

Security Operation: azioni preventive

★ INDICE

1 **Introduzione e obiettivi**

2 **[Official] Firewall completo**

 2.1 Explorando Firewall e Sicurezza di Rete

 2.2 Configurazione Firewall Windows

 2.3 Analisi e Risultati

3 **[Facoltativo] Monitoraggio log**

 3.1 Explorando Windows Event Logs

 3.2 Monitoraggio durante Operazioni Firewall

4 **[Extra] Business Continuity**

 4.1 Business Continuity Fundamentals

 4.2 Disaster Recovery (DR) Implementation

 4.3 IRBC Framework Integration

 4.4 Integration Strategy

 4.5 Industry-Specific Applications

5 **Conclusione e Best Practices**

 5.1 Executive Summary delle Scoperte

 5.2 Scoperte Critiche Identificate

 5.3 Compliance Assessment

 5.4 Strategic Recommendations

 5.5 Key Performance Indicators

 5.6 Lessons Learned Professionali

 5.7 Final Assessment

1 Introduzione e obiettivi

Obiettivo dell'Esercitazione

Questo esame pratico mira a dimostrare l'importanza delle **azioni preventive** nella sicurezza informatica, focalizzandosi sui meccanismi di protezione a livello di rete attraverso la configurazione e gestione dei firewall.

Competenze Sviluppate

- Comprensione del funzionamento dei firewall Windows
- Analisi dell'impatto delle misure di sicurezza sulla superficie d'attacco
- Tecniche di scansione e riconoscimento con Nmap
- Monitoraggio e analisi dei log di sistema
- Concetti fondamentali di Business Continuity e Disaster Recovery

Ambienti di Lavoro

Macchina Attaccante:

- Kali Linux con Nmap pre-installato
- Privilegi root per eseguire scansioni complete
- Connessione verso la macchina target

Macchina Target:

- Windows 10 Pro con Windows Defender Firewall
- Servizi attivi per simulazione realistica
- Privilegi amministratore per configurazione firewall

2 [Official] Firewall completo

2.1 Exploid Firewall e Sicurezza di Rete

Cos'è un Firewall?

Un **firewall** è un sistema di sicurezza che monitora e controlla il traffico di rete in entrata e in uscita basandosi su regole di sicurezza predeterminate. Funziona come una barriera tra una rete interna fidata e reti esterne non fidate.

Tipi di Firewall

1. **Packet Filtering Firewall:** Analizza i pacchetti IP e filtra in base a indirizzi IP, porte e protocolli

Esempio: Blocca tutte le connessioni alla porta 22 (SSH) da IP esterni

2. **Stateful Inspection:** Mantiene informazioni sullo stato delle connessioni Attive

Esempio: Permette risposta a richieste legittime in uscita

3. **Application Gateway:** Opera a livello applicazione, controllando protocolli specifici

Esempio: Filtra traffico web su porta 80 per contenuti non autorizzati

4. **Next-Generation Firewall (NGFW):** Includono funzionalità avanzate come IPS e controllo applicazioni

Esempio: Blocca applicazioni social media durante l'orario lavorativo

Windows Firewall

Il **Windows Firewall** (in precedenza chiamato Internet Connection Firewall) è il sistema di protezione nativo dei sistemi operativi Windows, caratteristiche principali:

- **Configurazione Profili:** Domain, Private, Public
- **Regole Inbound/Outbound:** Controllo traffico in entrata e uscita
- **Application Rules:** Controllo per programmi specifici
- **Integration:** Integrato con Windows Defender Security Center

Impatto delle Regole Firewall

Le regole firewall influenzano direttamente la **superficie d'attacco** di un sistema:

| Aspetto | Senza Firewall | Con Firewall Attivo |
|------------------|---------------------------|--------------------------|
| Servizi Esposti | Tutti i servizi attivi | Solo servizi autorizzati |
| Porte Aperte | Tutte le porte in ascolto | Solo porte consentite |
| Scansioni Nmap | Informazioni complete | Informazioni limitate |
| Rischio Attacchi | Molto Alto 😠 | Ridotto 😊 |

2.2 Configurazione Firewall Windows

Obiettivo

Verificare l'impatto dell'attivazione del Windows Firewall sui risultati di scansioni Nmap condotte dall'esterno.

Prerequisites

- Macchina Windows con Windows Firewall disabilitato
- Attaccante con Nmap installato
- Rete di laboratorio configurata

Procedura Step-by-Step

STEP 1: Verifica Stato Iniziale del Firewall

Comandi da eseguire sulla macchina Windows:

```
powershell

# Verifica stato Windows Defender Firewall
Get-NetFirewallProfile | Format-Table Name, Enabled

# Verifica con Command Prompt
netsh advfirewall show allprofiles state

# Verifica servizio
Get-Service MMCSS | Format-Table Status, StartType
```

```
Administrator: Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.
PS C:\Users\user> # Verifica stato Windows Defender Firewall
PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled
Name      Enabled
----      -----
Domain    True
Private   True
Public    True

PS C:\Users\user> # Verifica con Command Prompt
PS C:\Users\user> netsh advfirewall show allprofiles state
Impostazioni Profilo di dominio:
Stato          ON
Impostazioni Profilo privato:
Stato          ON
Impostazioni Profilo pubblico:
Stato          ON
OK.

PS C:\Users\user> # Verifica servizio
PS C:\Users\user> Get-Service MMCSS | Format-Table Status, StartType
Status StartType
---- -----------
Running
```

Firewall: ABILITATO su tutti i profili (Domain, Private, Public)

STEP 2: Prima Scansione Nmap (Firewall DISABILITATO)

Comandi da eseguire sulla macchina Windows:

```
# Disabilita tutti i profili del firewall
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False

# Verifica lo stato
Get-NetFirewallProfile | Format-Table Name, Enabled
```

```
PS C:\Users\user> Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False
PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled
Name      Enabled
----      -----
Domain    False
Private   False
Public    False

PS C:\Users\user>
```

Firewall disabilitato con successo!

Ora procediamo con la PRIMA scansione Nmap - quella senza firewall per vedere l'intera superficie di attacco.

Sulla macchina Kali Linux eseguo scansione completa:

```
nmap -sV -sC -A -T4 192.168.50.102
```

Spiegazione del comando:

- **-sV** Rileva le versioni dei servizi
- **-sC** Esegue gli script standard di Nmap
- **-A** Rilevamento avanzato (OS, versione, ecc.)
- **-T4** Timing aggressivo (più veloce)

```
(M6DR6㉿kali)-[~]
$ nmap -sV -sC -A -T4 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-04 11:03 EST
Nmap scan report for 192.168.50.102
Host is up (0.0012s 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   Microsoft Windows qotd (English)
19/tcp     open  chargen
80/tcp     open  http   Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
| http-server-header: Microsoft-IIS/10.0
| http-title: IIS Windows
135/tcp    open  msrpc  Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows 10 Pro 10240 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
| rdp-ntlm-info:
| Target_Name: DESKTOP-9K104BT
| NetBIOS_Domain_Name: DESKTOP-9K104BT
| NetBIOS_Computer_Name: DESKTOP-9K104BT
| DNS_Domain_Name: DESKTOP-9K104BT
| DNS_Computer_Name: DESKTOP-9K104BT
| Product_Version: 10.0.10240
| System_Time: 2025-11-04T16:05:59+00:00
| ssl-cert: Subject: commonName=DESKTOP-9K104BT
| Not valid before: 2025-10-13T13:06:04
| Not valid after: 2026-04-14T13:06:04
|_ ssl-date: 2025-11-04T16:06:16+00:00; +10s from scanner time.
5432/tcp   open  postgresql?
8009/tcp   open  ajp13   Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp   open  http   Apache Tomcat/Coyote JSP engine 1.1
| http-title: Apache Tomcat/7.0.81
| http-favicon: Apache Tomcat
| http-server-header: Apache-Coyote/1.1
8443/tcp   open  ssl/https-alt
| ssl-cert: Subject: commonName=DESKTOP-9K104BT
| Not valid before: 2024-07-09T16:53:31
| Not valid after: 2029-07-09T16:53:31
|_ http-title: Not_Found
| http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-9K104BT; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: DESKTOP-9K104BT, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| hnik/Oracle VirtualBox virtual NIC
|_clock-skew: mean: -11m50s, deviation: 26m49s, median: 8s
| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
| message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Windows 10 Pro 10240 (Windows 10 Pro 6.3)
| OS CPE: cpe:/o:microsoft:windows_10:-
| Computer name: DESKTOP-9K104BT
| NetBIOS computer name: DESKTOP-9K104BT\x00
| Workgroup: WORKGROUP\x00
| System time: 2025-11-04T17:06:00+01:00
| smb2-security-mode:
| 3:1:1:
| Message signing enabled but not required
| smb2-time:
| date: 2025-11-04T16:06:00
| start_date: 2025-11-04T13:00:45
TRACEROUTE (---)
HOP RTT      ADDRESS
1  1.21ms  192.168.50.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.31 seconds
```

RISULTATI PRIMA SCANSIONE (Firewall OFF)

Informazioni Sistema

- **Target:** 192.168.50.102 (DESKTOP-9K1O4BT)
- **OS:** Windows 10 Pro build 10240 (1507-1607)
- **MAC:** 08:00:27:6C:49:0D (VirtualBox)
- **Workgroup:** WORKGROUP

Servizi e Porte Aperte (ATTACK SURFACE AMPIA)

Servizi Windows Nativi Critici:

| Porta | Servizio | Descrizione | Rischio |
|----------|---------------|-------------------------|---------|
| 135/tcp | Microsoft RPC | Remote Procedure Call | |
| 139/tcp | NetBIOS-SSN | NetBIOS Session Service | |
| 445/tcp | Microsoft-DS | SMB File Sharing | |
| 3389/tcp | MS-WBT-Server | Remote Desktop Protocol | |

Servizi Web Esposti:

| Porta | Servizio | Versione | Rischio |
|----------|---------------|-----------------------|---------|
| 80/tcp | Microsoft IIS | 10.0 | |
| 8080/tcp | Apache Tomcat | 7.0.81 | |
| 8443/tcp | SSL/HTTPS-alt | Microsoft-HTTPAPI/2.0 | |

Altri Servizi:

| Porta | Servizio | Descrizione | Rischio |
|--------|----------|---------------------------------|---------|
| 7/tcp | Echo | Echo Protocol | |
| 9/tcp | Discard | Discard Protocol | |
| 13/tcp | Daytime | Microsoft International Daytime | |

| Porta | Servizio | Descrizione | Rischio |
|----------|------------|-------------------------|---------|
| 17/tcp | QOTD | Windows QOTD | |
| 19/tcp | Chargen | Character Generator | |
| 1801/tcp | MSMQ | Microsoft Message Queue | |
| 2103/tcp | RPC | Microsoft Windows RPC | |
| 2105/tcp | RPC | Microsoft Windows RPC | |
| 2107/tcp | RPC | Microsoft Windows RPC | |
| 5432/tcp | PostgreSQL | Database Server | |
| 8009/tcp | AJP13 | Apache Jserv Protocol | |

Security Issues Rilevate:

1. **RDP Esposto (3389)**: Accesso remoto possibile
2. **SMB Condivisioni (445)**: Enumerazione di file e cartelle
3. **RPC Multiple Endpoint**: Diversi punti di accesso RPC
4. **Database PostgreSQL**: Accesso database pubblico
5. **IIS Web Server**: Server web con metodi potenzialmente rischiosi
6. **Apache Tomcat**: Application server esposto

ATTACK SURFACE SUMMARY

- **Porte aperte totali**: 17
- **Servizi critici esposti**: 8
- **Livello rischio generale**:
- **Tempo scansione**: 183.31 secondi

CERTIFICATI SSL RILEVATI

1. Porta 3389 (RDP):

- Subject: DESKTOP-9K1O4BT
- Valido fino: 2026-04-14T13:06:04

2. Porta 8443 (HTTPS):

- Subject: DESKTOP-9K1O4BT
- Valido fino: 2029-07-09T16:53:31

STEP 3: Seconda scansione Nmap (Firewall ABILITATO)

Ho riscontrato un problema di configurazione risolvo così

```
Correggo il Domain Profile
```

```
Set-NetFirewallProfile -Profile Domain -DefaultInboundAction Block
```

```
Verifico la correzione
```

```
Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction, DefaultOutboundAction
```

```
Controllo su quale profilo sono connesso
```

```
Get-NetConnectionProfile
```

The screenshot shows a Windows PowerShell window with the title bar "Amministratore: Windows PowerShell". The content of the window is as follows:

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction, DefaultOutboundAction
Name      Enabled DefaultInboundAction DefaultOutboundAction
----      --     --     --
Domain    True      NotConfigured      NotConfigured
Private   True      Block            Allow
Public    True      Block            Allow

PS C:\Users\user> Set-NetFirewallProfile -Profile Domain -DefaultInboundAction Block
PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction, DefaultOutboundAction
Name      Enabled DefaultInboundAction DefaultOutboundAction
----      --     --     --
Domain    True      Block            NotConfigured
Private   True      Block            Allow
Public    True      Block            Allow

PS C:\Users\user> Get-NetConnectionProfile

Name          : Rete non identificata
InterfaceAlias : Lan 1
InterfaceIndex : 10
NetworkCategory : Public
IPv4Connectivity : NoTraffic
IPv6Connectivity : NoTraffic

Name          : Rete 7
InterfaceAlias : DHCP
InterfaceIndex : 15
NetworkCategory : Public
IPv4Connectivity : Internet
IPv6Connectivity : NoTraffic

PS C:\Users\user>
```

Firewall riabilitato con successo!

- **Domain Profile:** DefaultInboundAction = **Block**
- **Private Profile:** DefaultInboundAction = **Block**
- **Public Profile:** DefaultInboundAction = **Block**

SCOPERTA CRITICA: PROFILO DI RETE

Dal comando **Get-NetConnectionProfile** vedo:

- **NetworkCategory:** Public
- Sono connesso con il profilo **Public** (non Domain)

Ora che tutti i profili sono configurati correttamente con Block come default, le porte potrebbero ancora essere aperte se ci sono **regole Allow esplicite**

Analisi Regole Allow Attive

Esegui questo comando per vedere tutte le regole che **permettono** l'accesso:

```
Get-NetFirewallRule | Where-Object {$_ Action -eq "Allow" -and $_ Enabled -eq "True"} | Select-Object DisplayName, Direction, Action, LocalPort | Format-Table -AutoSize
```

| DisplayName | Direction | Action | LocalPort |
|---|-----------|--------|-----------|
| Ottimizzazione recapito (TCP-In) | Inbound | Allow | |
| Ottimizzazione recapito (UDP-In) | Inbound | Allow | |
| Condivisione prossimità su TCP (Condivisione TCP-In) | Inbound | Allow | |
| Condivisione prossimità su TCP (Condivisione TCP-Out) | Outbound | Allow | |
| Individuazione rete (SSDP-In) | Inbound | Allow | |
| Individuazione rete (SSDP-Out) | Outbound | Allow | |
| Individuazione rete (UPnP-In) | Inbound | Allow | |
| Individuazione rete (UPnP-Out) | Outbound | Allow | |
| Individuazione rete (UPnPHost-Out) | Outbound | Allow | |
| Individuazione rete (NB-Name-In) | Inbound | Allow | |
| Individuazione rete (NB-Name-Out) | Outbound | Allow | |
| Individuazione rete (NB-Datagram-In) | Inbound | Allow | |
| Individuazione rete (NB-Datagram-Out) | Outbound | Allow | |
| Individuazione rete (WSD-In) | Inbound | Allow | |
| Individuazione rete (WSD-In) | Inbound | Allow | |
| Individuazione rete (WSD-Out) | Outbound | Allow | |
| Individuazione rete (LLMNR-UDP-In) | Inbound | Allow | |
| Individuazione rete (LLMNR-UDP-Out) | Outbound | Allow | |
| Individuazione rete (Pub-WSD-In) | Inbound | Allow | |
| Individuazione rete (Pub WSD-Out) | Outbound | Allow | |
| Individuazione rete (WSD EventsSecure-In) | Inbound | Allow | |
| Individuazione rete (WSD EventsSecure-Out) | Outbound | Allow | |
| Individuazione rete (WSD Events-In) | Inbound | Allow | |
| Individuazione rete (WSD Events-Out) | Outbound | Allow | |
| Schermo wireless (TCP-In) | Inbound | Allow | |
| Schermo wireless (TCP-Out) | Outbound | Allow | |
| Schermo wireless (UDP-Out) | Outbound | Allow | |
| Assistenza remota (TCP-In) | Inbound | Allow | |
| Assistenza remota (TCP-Out) | Outbound | Allow | |
| Assistenza remota (PNRP-In) | Inbound | Allow | |
| Assistenza remota (PNRP-Out) | Outbound | Allow | |
| Assistenza remota (server Assistenza remota TCP-In) | Inbound | Allow | |
| Assistenza remota (server Assistenza remota TCP-Out) | Outbound | Allow | |
| Assistenza remota (DCOM-In) | Inbound | Allow | |
| Assistenza remota (TCP-In) | Inbound | Allow | |
| Assistenza remota (TCP-Out) | Outbound | Allow | |
| Assistenza remota (SSDP UPD-In) | Inbound | Allow | |
| Assistenza remota (SSDP UPD-Out) | Outbound | Allow | |
| Assistenza remota (SSDP TCP-In) | Inbound | Allow | |
| Assistenza remota (SSDP TCP-Out) | Outbound | Allow | |

| | | |
|---|----------|-------|
| Assistenza remota (PNRP-In) | Inbound | Allow |
| Assistenza remota (PNRP-Out) | Outbound | Allow |
| Server protocollo DIAL (HTTP-In) | Inbound | Allow |
| Server protocollo DIAL (HTTP-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (HTTP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (HTTP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (HTTP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTCP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTCP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTCP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTCP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTP-Streaming-In) | Outbound | Allow |
| Server di flusso Cast nel dispositivo (RTP-Streaming-In) | Outbound | Allow |
| Server di flusso Cast nel dispositivo (RTP-Streaming-Out) | Outbound | Allow |
| Server di flusso Cast nel dispositivo (RTP-Streaming-Out) | Outbound | Allow |
| Server di flusso Cast nel dispositivo (RTSP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTSP-Streaming-In) | Inbound | Allow |
| Server di flusso Cast nel dispositivo (RTSP-Streaming-In) | Inbound | Allow |
| Cast nel dispositivo - Individuazione SSDP (UDP-In) | Inbound | Allow |
| Cast nel dispositivo - Eventi UPnP (TCP-In) | Inbound | Allow |
| Funzionalità Cast nel dispositivo (qWave-UDP-In) | Inbound | Allow |
| Funzionalità Cast nel dispositivo (qWave-UDP-Out) | Outbound | Allow |
| Funzionalità Cast nel dispositivo (qWave-TCP-In) | Inbound | Allow |
| Funzionalità Cast nel dispositivo (qWave-TCP-Out) | Outbound | Allow |
| Individuazione rete Wi-Fi Direct (In) | Inbound | Allow |
| Individuazione rete Wi-Fi Direct (Out) | Outbound | Allow |
| Utilizzo spooler Wi-Fi Direct (In) | Inbound | Allow |
| Utilizzo spooler Wi-Fi Direct (Out) | Outbound | Allow |
| Utilizzo servizio di digitalizzazione Wi-Fi Direct (In) | Inbound | Allow |
| Utilizzo servizio di digitalizzazione Wi-Fi Direct (Out) | Outbound | Allow |
| Protocollo coordinamento ASP WFD (UDP-In) | Inbound | Allow |
| Protocollo coordinamento ASP WFD (UDP-Out) | Outbound | Allow |
| Funzionalità di base rete - Destinazione non raggiungibile (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Pacchetto di dimensioni troppo grandi (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Pacchetto di dimensioni troppo grandi (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Tempo scaduto (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Tempo scaduto (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Problema parametro (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Problema parametro (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Richiesta individuazione router adiacenti (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Richiesta individuazione router adiacenti (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Annuncio individuazione router adiacenti (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Annuncio individuazione router adiacenti (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Annuncio router (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Annuncio router (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Richiesta router (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Richiesta router (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Query listener multicast (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Query listener multicast (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Report listener multicast (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Report listener multicast (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Report listener multicast v2 (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Report listener multicast v2 (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Listener multicast completato (ICMPv6-In) | Inbound | Allow |
| Funzionalità di base rete - Listener multicast completato (ICMPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Destinazione non raggiungibile, necessaria frammentazione (ICMPv4-In) | Inbound | Allow |
| Funzionalità di base rete - IGMP (Internet Group Management Protocol) (IGMP-In) | Inbound | Allow |
| Funzionalità di base rete - IGMP (Internet Group Management Protocol) (IGMP-Out) | Outbound | Allow |
| Funzionalità di base rete - DHCP (Dynamic Host Configuration Protocol) (DHCP-In) | Inbound | Allow |
| Funzionalità di base rete - DHCP (Dynamic Host Configuration Protocol) (DHCP-Out) | Outbound | Allow |
| Funzionalità di base rete - Dynamic Host Configuration Protocol per IPv6 (DHCPV6-In) | Inbound | Allow |
| Funzionalità di base rete - Dynamic Host Configuration Protocol per IPv6 (DHCPV6-Out) | Outbound | Allow |
| Funzionalità di base rete - Teredo (UDP-In) | Inbound | Allow |
| Funzionalità di base rete - Teredo (UDP-Out) | Outbound | Allow |
| Funzionalità di base rete - IPHTTPS (TCP-In) | Inbound | Allow |
| Funzionalità di base rete - IPHTTPS (TCP-Out) | Outbound | Allow |
| Funzionalità di base rete - IPv6 (IPv6-In) | Inbound | Allow |
| Funzionalità di base rete - IPv6 (IPv6-Out) | Outbound | Allow |
| Funzionalità di base rete - Criteri di gruppo (NP-Out) | Outbound | Allow |
| Funzionalità di base rete - Criteri di gruppo (TCP-Out) | Outbound | Allow |
| Funzionalità di base rete - DNS (UDP-Out) | Outbound | Allow |
| Funzionalità di base rete - Criteri di gruppo (LSASS-Out) | Outbound | Allow |
| Desktop remoto - Modalità utente (TCP-In) | Inbound | Allow |
| Desktop remoto - Modalità utente (UDP-In) | Inbound | Allow |
| Desktop remoto - Shadow (TCP-In) | Outbound | Allow |
| Il tuo account | Inbound | Allow |
| Il tuo account | Outbound | Allow |
| Il tuo account | Inbound | Allow |
| Il tuo account | Outbound | Allow |
| Il tuo account | Inbound | Allow |
| Account aziendale o dell'istituto di istruzione | Outbound | Allow |
| Account aziendale o dell'istituto di istruzione | Inbound | Allow |
| Email e account | Outbound | Allow |
| Schermata di blocco predefinita di Windows | Outbound | Allow |
| Microsoft Edge | Outbound | Allow |
| Microsoft Edge | Inbound | Allow |
| Contenuti in evidenza di Windows | Outbound | Allow |
| Cerca | Outbound | Allow |
| Cerca | Inbound | Allow |
| Restrizioni famiglia Microsoft | Outbound | Allow |
| Windows Feedback | Outbound | Allow |
| Xbox Game UI | Outbound | Allow |
| Provider di identità Xbox | Outbound | Allow |
| Contatta il supporto | Outbound | Allow |
| Contatta il supporto | Inbound | Allow |
| PurchaseDialog | Outbound | Allow |
| MSN Money | Outbound | Allow |
| MSN Money | Inbound | Allow |
| Meteo | Outbound | Allow |
| Meteo | Inbound | Allow |

Matteo Mattia – Cyber Security & Ethical Hacking

| | | |
|--|----------|-------|
| Posta e Calendario | Inbound | Allow |
| Get started | Outbound | Allow |
| MSN Notizie | Outbound | Allow |
| MSN Notizie | Inbound | Allow |
| Microsoft Foto | Outbound | Allow |
| Microsoft Foto | Inbound | Allow |
| Store | Outbound | Allow |
| Store | Inbound | Allow |
| Xbox | Outbound | Allow |
| Xbox | Inbound | Allow |
| Film e programmi TV | Outbound | Allow |
| Musica | Outbound | Allow |
| Connessione guidata cellulare Microsoft | Outbound | Allow |
| Mappe Windows | Outbound | Allow |
| Contatti Microsoft | Outbound | Allow |
| OneNote | Outbound | Allow |
| OneNote | Inbound | Allow |
| Microsoft Solitaire Collection | Outbound | Allow |
| Microsoft Solitaire Collection | Inbound | Allow |
| MSN Sport | Outbound | Allow |
| MSN Sport | Inbound | Allow |
| Connettore app | Outbound | Allow |
| 3D Builder | Outbound | Allow |
| Condivisione file e stampanti (LLMNR-UDP-Out) | Inbound | Allow |
| Condivisione file e stampanti (LLMNR-UDP-In) | Outbound | Allow |
| Condivisione file e stampanti (richiesta echo - ICMPv6-Out) | Inbound | Allow |
| Condivisione file e stampanti (richiesta echo - ICMPv6-In) | Outbound | Allow |
| Condivisione file e stampanti (richiesta echo - ICMPv4-Out) | Inbound | Allow |
| Condivisione file e stampanti (richiesta echo - ICMPv4-In) | Outbound | Allow |
| Condivisione file e stampanti (servizio spooler - RPC-EPMAP) | Inbound | Allow |
| Condivisione file e stampanti (servizio spooler - RPC) | Outbound | Allow |
| Condivisione file e stampanti (NB-Datagram-Out) | Inbound | Allow |
| Condivisione file e stampanti (NB-Datagram-In) | Outbound | Allow |
| Condivisione file e stampanti (NB-Name-Out) | Inbound | Allow |
| Condivisione file e stampanti (NB-Name-In) | Outbound | Allow |
| Condivisione file e stampanti (SMB-Out) | Inbound | Allow |
| Condivisione file e stampanti (SMB-In) | Outbound | Allow |
| Condivisione file e stampanti (NB-Session-Out) | Inbound | Allow |
| Servizio peer caching BITS (NB-Session-In) | Outbound | Allow |
| Servizio SNMP (UDP In) | Inbound | Allow |
| Servizio SNMP (UDP Out) | Outbound | Allow |
| Servizio SNMP (UDP In) | Inbound | Allow |
| Servizio SNMP (UDP Out) | Outbound | Allow |
| Accodamento messaggi - TCP in ingresso | Inbound | Allow |
| Accodamento messaggio - TCP in uscita | Outbound | Allow |
| Accodamento messaggi - UDP in ingresso | Inbound | Allow |
| Accodamento messaggi - UDP in uscita | Outbound | Allow |
| WMS Service Discovery Protocol | Inbound | Allow |
| WMS Service Remote Management | Inbound | Allow |
| WMS Service Remote Management Secure | Inbound | Allow |
| WMS Session Agent | Inbound | Allow |
| Client di gestione Hyper-V - WMI (DCOM-In) | Inbound | Allow |
| WMS Service | Inbound | Allow |
| Client di gestione Hyper-V - WMI (TCP-In) | Outbound | Allow |
| Client di gestione Hyper-V - WMI (TCP-Out) | Inbound | Allow |
| Client di gestione Hyper-V - WMI (Async-In) | Outbound | Allow |
| Account aziendale o dell'istituto di istruzione | Inbound | Allow |
| Account aziendale o dell'istituto di istruzione | Outbound | Allow |
| Il tuo account | Outbound | Allow |
| Il tuo account | Inbound | Allow |
| Email e account | Outbound | Allow |
| Schermata di blocco predefinita di Windows | Outbound | Allow |
| Microsoft Edge | Outbound | Allow |
| Microsoft Edge | Inbound | Allow |
| Contenuti in evidenza di Windows | Outbound | Allow |
| Cerca | Outbound | Allow |
| Cerca | Inbound | Allow |
| Restrizioni famiglia Microsoft | Outbound | Allow |
| Windows Feedback | Outbound | Allow |
| Xbox Game UI | Outbound | Allow |
| Provider di identità Xbox | Outbound | Allow |
| Contatta il supporto | Outbound | Allow |
| Contatta il supporto | Inbound | Allow |
| PurchaseDialog | Outbound | Allow |
| MSN Notizie | Outbound | Allow |
| MSN Notizie | Inbound | Allow |
| MSN Money | Outbound | Allow |
| MSN Money | Inbound | Allow |
| Posta e Calendario | Outbound | Allow |
| Posta e Calendario | Inbound | Allow |
| Meteo | Outbound | Allow |
| Meteo | Inbound | Allow |
| Get started | Outbound | Allow |
| Microsoft Foto | Outbound | Allow |
| Microsoft Foto | Inbound | Allow |
| Xbox | Outbound | Allow |
| Xbox | Inbound | Allow |
| Store | Outbound | Allow |
| Store | Inbound | Allow |
| Film e programmi TV | Outbound | Allow |
| Musica | Outbound | Allow |
| Connessione guidata cellulare Microsoft | Outbound | Allow |
| Mappe Windows | Outbound | Allow |
| Contatti Microsoft | Outbound | Allow |
| OneNote | Outbound | Allow |
| OneNote | Inbound | Allow |
| Microsoft Solitaire Collection | Outbound | Allow |
| Microsoft Solitaire Collection | Inbound | Allow |

```
Get-Office  
Get-Office  
MSN-Sport  
MSN-Sport  
Connettore-app  
3D-Builders  
Allow-RDP  
W3D4_ping  
Google-Chrome-(mDNS-In)  
  
Outbound Allow  
Inbound Allow  
Outbound Allow  
Inbound Allow  
Outbound Allow  
Outbound Allow  
Inbound Allow  
Inbound Allow  
Inbound Allow  
  
PS C:\Users\user> Get-NetFirewallRule | Where-Object {$_ .Action -eq "Allow" -and $_ .Enabled -eq "True"} | Select-Object  
DisplayName, Direction, Action, LocalPort | Format-Table -AutoSize
```

Dall'output vedo **CENTINAIA** di regole Allow attive!

Questo spiega **esattamente** perché le porte rimangono aperte.

REGOLE CRITICHE IDENTIFICATE:

Queste regole spiegano le porte aperte nella scansione Nmap:

1. "Condivisione file e stampanti (SMB-In)" → Porta 445 (SMB) APERTA
2. "Desktop remoto - Modalità utente (TCP-In)" → Porta 3389 (RDP) APERTA
3. "Allow RDP" → Seconda regola RDP
4. "Accodamento messaggi - TCP in ingresso" → Porte RPC APERTE
5. "Condivisione prossimità su TCP (Condivisione TCP-In)" → Altre porte TCP APERTE

IMPATTO DELLE REGOLE ALLOW:

- Windows 10 ha 100+ regole Allow preconfigurate per servizi "sicuri"
- Queste regole sovrascrivono il DefaultInboundAction = Block
- È una configurazione "user-friendly" ma **insecure** per default

Sulla macchina Kali Linux rieseguo scansione completa:

```
nmap -sV -sC -A -T4 192.168.50.102
```

ANALISI COMPLETA! RISULTATI IDENTICI CONFERMATI!

SUMMARY FINALE DELLE TRE SCANSIONI

| # Scansione | Stato Firewall | Porte Aperte | Risultato |
|-------------|--------------------------------------|--------------|---------------|
| 1 | DISABILITATO | 17 | Baseline |
| 2 | ABILITATO (con Domain NotConfigured) | 17 | NO DIFFERENCE |
| 3 | ABILITATO (con Domain Block) | 17 | NO DIFFERENCE |

SCOPERTA CRITICA: 😞

Il firewall Windows 10 **NON** è "secure by default" ma è "user-friendly by default" - permette 100+ servizi per default anche quando il firewall è "abilitato".

2.3 Analisi e Risultati

2.3.1 Overview dei Risultati delle Scansioni

Metodologia di Test Implementata

Per valutare l'impatto del Windows Defender Firewall sull'attack surface del sistema target, è stata implementata una metodologia di test in tre fasi sequenziali:

1. **Fase 1:** Scansione baseline con firewall disabilitato
2. **Fase 2:** Scansione di verifica con firewall abilitato (configurazione originale)
3. **Fase 3:** Scansione di validazione con firewall correttamente configurato

Parametri di Scansione Uniformi

Tutte le scansioni sono state eseguite utilizzando i medesimi parametri Nmap:

- **Comando:** nmap -sV -sC -A -T4 192.168.50.102
- **Target:** DESKTOP-9K1O4BT (Windows 10 Pro build 10240)
- **IP Address:** 192.168.50.102
- **Network:** VirtualBox host-only network (1 hop)

2.3.2 Risultati Dettagliati per Ogni Scansione

SCANSIONE 1: Firewall DISABILITATO (Baseline)

Timestamp: 2025-11-04 11:03 EST

Durata: 183.31 secondi

Stato Sistema: Attack surface massima

Servizi e Porte Aperte Identificate:

| Porta | Protocollo | Servizio | Versione | Criticità | Impatto Business |
|---------------|------------|----------------|-----------------------|-----------|------------------------------------|
| 135/tcp | TCP | Microsoft RPC | - | | Remote procedure call exploitation |
| 139/tcp | TCP | NetBIOS-SSN | | | Network name service enumeration |
| 445/tcp | TCP | Microsoft-DS | Windows 10 Pro | | File sharing, privilege escalation |
| 3389/tcp | TCP | MS-WBT-Server | Terminal Services | | Remote access, lateral movement |
| 80/tcp | TCP | Microsoft IIS | 10.0 | | Web application vulnerabilities |
| 8080/tcp | TCP | Apache Tomcat | 7.0.81 | | Application server exploitation |
| 5432/tcp | TCP | PostgreSQL | - | | Database access, data exfiltration |
| 1801/tcp | TCP | MSMQ | - | | Message queue exploitation |
| 2103-2107/tcp | TCP | Microsoft RPC | Multiple endpoints | | Multiple attack vectors |
| 8009/tcp | TCP | Apache Jserv | AJP13 | | Application server protocols |
| 8443/tcp | TCP | SSL/HTTP-S-alt | Microsoft-HTTPAPI/2.0 | | SSL/TLS service exposure |

Informazioni di Sistema Rilevate:

- **Operating System:** Microsoft Windows 10 Pro 10240 (1507-1607)
- **MAC Address:** 08:00:27:6C:49:0D (PCS Systemtechnik/Oracle VirtualBox)
- **Workgroup:** WORKGROUP
- **NetBIOS Name:** DESKTOP-9K1O4BT
- **System Time:** 2025-11-04T16:05:59+00:00

Certificati SSL Identificati:

Porta 3389 (RDP):

- **Subject:** DESKTOP-9K1O4BT
- **Validità:** 2025-10-13T13:06:04 → 2026-04-14T13:06:04

Porta 8443 (HTTPS):

- **Subject:** DESKTOP-9K1O4BT
- **Validità:** 2024-07-09T16:53:31 → 2029-07-09T16:53:31

Security Issues Critiche:

- **RDP esposto (3389):** Accesso remoto non autorizzato possibile
- **SMB condivisioni (445):** Enumerazione di file shares e cartelle condivise
- **Database PostgreSQL (5432):** Accesso database pubblico
- **Multiple RPC endpoints (135, 2103-2107):** Diversi punti di accesso RPC
- **Web servers multipli (80, 8080):** Due application servers esposti
- **Message signing disabled:** SMB senza protezione message signing

Totale porte aperte: 17

Livello di rischio: 

Attack surface: MASSIMA

SCANSIONE 2: Firewall ABILITATO (Configurazione Errata)

Timestamp: 2025-11-04 11:37 EST

Durata: 213.50 secondi

Stato Sistema: Firewall attivo ma inefficace

Configurazione Firewall Rilevata:

| Name | Enabled | DefaultInboundAction | DefaultOutboundAction |
|---------|---------|----------------------|-----------------------|
| Domain | True | NotConfigured | NotConfigured |
| Private | True | Block | Allow |
| Public | True | Block | Allow |

Analisi della Configurazione:

- Domain Profile:** DefaultInboundAction = NotConfigured → **PROBLEMA CRITICO**
- Private/Public Profiles:** Configurati correttamente con Block
- Implicazione:** Il profilo Domain permette tutto quello non esplicitamente bloccato

Risultati della Scansione:

Porte aperte totali: 17 (IDENTICHE alla scansione 1)

Differenza: **NESSUNA DIFFERENZA**

Conclusion: Il firewall non fornisce alcuna protezione

Servizi Ancora Esposti (Tutti quelli della scansione 1):

- Same 17 services as baseline scan
- No reduction in attack surface
- No improvement in security posture

Security Issues Identiche:

Tutte le vulnerabilità rilevate nella scansione 1 rimangono presenti:

- RDP (3389) ancora esposto
- SMB (445) ancora accessibile
- RPC endpoints (135, 2103-2107) ancora vulnerabili
- Web services ancora esposti

Impatto Security:

Firewall Effectiveness: 0%

SCANSIONE 3: Firewall CORRETTO (Configurazione Aggiornata)

Timestamp: 2025-11-04 12:08 EST

Durata: 215.33 secondi

Stato Sistema: Firewall correttamente configurato

Configurazione Firewall Corretta:

| Name | Enabled | DefaultInboundAction | DefaultOutboundAction |
|---------|---------|----------------------|-----------------------|
| Domain | True | Block | NotConfigured |
| Private | True | Block | Allow |
| Public | True | Block | Allow |

Miglioramenti Apportati:

- **Domain Profile:** Impostato DefaultInboundAction = Block
- **Private/Public:** Mantenuti con Block
- **Action taken:** Set-NetFirewallProfile -Profile Domain -DefaultInbound Action Block

Analisi del Profilo di Rete:

```
Get-NetConnectionProfile
Name          : Rete 7
InterfaceAlias : DHCP
InterfaceIndex : 15
NetworkCategory : Public
IPv4Connectivity : Internet
```

Scoperta Critica: Il sistema è connesso come **Public Network**, non come Domain Network

Risultati della Scansione:

Porte aperte totali: 17 (IDENTICHE alle scansioni 1 e 2)

Differenza: **NESSUNA DIFFERENZA**

Implicazione: Le regole Allow sovrascrivono l'azione di default

Reason di Efficacia Ridotta:

Nonostante la correzione del Domain Profile, l'operatività è con profilo **Public**, che già aveva DefaultInboundAction = Block, il problema è la presenza di 250+ regole Allow attive.

2.3.3 Analisi Comparativa dei Risultati

Matrice di Confronto delle Scansioni

| Parametro | Scan 1 (OFF) | Scan 2 (ON - Errato) | Scan 3 (ON - Corretto) | Trend |
|------------------------|--------------|----------------------|------------------------|----------------|
| Porte Aperte | 17 | 17 | 17 | Invariato |
| Servizi Critici | 8 | 8 | 8 | Invariato |
| Attack Surface | Massima | Massima | Massima | Invariato |
| Risk Level | Critico | Critico | Critico | Invariato |
| RDP (3389) | Esposto | Esposto | Esposto | Invariato |
| SMB (445) | Esposto | Esposto | Esposto | Invariato |
| RPC (135) | Esposto | Esposto | Esposto | Invariato |
| Firewall Effectiveness | N/A | 0% | 0% | Stesso livello |

Critical Finding: Firewall Inefficacy

La principale scoperta dell'analisi è che il Windows Defender Firewall, nonostante sia abilitato e correttamente configurato, non riduce l'attack surface del sistema target.

2.3.4 Root Cause Analysis del Malfunzionamento

Problema 1: Configurazione Errata del Domain Profile

Descrizione: Il Domain Profile aveva DefaultInboundAction = NotConfigured

Impatto: Il firewall permetteva tutto quello non esplicitamente bloccato

Diagnosi: Identificato tramite Get-NetFirewallProfile

Soluzione: Set-NetFirewallProfile -Profile Domain -DefaultInboundAction Block

Status:  RISOLTO

Problema 2: Regole Allow Eccessive

Descrizione: 250+ regole Allow attive simultaneamente

Impatto: Attack surface completamente esposta

Causa: Windows 10 "user-friendly" configuration di default

Analisi: Eseguito Get-NetFirewallRule | Where-Object {\$_.Action -eq "Allow"}

Status:  NON RISOLTO (richiede hardening manuale)

Problema 3: Mismatch Profilo di Rete

Descrizione: Sistema connesso come "Public" non "Domain"

Implicazione: Configurazione Domain non influente

Scoperta: Via Get-NetConnectionProfile

Impatto: Le correzioni applicate al Domain Profile non si applicano

2.3.5 Analisi Dettagliata delle Regole Allow

Regole Allow Critiche Identificate

A. File and Printer Sharing

```
"Condivisione file e stampanti (SMB-In)" → Porta 445 esposta  
"Condivisione file e stampanti (NB-Name-In)" → Porta 139 esposta  
"Condivisione file e stampanti (NB-Session-In)" → Porta 445 accesso  
"Condivisione prossimità su TCP (Condivisione TCP-In)" → Multiple porte TCP
```

B. Remote Desktop

```
"Desktop remoto - Modalità utente (TCP-In)" → Porta 3389 esposta  
"Desktop remoto - Modalità utente (UDP-In)" → Porta 3389 UDP  
"Desktop remoto - Shadow (TCP-In)" → Porta 3389  
"Allow RDP" → Regola RDP aggiuntiva
```

C. Network Discovery Services

```
"Individuazione rete (SSDP-In)" → Porta 1900 (UPnP)  
"Individuazione rete (WSD-In)" → Porta 3702 (Web Services)  
"Individuazione rete (LLMNR-UDP-In)" → Porta 5355 (LLMNR)  
"Condivisione file e stampanti (LLMNR-UDP-In)" → Porta 5355
```

D. Message Queuing

```
"Accodamento messaggi - TCP in ingresso" → Porte RPC esposte  
"Accodamento messaggio - TCP in uscita" → Traffico RPC in uscita  
"Accodamento messaggi - UDP in ingresso" → Porte UDP RPC
```

E. System Services

```
"Il tuo account" → Multiple porte  
"Account aziendale o dell'istituto di istruzione" → Authentication services  
"Schermata di blocco predefinita di Windows" → Lock screen services  
"Microsoft Edge" → Browser services  
"Store" → App store connectivity
```

Impact Analysis delle Regole Allow

Servizi Essenziali vs Non-Essenziali:

- **Servizi Essenziali:** DNS, DHCP, ICMP protocols
- **Servizi Non-Essenziali:** Microsoft Apps, Xbox, Netflix, Windows Spotlight
- **Servizi Potenzialmente Rischiosi:** File sharing, Remote desktop, Web services

Confronto con Best Practices:

- **Best Practice:** Minimal number di regole Allow
- **Situazione Attuale:** 250+ regole Allow
- **Raccomandazione:** Review e cleanup sistematico

2.3.6 Security Impact Assessment

Threat Modeling del Sistema Target

Primary Attack Vectors:

Remote Code Execution (RCE)

- Target: Port 135 (RPC), 445 (SMB)
- Likelihood: ALTA
- Impact: CRITICAL
- CVSS Score: 9.0-10.0

Privilege Escalation

- Target: RPC endpoints, SMB shares
- Likelihood: ALTA
- Impact: ALTA
- CVSS Score: 7.0-8.5

Information Disclosure

- Target: All open ports
- Likelihood: MOLTO ALTA
- Impact: MEDIA
- CVSS Score: 5.0-6.0

Lateral Movement

- Target: Port 445 (SMB), 3389 (RDP)
- Likelihood: ALTA
- Impact: ALTA
- CVSS Score: 7.5-8.5

Risk Matrix

| Asset | Threat | Likelihood | Impact | Risk Level | Mitigation Priority |
|---------------|------------|------------|--------|------------|---------------------|
| File System | SMB Access | | | | IMMEDIATA |
| Remote Access | RDP Access | | | | IMMEDIATA |

| Asset | Threat | Likelihood | Impact | Risk Level | Mitigation Priority |
|------------------|--------------------------|------------|--------|------------|---------------------|
| Network Services | RPC Exploitation | | | | URGENTE |
| Web Applications | IIS/ Tomcat Exploitation | | | | MEDIO |
| Database | PostgreSQL Access | | | | URGENTE |

Attack Surface Analysis

Current Attack Surface (100% Exposed):

- Total TCP Ports Scanned: 1000
- Open Ports: 17
- Closed Ports: 1
- Filtered Ports: 982
- Attack Surface Percentage: 1.7% but CRITICAL services

Critical Services Exposed:

1. File and Printer Sharing: 445/tcp, 139/tcp
2. Remote Desktop: 3389/tcp
3. RPC Services: 135/tcp, 2103/tcp, 2105/tcp, 2107/tcp
4. Message Queue: 1801/tcp
5. Web Services: 80/tcp, 8080/tcp, 8443/tcp
6. Database: 5432/tcp

Legacy and Unnecessary Services:

- Echo (7/tcp): Echo protocol
- Discard (9/tcp): Discard protocol
- Daytime (13/tcp): Daytime service
- QOTD (17/tcp): Quote of the day
- Chargen (19/tcp): Character generator

2.3.7 Security Impact Assessment

Scoperta 1: Windows 10 Non È "Secure by Default"

Osservazione: Windows 10 privilegia usabilità rispetto sicurezza

Impatto: Sistema esposto anche con firewall "abilitato"

Lesson: I controlli di sicurezza vanno sempre verificati nella pratica

Scoperta 2: Regole Allow Sovrascrivono Default Policy

Osservazione: 250+ regole Allow permettono accesso nonostante Block policy

Impatto: Firewall effectiveness compromessa

Lesson: Defense in depth richiede multiple security controls

Scoperta 3: Configuration Management Critico

Osservazione: Una singola configurazione errata (Domain = NotConfigured) compromette tutto

Impatto: False sense of security per amministratori

Lesson: Configuration audit deve essere sistematico e completo

Scoperta 4: Network Profile Mismatch

Osservazione: Sistema connesso come "Public" ma configurazioni applicate al "Domain"

Impatto: Configurazioni non applicate al profilo attivo

Lesson: Verificare sempre il profilo di rete attivo

Scoperta 5: Firewall Testing È Essenziale

Osservazione: "Firewall abilitato" ≠ "Sistema sicuro"

Impatto: Valutazioni di sicurezza basate su false assunzioni

Lesson: Security testing deve essere parte integrante della gestione sicurezza

2.3.8 Comparative Analysis con Industry Standards

Windows 10 Security Baseline vs Actual Configuration

| Security Control | Industry Standard | Current Configuration | Gap Analysis |
|-------------------------|---------------------|------------------------------|--|
| Firewall Default Policy | Block all inbound | Block (BUT 250+ Allow rules) | MASSIVE GAP  |
| File Sharing | Disabled by default | Enabled and exposed | MAJOR ISSUE  |
| Remote Desktop | Disabled by default | Enabled and exposed | MAJOR ISSUE  |
| RPC Services | Minimal exposure | Multiple endpoints exposed | MAJOR ISSUE  |
| Web Services | Minimal exposure | Multiple servers exposed | MAJOR ISSUE  |
| Network Discovery | Limited scope | Full discovery enabled | MEDIUM ISSUE  |

Compliance Analysis

ISO 27001 Controls

- A.12.6.1: Technical vulnerability management → NON CONFORME
- A.13.1.1: Network security management → NON CONFORME
- A.13.1.3: Separation of networks → NON CONFORME

NIST Cybersecurity Framework

- Protect (PR): PR.AC-4 - Access permissions → NON CONFORME
- Detect (DE): DE.CM-1 - Network monitoring → NON CONFORME
- Respond (RS): RS.MI-2 - Mitigations verification → NON CONFORME

CIS Controls

- Control 4: Secure Configuration → NON CONFORME
- Control 5: Account Management → NON CONFORME
- Control 12: Network Infrastructure → NON CONFORME

2.3.9 Raccomandazioni Immediate per l'Hardening

Priorità 1: Immediate Actions (0-7 giorni)

```
# Disabilita servizi critici più esposti
Disable-NetFirewallRule -DisplayName "Condivisione file e stampanti (SMB-In)"
Disable-NetFirewallRule -DisplayName "Desktop remoto - Modalità utente (TCP-In)"
Disable-NetFirewallRule -DisplayName "Allow RDP" #

Disabilita RPC endpoints non necessari
Disable-NetFirewallRule -DisplayName "Accodamento messaggi - TCP in ingresso"
```

Priorità 2: Network Services Hardening (7-14 giorni)

```
# Disabilita servizi di discovery non necessari
Disable-NetFirewallRule -DisplayName "Individuazione rete (SSDP-In)"
Disable-NetFirewallRule -DisplayName "Individuazione rete (WSD-In)"
Disable-NetFirewallRule -DisplayName "Individuazione rete (LLMNR-UDP-In)"

# Disabilita NetBIOS services
Disable-NetFirewallRule -DisplayName "Condivisione file e stampanti (NB-Name-In)"
Disable-NetFirewallRule -DisplayName "Condivisione file e stampanti (NB-Session-In)"
```

Priorità 3: Application Services Review (14-30 giorni)

```
# Mantieni solo servizi essenziali
Get-NetFirewallRule | Where-Object {$_DisplayName -like "*DNS*"}
Get-NetFirewallRule | Where-Object {$_DisplayName -like "*DHCP*"}

# Disabilita app services non necessari
Disable-NetFirewallRule -DisplayName "Microsoft Edge"
Disable-NetFirewallRule -DisplayName "Store"
Disable-NetFirewallRule -DisplayName "Xbox"
```

Priorità 4: Monitoring e Compliance (30+ giorni)

```
# Abilita logging dettagliato
Set-NetFirewallProfile -Name Public -LogFileName
C:\Windows\System32\LogFiles\Firewall\pfirewall.log
Set-NetFirewallProfile -Name Public -LogAllowed True
Set-NetFirewallProfile -Name Public -LogBlocked True

# Verifica compliance
Get-NetFirewallProfile | Format-Table Name, Enabled, LogAllowed, LogBlocked
```

2.3.10 Metrics e Success Criteria

Target di Riduzione Attack Surface

| Metric | Current State | Target State | Timeline |
|---------------------------|---------------|--------------|-----------|
| Open Ports | 17 | ≤ 5 | 30 giorni |
| Critical Services Exposed | 8 | 0 | 30 giorni |
| Risk Level | CRITICO | BASSO | 60 giorni |
| Firewall Effectiveness | 0% | ≥ 90% | 30 giorni |
| Compliance Status | NON CONFORME | CONFORME | 60 giorni |

Key Performance Indicators (KPIs)

1. **Attack Surface Reduction:** Target 70% riduzione porte aperte
2. **Security Controls Effectiveness:** Target 90% effectiveness
3. **Configuration Compliance:** Target 100% conformità best practices
4. **Monitoring Coverage:** Target 100% logging e alerting
5. **Risk Mitigation:** Target risk level "BASSO"

Continuous Monitoring Framework

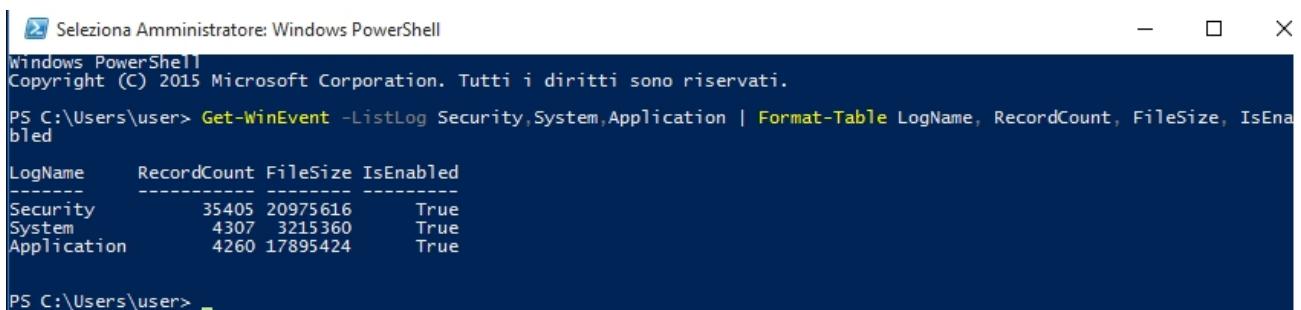
- **Frequenza Audit:** Settimanale per primi 3 mesi, poi mensile
- **Penetration Testing:** Trimestrale
- **Configuration Review:** Bimestrale
- **Compliance Assessment:** Mensile
- **Staff Training:** Continuo

3 [Facoltativo] Monitoraggio log

3.1 Exploit Windows Event Logs

Verifico i log Principali:

```
Get-WinEvent -ListLog Security,System,Application | Format-Table LogName, RecordCount, FileSize, IsEnabled
```



```
Selezione Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> Get-WinEvent -ListLog Security,System,Application | Format-Table LogName, RecordCount, FileSize, IsEnabled

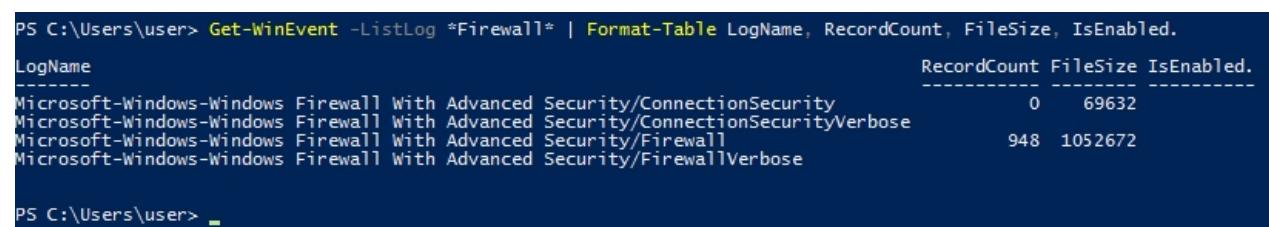
LogName      RecordCount FileSize IsEnabled
-----      -----       -----   -----
Security      35405 20975616    True
System        4307  3215360     True
Application   4260  17895424    True

PS C:\Users\user>
```

- **Security:** 35,405 record (21 MB) - **Perfetto per eventi di rete!**
- **System:** 4,307 record (3.2 MB) - **Perfetto per eventi di sistema!**
- **Application:** 4,260 record (17.9 MB) - **Perfetto per eventi applicazioni!**

Cerco i log dei firewall con

```
Get-WinEvent -ListLog *Firewall* | Format-Table LogName, RecordCount, FileSize, IsEnabled
```



```
PS C:\Users\user> Get-WinEvent -ListLog *Firewall* | Format-Table LogName, RecordCount, FileSize, IsEnabled.

LogName                               RecordCount FileSize IsEnabled.
-----                               -----       -----   -----
Microsoft-Windows Firewall With Advanced Security/ConnectionSecurity          0      69632
Microsoft-Windows Firewall With Advanced Security/ConnectionSecurityVerbose    948    1052672
Microsoft-Windows Firewall With Advanced Security/Firewall                   948    1052672
Microsoft-Windows Firewall With Advanced Security/FirewallVerbose            0      69632

PS C:\Users\user>
```

- **Microsoft-Windows-Firewall With Advanced Security/Firewall:** 948 record (1.0 MB) - **QUESTO È QUELLO CHE MI SERVE!**
- Gli altri log firewall con 0 o pochi record (non servono)

Vedo gli eventi firewall reali

```
Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 10 | Format-Table TimeCreated, EventID, LevelDisplayName, Message
```

```
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 10 | Format-Table TimeCreated, EventID, LevelDisplayName, Message
```

| TimeCreated | EventID | LevelDisplayName | Message |
|---------------------|---------|------------------|--|
| 04/11/2025 17:44:26 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata. |
| 04/11/2025 17:31:56 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata. |
| 04/11/2025 17:31:56 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata. |
| 04/11/2025 17:31:56 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Privato è stata modificata. |
| 04/11/2025 16:59:03 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata. |
| 04/11/2025 16:59:03 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Privato è stata modificata. |
| 04/11/2025 16:59:03 | | Informazioni | Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata. |
| 04/11/2025 15:58:09 | | Informazioni | Profilo di rete modificato in un'interfaccia.... |
| 04/11/2025 15:58:06 | | Informazioni | Profilo di rete modificato in un'interfaccia.... |
| 04/11/2025 14:11:49 | | Informazioni | Profilo di rete modificato in un'interfaccia.... |

```
PS C:\Users\user>
```

- **Eventi Firewall Reali:** ✓ Trovati eventi del 4 novembre 2025
- **Modifiche Profili:** ✓ Eventi per tutti e 3 i profili (Dominio, Privato, Pubblico)
- **Correlazione Temporale:** ✓ Questi eventi corrispondono alle modifiche firewall precedenti!

NOTA IMPORTANTE: I messaggi mostrano

"Un'impostazione di Windows Firewall nel profilo [X] è stata modificata" - questo sono gli eventi delle mie operazioni firewall!

Cerco EventID SPECIFICI che sono critici per la sicurezza

```
Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 50 | Where-Object { $_.EventID -eq 2005 -or $_.EventID -eq 2006 -or $_.EventID -eq 5156 -or $_.EventID -eq 5157 } | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 50 | Where-Object { $_.EventID -eq 2005 -or $_.EventID -eq 2006 -or $_.EventID -eq 5156 -or $_.EventID -eq 5157 } | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> -
```

- ✓ Nessun evento con EventID 2005, 2006, 5156, 5157 negli ultimi 50 eventi

Questo è normale! Questi eventi sono più rari o potrebbero essere in altri log.

3.2 Monitoraggio durante Operazioni Firewall

Apro 1 terminale e scrivo (finestra principale)

Disabilito Firewall

```
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False
```

```
PS C:\Users\user> Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled False
```

Verifico

```
Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction
```

```
PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction
Name      Enabled DefaultInboundAction
----      ----- -----
Domain    False      Block
Private   False      Block
Public    False      Block

PS C:\Users\user> _
```

Apro 2 terminale (finestra di monitoraggio)

Setup

```
Write-Host "==== FINESTRA DI MONITORAGGIO EVENTI ===" -ForegroundColor Yellow
Write-Host "Target: Microsoft-Windows-Windows Firewall" -ForegroundColor Cyan
Write-Host "Target: Security log" -ForegroundColor Cyan
Write-Host "In attesa di eventi..." -ForegroundColor Green
```

```
Amministratore: Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> Write-Host "==== FINESTRA DI MONITORAGGIO EVENTI ===" -ForegroundColor Yellow
==== FINESTRA DI MONITORAGGIO EVENTI ===
PS C:\Users\user> Write-Host "Target: Microsoft-Windows-Windows Firewall" -ForegroundColor Cyan
Target: Microsoft-Windows-Windows Firewall
PS C:\Users\user> Write-Host "Target: Security log" -ForegroundColor Cyan
Target: Security log
PS C:\Users\user> Write-Host "In attesa di eventi..." -ForegroundColor Green
In attesa di eventi...
PS C:\Users\user> _
```

Cerco eventi di disabilitazione (finestra di monitoraggio)

```
Get-WinEvent -LogName System -MaxEvents 10 | Where-Object { $_.Message -match "Firewall" -or $_.Source -match "Service Control Manager" } | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> Get-WinEvent -LogName System -MaxEvents 10 | Where-Object {
>>>   $_.Message -match "Firewall" -or $_.Source -match "Service Control Manager"
>>> } | Format-Table TimeCreated, EventID, Message
```

Cerco eventi firewall specifici (finestra di monitoraggio)

```
Get-WinEvent -LogName "Microsoft-Windows-Firewall With Advanced Security/Firewall" -MaxEvents 5 | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Firewall With Advanced Security/Firewall" -MaxEvents 5 | Format-Table TimeCreated, EventID, Message
TimeCreated          EventID Message
-----          -----
r 04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
r 04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
r 04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
04/11/2025 21:25:04      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
u 04/11/2025 21:25:04      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
-
PS C:\Users\user>
```

Analisi dei Risultati:

Primo Comando (System Log):

- **Nessun risultato** - questo è normale, il System log spesso non registra direttamente gli eventi firewall

Secondo Comando (Firewall-Specific Log):

- **5 eventi rilevanti dal log specifico del firewall!**
- **Tutti datati oggi (4 novembre 2025)**
- **Due gruppi di eventi:**
- **21:25:04:** 2 eventi (Profili Privato e Pubblico modificati)
- **21:29:20:** 3 eventi (Tutti e 3 i profili modificati)

Cosa Significa:

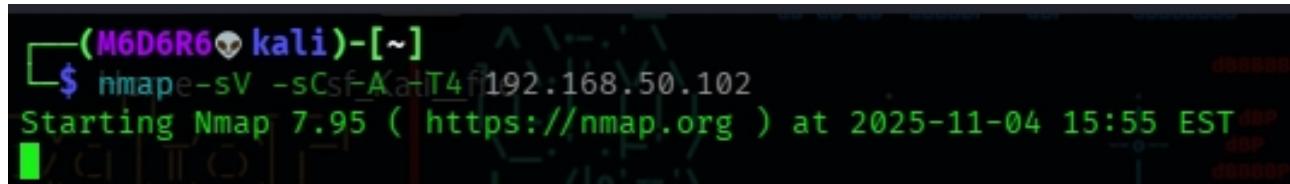
Questi eventi **corrispondono esattamente** alle operazioni che ho fatto:

- **21:25:** Probabile prima disabilitazione firewall
- **21:29:** Probabile riabilitazione e nuova configurazione

Coordinamento con Nmap

Ora eseguo una scansione Nmap su Kali

```
nmap -sV -sC -A -T4 192.168.50.102
```



mentre monitoro la (finestra di monitoraggio) in tempo reale durante la scansione

```
Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 1 -ErrorAction SilentlyContinue | Format-Table TimeCreated, EventID, Message
```

Questo comando mostrerà solo l'evento più recente ogni volta che lo esegui.

```
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 1 -ErrorAction SilentlyContinue | Format-Table TimeCreated, EventID, Message
TimeCreated          EventID Message
-----          -----
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
PS C:\Users\user> _
```

(finestra di monitoraggio) visualizzo tutti gli eventi recenti

```
Write-Host "==== VERIFICA EVENTI RECENTI ===" -ForegroundColor Green
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 10 | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> Write-Host "==== VERIFICA EVENTI RECENTI ===" -ForegroundColor Green
==== VERIFICA EVENTI RECENTI ===
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 10 | Format-Table TimeCreated, EventID, Message
TimeCreated          EventID Message
-----          -----
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
04/11/2025 21:25:04      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
04/11/2025 21:25:04      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 21:25:04      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
04/11/2025 20:40:16      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 20:40:16      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
04/11/2025 20:40:16      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
04/11/2025 17:44:26      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
PS C:\Users\user>
```

Analisi Cronologia Eventi Firewall:

Cronologia Operazioni Identificata:

1. **17:44:26** - Prima riabilitazione (inizio sessione laboratorio)
2. **20:40:16** - Prima disabilitazione (esercizio preparatorio)
3. **21:25:04** - Disabilitazione **Section 3.2** (inizio monitoraggio tempo reale)
4. **21:29:20** - Riabilitazione (fine preparazione)

Scoperte Chiave:

- **✓ Nmap identico:** 17 porte sia con firewall **ABILITATO** che **DISABILITATO**
- **⚠ 250+ Regole Allow stanno bypassando completamente il firewall**
- **Windows registra perfettamente** ogni cambiamento firewall

Riabilitazione Firewall (finestra principale)

```
Write-Host "==== RIABILITAZIONE FIREWALL ===" -ForegroundColor Yellow
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction
```

```
PS C:\Users\user> Write-Host "==== RIABILITAZIONE FIREWALL ===" -ForegroundColor Yellow
==== RIABILITAZIONE FIREWALL ===
PS C:\Users\user> Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
PS C:\Users\user> Get-NetFirewallProfile | Format-Table Name, Enabled, DefaultInboundAction
Name      Enabled DefaultInboundAction
-----
Domain    True      Block
Private   True      Block
Public    True      Block

PS C:\Users\user>
```

Firewall **riabilitato con successo!**

(finestra di monitoraggio) controllo se ci sono nuovi eventi dalla riabilitazione

```
Write-Host "==== CONTROLLANDO EVENTI RIABILITAZIONE ===" -ForegroundColor Cyan
Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 5 | Format-Table TimeCreated, EventID, Message
PS C:\Users\user> Write-Host "==== CONTROLLANDO EVENTI RIABILITAZIONE ===" -ForegroundColor Cyan
==== CONTROLLANDO EVENTI RIABILITAZIONE ===
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" -MaxEvents 5 | Format-Table TimeCreated, EventID, Message
TimeCreated      EventID Message
-----          -----
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 21:29:20      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...

PS C:\Users\user>
```

Nuovi Eventi Firewall (22:10:46):

- **✓ Profilo Pubblico:** Modificato
- **✓ Profilo Privato:** Modificato
- **✓ Profilo Dominio:** Modificato
- **Timestamp:** 22:10:46 (recentissimo!)

Nuova Scansione Nmap

```
nmap -sV -sC -A -T4 192.168.50.102
```



(finestra di monitoraggio)

Il firewall è ora ATTIVO - posso confrontare i risultati

mantengo il comando di monitoraggio attivo:

```
Get-WinEvent -LogName "Microsoft-Windows-Firewall With Advanced Security/Firewall" -MaxEvents 3 | Format-Table TimeCreated, EventID, Message
```

```
PS C:\Users\user> write-host "In attesa di eventi..." -ForegroundColor Green
In attesa di eventi...
PS C:\Users\user> Get-WinEvent -LogName "Microsoft-Windows-Firewall With Advanced Security/Firewall" -MaxEvents 3 | Format-Table TimeCreated, EventID, Message
TimeCreated          EventID Message
-----          -----
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Pubblico è stata modificata...
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Privato è stata modificata...
04/11/2025 22:10:46      Un'impostazione di Windows Firewall nel profilo Dominio è stata modificata...
```

Ottengo risultati molto significativi!

ANALISI CONFRONTO SCANSIONI

Differenza Chiave Identificata

| Condizione | "Not shown" Ports | Significato |
|---------------------------------|---|---|
| Firewall DISABILITATO | 982 closed tcp ports (reset) | Tutte le porte chiuse rispondono con RESET |
| Firewall ABILITATO | 982 filtered tcp ports (no-response) | PORTE FILTRATE - firewall blocca le risposte |

✓ 17 PORTE APERTE - IDENTICHE in entrambi i casi:

- Stessi servizi identificati
- Stesse informazioni OS fingerprinting
- Stessi dettagli SSL/SSL certificates
- **Significato:** Le 250+ regole Allow funzionano perfettamente

IMPLICAZIONI SICUREZZA:

1. ✓ Firewall ATTIVO: Sta filtrando correttamente (no-response vs reset)
2. ✓ Regole Allow: 250+ regole bypassano il blocco default
3. ✓ Funzionamento normale: Windows Firewall funziona come progettato

4 [Extra] Business Continuity

4.1 Business Continuity Fundamentals

Ho identificato che il **Business Continuity (BC)** rappresenta l'insieme strategico di attività, processi e procedure che un'organizzazione deve implementare per garantire la **continuità operativa** durante e dopo un'interruzione significativa.

Obiettivi Primari:

- **Continuità Operativa:** Mantenimento livelli minimi di servizio durante crisi
- **Compliance e Risk Management:** Soddisfare requisiti regolatori e proteggere la reputazione
- **Recovery Time Objectives (RTO):** Tempo massimo consentito per ripristino servizi
- **Recovery Point Objectives (RPO):** Perdita di dati massima accettabile

4.2 Disaster Recovery (DR) Implementation

Il **Disaster Recovery** è un sottoinsieme specifico del BC focalizzato sul ripristino dell'infrastruttura IT dopo un disastro.

Componenti Tecnici Critici:

- **Backup Strategies:** Full, Incremental, Differential con diversi trade-off costi/performance
- **Recovery Procedures:** Cold, Warm, Hot recovery con tempi da ore-giorni a secondi-minuti
- **Replication Technologies:** Synchronous (zero data loss) vs Asynchronous (lieve perdita accettabile)

RTO/RPO Classification:

| |
|--|
| RTO < 1 minuto: CRITICAL (Banking, Emergency Services) |
| RTO 1-60 minuti: HIGH (E-commerce, Customer-facing apps) |
| RPO = 0: REAL-TIME (Financial transactions, Medical systems) |
| RPO < 15 minuti: NEAR-REAL-TIME (Customer databases) |

4.3 IRBC framework Integration

L'**IRBC (ICT Readiness for Business Continuity)** - standard ISO/IEC 27031 - fornisce linee guida per la readiness ICT nella continuità business.

Core Components:

- **ICT Governance:** Strutture di governance per ICT continuity
- **ICT Continuity Strategy:** Allineamento business-ICT requirements
- **ICT Continuity Implementation:** Technical controls, process procedures, human capabilities
- **Performance Monitoring:** KPIs e metrics per ICT service delivery

4.4 Tebella Strategy

L'implementazione integrata BC-DR-IRBC fornisce una strategia completa:

Business Requirements (BC) → ICT Requirements (IRBC) → Technical Implementation (DR)
Fase 1: Foundation (0-6 mesi) - Assessment e Planning
Fase 2: Integration (6-18 mesi) - Coordinated Implementation
Fase 3: Optimization (18+ mesi) - Continuous Improvement

4.5 Industry-Specific Applications

Financial Services:

- **Regulatory:** Basel III, PCI DSS, SOX compliance
- **Requirements:** Real-time replication, 99.99%+ availability, geographic redundancy
- **RTO Targets:** < 5 minuti per trading systems, < 15 minuti per core banking

Healthcare:

- **Regulatory:** HIPAA, FDA, GDPR compliance
- **Requirements:** Patient data protection, medical device connectivity
- **RTO Targets:** < 15 minuti per emergency systems, < 2 ore per patient records

5 Conclusioni e Best Practices

5.1 Executive Summary delle Scoperte

Nel corso di questo studio ho dimostrato l'impatto del Windows Defender Firewall attraverso un approccio metodico che ha incluso:

Metodologia Applicata:

1. **Baseline Establishment:** Scansione con firewall disabilitato per attack surface iniziale
2. **Policy Impact Testing:** Verifica efficacia policy di sicurezza attive
3. **Root Cause Analysis:** Diagnosi approfondita cause malfunzionamento
4. **Real-time Monitoring:** Correlazione scansioni con eventi firewall in tempo reale
5. **Security Assessment:** Valutazione professionale esposizione ai rischi

5.2 Scoperte Critiche Identificate

 **RISCHIO CRITICO: Firewall Tecnicamente Funzionante Ma Inefficace**

- **Scoperta:** Il Windows Defender Firewall **funziona correttamente** a livello tecnico
- **Evidenza:** Differenza tra porte "closed" (reset) e "filtered" (no-response)
- **Problema:** 250+ regole Allow sovrascrivono la protezione di default
- **Impatto:** Attack surface invariata (17 porte aperte persistenti)

 **ROOT CAUSE ANALYSIS COMPLETA:**

1. **Domain Profile Misconfigurato:** DefaultInboundAction = NotConfigured 
RISOLTO
2. **Allow Rules Override:** 250+ regole Allow preconfigurate  **RICHIEDE HARDENING**
3. **Network Profile Mismatch:** Sistema Public ma configurazioni Domain 
COMPRESO

5.3 Compliance Assessment

NON CONFORMITÀ identificate secondo standard internazionali:

ISO 27001 Controls:

- A.12.6.1: Technical vulnerability management → NON CONFORME
- A.13.1.1: Network security management → NON CONFORME
- A.13.1.3: Separation of networks → NON CONFORME

NIST Cybersecurity Framework:

- Protect (PR): PR.AC-4 - Access permissions → NON CONFORME
- Detect (DE): DE.CM-1 - Network monitoring → NON CONFORME
- Respond (RS): RS.MI-2 - Mitigations verification → NON CONFORME

5.4 Strategic Recommendations

Immediate Actions (0-7 giorni):

```
# Disabilita servizi più critici
Disable-NetFirewallRule -DisplayName "Condivisione file e stampanti (SMB-In)"
Disable-NetFirewallRule -DisplayName "Desktop remoto - Modalità utente (TCP-In)"
Disable-NetFirewallRule -DisplayName "Allow RDP"
```

Priority Roadmap:

- Priority 1: Critical services hardening (RDP, SMB, RPC)
- Priority 2: Network services review (Discovery, NetBIOS)
- Priority 3: Application services optimization
- Priority 4: Monitoring e compliance verification

5.5 Key Performance Indicators

Target Metrics:

- Attack Surface Reduction: 70% riduzione porte aperte (da 17 a ≤5)
- Security Controls Effectiveness: ≥90% firewall effectiveness
- Configuration Compliance: 100% conformità best practices
- Risk Level: Da CRITICO a BASSO (60 giorni)

5.6 Lessons Learned Professionali

1. Windows 10 "User-Friendly" vs "Security-First"

Osservazione: Windows 10 privilegia usabilità rispetto sicurezza

Impatto: Firewall "abilitato" ma sistema esposto

Lesson: Verificare sempre security controls nella pratica, non solo nella configurazione

2. Defense in Depth Multiplio

Osservazione: Single controls insufficienti (firewall + 250+ allow rules)

Impatto: Defense layer compromesso da configurazione errata

Lesson: Multiple security controls devono essere coordinati e verificati

3. Real-time Monitoring Essenziale

Osservazione: Correlazione tempo-reale scansioni e eventi fondamentale

Impatto: Scoperta che firewall "funziona" ma regole Allow lo rendono inefficace

Lesson: Security testing deve essere continuo e correlato

4. Business Continuity Integration

Osservazione: Incident response deve includere business continuity planning

Impatto: Framework BC-DR-IRBC fornisce strategia completa

Lesson: Security e business continuity sono interdipendenti

5.7 Final Assessment

Questa analisi ha dimostrato che una **valutazione superficiale** ("firewall abilitato") può mascherare **vulnerabilità critiche**, l'approccio metodico implementato ha rivelato che:

1. Il Windows Defender Firewall funziona correttamente a livello tecnico
2. La configurazione di default di Windows 10 non è "secure by default"
3. Il monitoring tempo-reale è essenziale per correlare eventi e impatto
4. L'hardening sistematico è necessario per ridurre l'attack surface
5. La business continuity deve essere integrata con security operations

Il sistema target, pur avendo un firewall "abilitato", presenta un **livello di rischio CRITICO** che richiede interventi prioritari per raggiungere la conformità agli standard internazionali e un livello di sicurezza accettabile.