

# Cyber Security Report



**W18D1**

**06/11/2025**

**Autore :**

*Pace Massimiliano*

**email :** *efmpas@gmail.com*

**Indice :**

- ° Introduzione pag. 2
- ° Spiegazione esercizio e svolgimento pag.2 - 3
- ° Conclusioni pag. 4
- ° Esercizio facoltativo pag. 5 - 6



# INTRODUZIONE ESERCIZIO FIREWALL

° L'esercizio odierna punta al dimostrare come cambiano i sistemi di sicurezza delle nostre macchine con l'attivazione della protezione Firewall. Andremo a dimostrare che eseguendo una scansione delle porte troveremo dati diversi con protezione disattivata e attivata

## SPIEGAZIONE ESERCIZIO

° Avviamo sia Kali che Windows eseguiamo un ping di controllo e analizziamo la macchina target con nmap -sV per la service detection e -o per creare un file da visionare in seguito con i risultati ottenuti

Firewall spento

```
kali@kali2023: ~  
File Actions Edit View Help  
— 192.168.64.3 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 1.909/3.520/4.457/1.144 ms  
  
(kali@kali2023)-[~]  
$ nmap -sV -o dati.txt 192.168.64.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-06 13:58 CET  
  
(kali@kali2023)-[~]  
$ nmap -sV -o scansione 192.168.64.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-06 14:01 CET  
Nmap scan report for 192.168.64.3  
Host is up (0.00090s latency).  
Not shown: 981 closed tcp ports (conn-refused)  
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  ssl/ms-wbt-server?   
5357/tcp  open  http              Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
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       
Service Info: Host: DESKTOP-9K104BT; 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 161.04 seconds  
  
(kali@kali2023)-[~]  
$
```



° Ora attiviamo il Firewall e andiamo a visionare le differenze chiaramente visibili



```
kali@kali2023: ~  
File Actions Edit View Help  
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 ssl/ms-wbt-server?  
5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
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  
Service Info: Host: DESKTOP-9K104BT; 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 161.04 seconds  
  
(kali@kali2023)-[~]  
$ nmap -sV -o scansioni 192.168.64.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-06 14:10 CET  
Nmap scan report for 192.168.64.3  
Host is up (0.0065s latency).  
Not shown: 990 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  
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  
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
8443/tcp  open  ssl/https-alt  
Service Info: Host: DESKTOP-9K104BT; 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 81.45 seconds  
  
(kali@kali2023)-[~]  
$
```

° Ora con il firewall attivo risultano meno porte aperte e le porte risultano filtrate. Le porte risultano filtrate quando non vi e' risposta alla scansione.



# CONCLUSIONI

Attivando i firewall nel nostro target , si verra' a creare una protezione maggiore. Alcune porte risultano bloccate dall'esterno ed essendo le altre filtrate avremo una macchina piu' sicura agli attacchi. Le impostazioni Firewall sono numerose si possono creare regole come abbiamo fatto in precedenza ed in altri esercizi e si possono chiudere anche tutte le porte rimanenti creando un target a prova di LUCA e MILENA.



# Esercizio Facoltativo

## Business Continuity

riguarda tutte le strategie i processi e le soluzioni che permette a un'azienda di mantenere i servizi essenziali attivi durante e dopo un'emergenza limitando al minimo le interruzione operative e proteggendo la reputazione le finanze e i clienti.

## Disaster recovery

si concentrano sulle procedure tecniche e operative per ripristinare sistemi IT dati e applicazioni dopo che si è verificato un disastro. L'obiettivo è tornare il più rapidamente possibile allo stato normale delle operazioni IT.

### TABELLA COMPARATIVA

| Titolo                      | Obiettivo   | Attivazione   | Azioni        | Tempistiche   |
|-----------------------------|---|---|---------------|---|
| <b>Continuità Operativa</b> | Garantire la continuità delle operazioni durante interruzioni | Eventi che minacciano l'operatività (es. guasti tecnici)                              | Fino a 72     | Sviluppo di un piano di continuità, test regolari       |
| <b>Attivazione</b>          | Tutte le funzioni aziendali essenziali                        | (es. pandemie, guasti tecnici, guasti naturali)                                       | Fino a 72 ore | Esempi  |
| <b>Ambito</b>               | Tutte le funzioni aziendali essenziali                        | Pianificazione preventiva, trasferimento delle attività, gestione della comunicazione | trasferimento | Sviluppo di un piano di continuità, test regolari       |
| Titolo                      |   |   |               |   |
| <b>Recupero Disastri</b>    | Ripristinare le operazioni dopo un disastro                   | Eventi catastrofici (es. incendi, terremoti)  | Ore/giorni    | Sistemi informativi e infrastrutture chiave             |
| <b>Azioni</b>               | Sistemi informativi e infrastrutture chiave                   | Ripristino dei dati, ripristino delle applicazioni, verifica della funzionalità       | Ore/giorni    | Backup dei dati, replica dei server, test di ripristino |



# Concetto di ICT readiness for business continuity secondo IRBC (ISO/IEC 27031)

ICT Readiness for Business Continuity (IRBC): Secondo la ISO/IEC 27031, ICT readiness significa preparare in modo strutturato sistemi informatici e di comunicazione per supportare e garantire la continuità operativa rispetto a ogni tipo di evento disruptive.

Il framework include:

Analisi delle dipendenze critiche nei sistemi, inclusi server, reti, applicazioni.

Definizione di obiettivi come il Recovery Time Objective (RTO – tempo massimo accettabile di inattività) e Recovery Point Objective (RPO – perdita massima di dati tollerabile).

Implementazione di resilienza (ridondanza, backup, test periodici dell'efficacia dei piani).

Integrazione con la gestione della sicurezza delle informazioni e dei processi di business continuity.

La norma ISO/IEC 27031 offre alle organizzazioni una guida fondamentale per assicurare che le infrastrutture ICT siano in grado di sostenere l'operatività anche in condizioni di emergenza e siano in grado di riprendersi secondo i tempi prefissati.