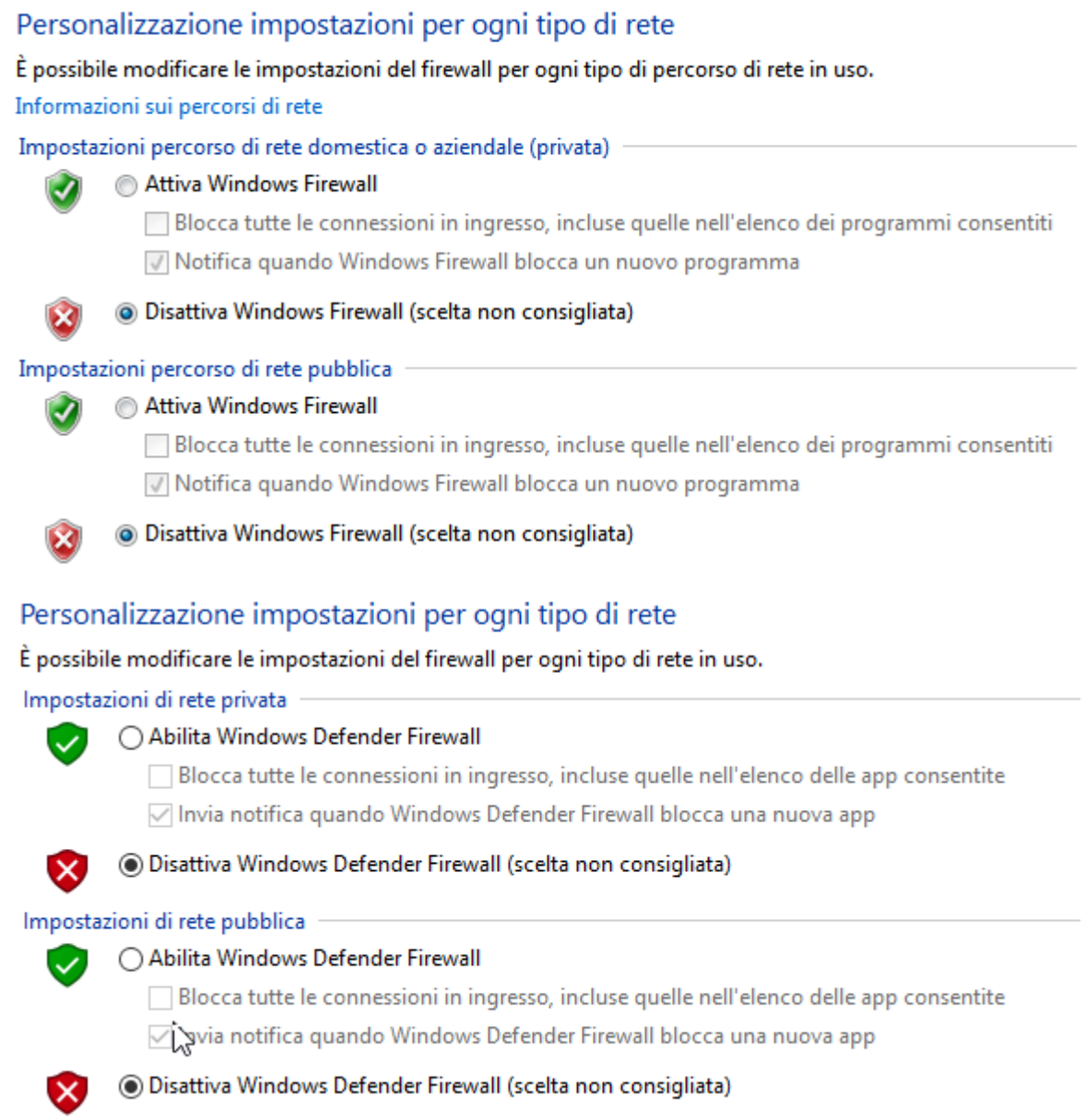
disabilitare i firewall in entrambe le macchine windows 7 e windows 10



usiamo kali e il comando nmap -sV su entrambe le macchine

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:14 EDT
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 13:16 (0:00:57 remaining)
Stats: 0:01:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 40.00% done; ETC: 13:17 (0:01:20 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.00016s latency).
Not shown: 990 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: STEFANO-PC; 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 77.50 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:16 EDT
Nmap scan report for 192.168.50.103
Host is up (0.00018s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:AA:96:6A (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 25.26 seconds
```

adesso abilitiamo il firewall e disabiltiamo l'allow ping, usiamo di nuovo il comando

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:19 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:19 EDT
Nmap scan report for 192.168.50.103
Host is up (0.00020s latency).
All 1000 scanned ports on 192.168.50.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AA:96:6A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.50 seconds
```

ci dice che è raggiungibile ma tutte le porte sono filtrate, proviamo usando -Pn

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.103 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:21 EDT
Nmap scan report for 192.168.50.103
Host is up (0.00023s latency).
All 1000 scanned ports on 192.168.50.103 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:AA:96:6A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.50.102 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 13:41 EDT
Nmap scan report for 192.168.50.102
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.50.102 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 08:00:27:E3:69:D0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.40 seconds
```

purtroppo non abbiamo avuto esito positivo ne su os7 ne su os10, dovuto probabilmente a delle regole firewall che scartano pacchetti di scansione

Conclusione

L’abilitazione del Firewall di Windows sta di fatto bloccando tutte le porte da scansioni provenienti dall’esterno. Possiamo dire che il Firewall sta preventivamente riducendo rischi di attacchi dall’esterno, rendendo inaccessibili dall’esterno i servizi sulle porte filtrate, riducendo la superficie d’attacco.

Business Continuity BC Esercizio Soluzione La Business Continuity, o Continuità Operativa, è un approccio olistico che mira a garantire che un'organizzazione possa continuare a operare a un livello predefinito in caso di interruzioni impreviste. Questo concetto va oltre la semplice gestione delle crisi IT e abbraccia tutti gli aspetti critici di un'azienda. Elementi chiave della BC a) Analisi d'impatto sul business BIA Identifica i processi critici e valuta l'impatto potenziale delle interruzioni. b) Valutazione dei rischi: Identifica le minacce potenziali e le vulnerabilità dell'organizzazione. c) Strategie di continuità: Sviluppa piani per mantenere le operazioni critiche durante le interruzioni. d) Piani di continuità operativa: Documenti dettagliati che delineano le procedure da seguire in caso di interruzione. e) Test e manutenzione: Assicura che i piani siano aggiornati e efficaci attraverso esercitazioni regolari. La BC si concentra sulla resilienza organizzativa, cercando di prevenire, rispondere e recuperarsi da potenziali minacce. Coinvolge vari dipartimenti e richiede il supporto del top management per essere efficace.
Disaster Recovery DR Esercizio Soluzione Il Disaster Recovery è un sottoinsieme della Business Continuity che si concentra specificamente sul ripristino dei sistemi IT e delle infrastrutture tecnologiche dopo un disastro o un'interruzione significativa. Componenti chiave del DR a) RPO Recovery Point Objective): Definisce la quantità massima di dati che l'organizzazione può permettersi di perdere in caso di disastro. b) RTO Recovery Time Objective): Indica il tempo massimo accettabile per ripristinare i sistemi dopo un'interruzione. c) Piano di DR Documento dettagliato che specifica le procedure per il ripristino dei sistemi IT. d) Infrastruttura di backup: Sistemi e dati replicati in luoghi sicuri per garantire il recupero. e) Test di DR Simulazioni regolari per verificare l'efficacia del piano. Il DR si concentra sulla continuità tecnologica, assicurando che i sistemi critici possano essere ripristinati rapidamente per minimizzare l'impatto sull'azienda.
ICT Readiness for Business Continuity Esercizio Soluzione L'IRBC, definito dallo standard ISO/IEC 27031, è un framework che si concentra sulla preparazione dei sistemi e servizi ICT Information and Communication Technology) per supportare la continuità operativa di un'organizzazione. Principi fondamentali dell'IRBC a) Allineamento strategico: L'IRBC deve essere allineato con gli obiettivi generali di business continuity dell'organizzazione e integrato nella strategia IT complessiva. b) Approccio proattivo: Enfatizza l'importanza di identificare e mitigare i rischi prima che si verifichino interruzioni, piuttosto che concentrarsi solo sulla risposta. c) Miglioramento continuo: Promuove un ciclo di pianificazione, implementazione, valutazione e miglioramento costante delle capacità di IRBC. d) Misurabilità: Fornisce metodi per misurare e valutare l'efficacia delle pratiche di IRBC in modo coerente e riconosciuto.