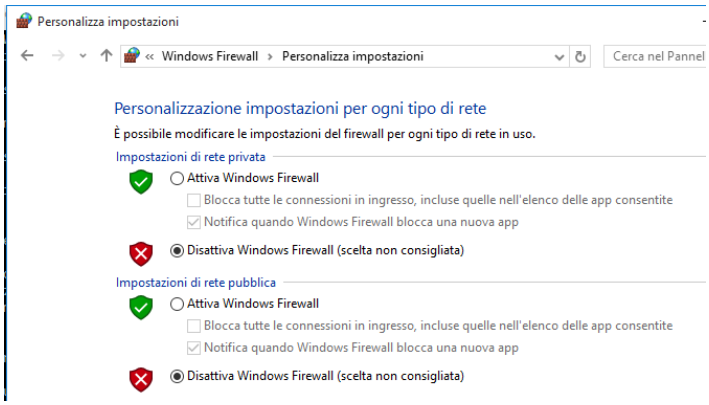
La macchina Windows, che abbiamo utilizzato, ha di default il Firewall disabilitato.

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.

Esercizio

Disattivo il firewall da Windows.

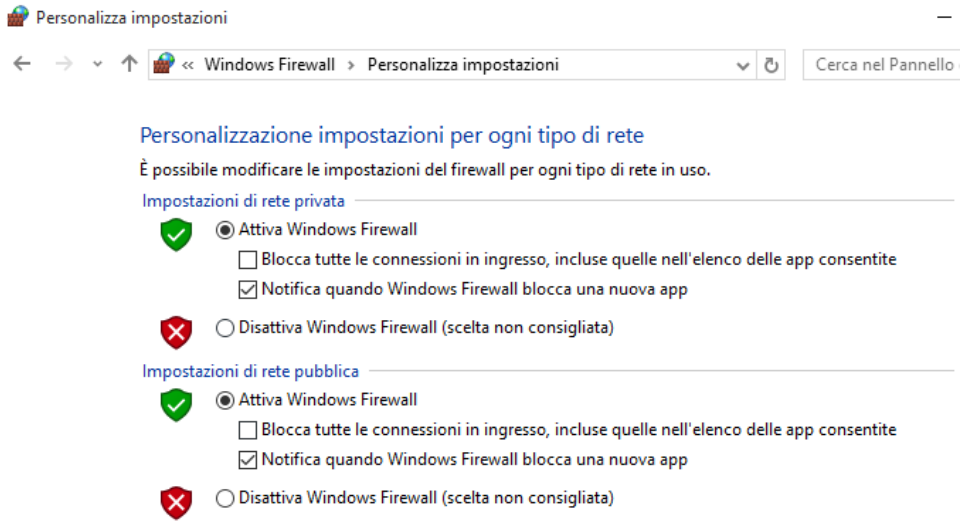


Eseguo nmap da Kali con firewall disattivato.

```
┌──(kali㉿kali)-[~/Esercizio]
└─$ nmap -sV -o nampWin_noFirewall 192.168.50.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 11:08 EST
Nmap scan report for 192.168.50.103
Host is up (0.0025s 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:AD:0A:B9 (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 172.89 seconds
```

Attivo il firewall su windows.



Lancio nmap da Kali con il firewall attivo.

```
┌──(kali㉿kali)-[~/Esercizio]
└─$ nmap -sV -o nmapWin_FirewallAttivo 192.168.50.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-05 11:13 EST
Nmap scan report for 192.168.50.103
Host is up (0.0010s 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:AD:0A:B9 (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 96.05 seconds
```

Noteremo che il firewall blocca l'accesso a molte porte riducendo le possibilità attacco.

Esercizio facoltativo – Monitoraggio dei log

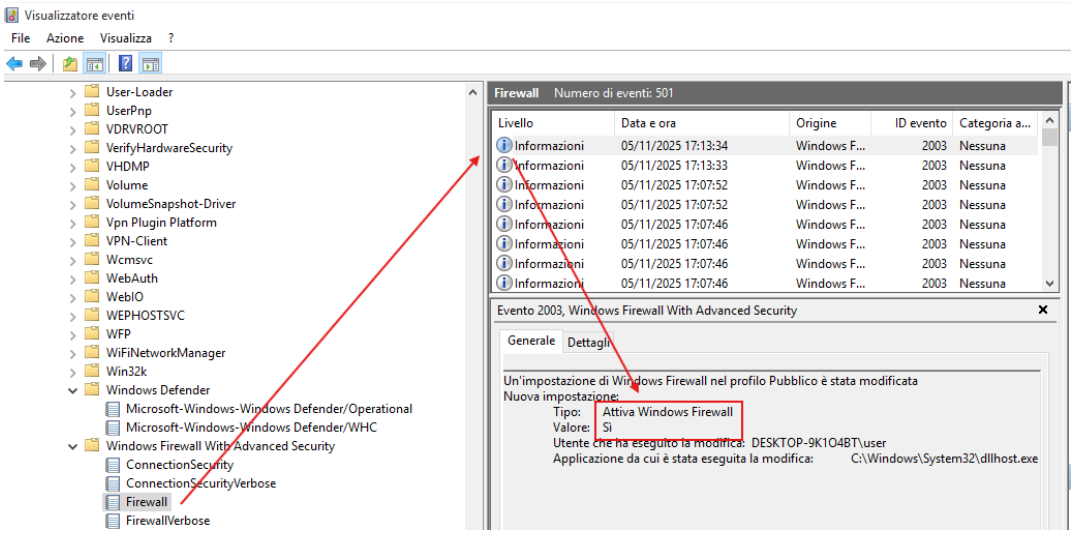
Traccia

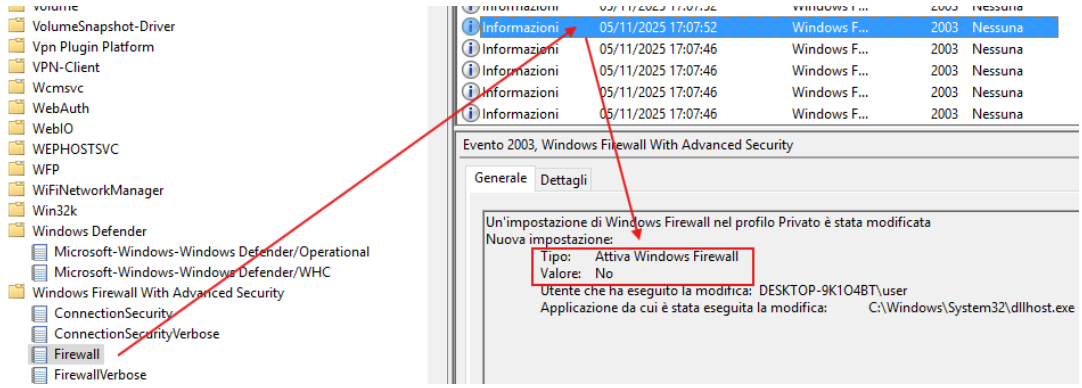
Monitorare i log di Windows durante queste operazioni:

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

Esercizio

Nei log di Windows viene rilevata sia l'abilitazione che la disabilitazione dell'antivirus.





Pratica extra: Business Continuity, Disaster Recovery e ICT

Traccia

1. Documentarsi su Business Continuity (BC) e Disaster Recovery (DR);
2. Produrre una tabella comparativa che evidenzi le differenze tra BC e DR;
3. Comprendere il concetto di ICT readiness for business continuity (IRBC - ISO/IEC 27031).

Esercizio

Business Continuity (BC)

Business Continuity (BC) è l'insieme di strategie e misure volte a garantire che un'organizzazione possa continuare a operare anche in caso di incidenti informatici (come attacchi ransomware, guasti ai server, perdita di dati, ecc) o ambientali (uragani, terremoti, incendi, ecc).

In breve:
- mira a ridurre l'interruzione delle attività;
- include piani di backup, ripristino e sistemi ridondanti;
- definisce procedure di emergenza per mantenere i servizi critici operativi;
- lavora insieme al disaster recovery, che invece si concentra sul ripristino tecnico dei sistemi IT dopo l'incidente.

Disaster Recovery (DR)

Il Disaster Recovery (DR) è l'insieme di strategie, procedure e strumenti pensati per ripristinare sistemi IT, dati e servizi critici dopo un evento grave che ne compromette la disponibilità (es. guasti hardware, attacchi informatici, incendi, blackout). Il DR assicura che l'azienda possa **riprendersi velocemente e con danni minimi** da eventi imprevisti che impattano l'infrastruttura IT.

In pratica, il DR serve a:

- Ridurre il downtime riportando i servizi operativi il più rapidamente possibile.
- Limitare la perdita di dati tramite backup, repliche e copie off-site.
- Garantire la continuità delle operazioni anche in caso di disastro.

Si basa su due parametri chiave:

- RTO (Recovery Time Objective): tempo massimo accettabile per ripristinare i servizi.
- RPO (Recovery Point Objective): quantità massima di dati che si può perdere (es. ultimi 5 minuti, 1 ora, ecc.).

Tabella comparativa

Aspetto	**Business Continuity (BC)**	**Disaster Recovery (DR)**
Obiettivo principale	Garantire che l'organizzazione continui a operare durante e dopo un incidente.	Ripristinare sistemi IT, dati e servizi critici dopo un disastro.
Focus	Continuità dei processi aziendali e dei servizi essenziali.	Ripristino tecnico dell'infrastruttura IT.
Ambito	Include procedure operative, organizzative e di gestione delle emergenze.	Include strategie, procedure e strumenti tecnici di recupero.
Tipo di eventi coperti	Eventi gravi che compromettono i sistemi IT (guasti, attacchi, incendi, blackout).	Eventi gravi che compromettono i sistemi IT (guasti, attacchi, incendi, blackout).

Misure tipiche	Sistemi ridondanti, piani di emergenza, continuità dei servizi critici.	Backup, repliche dei dati, ripristino server e infrastrutture IT.
Obiettivi chiave	Ridurre l'interruzione delle attività.	Ridurre downtime e perdita di dati.
Metriche utilizzate	Nessuna	RTO (tempo massimo per ripristinare i servizi) e RPO (massima perdita di dati accettabile).
Relazione tra BC e DR	BC fornisce il quadro generale per l'operatività dell'azienda durante un incidente.	DR è una componente della BC, focalizzato sul recupero tecnico.
Orizzonte temporale	Durante e immediatamente dopo l'incidente.	Dopo l'incidente, fino al ripristino completo o parziale dei sistemi IT.

ICT Readiness for Business Continuity (IRBC)

ICT Readiness for Business Continuity (IRBC) è il livello di preparazione delle tecnologie informatiche di un'organizzazione per garantire la continuità operativa in caso di incidenti, emergenze o disastri.

In pratica, l'IRBC rappresenta quanto l'infrastruttura IT è pronta a supportare la Business Continuity, assicurando che i servizi critici possano restare attivi o essere rapidamente ripristinati.

La norma **ISO/IEC 27031** fornisce linee guida su come progettare, implementare e migliorare un sistema che garantisca la resilienza ICT, in supporto ai piani di continuità operativa dell'organizzazione.