

Firewall

Nel compito di oggi viene richiesto di verificare la differenza di una scansione -sV sulla macchina windows con firewall attivo e con firewall non attivo.

Scansione con firewall disattivato:

```
(raul@192)-[~]
$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 13:41 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0057s latency).
Not shown: 996 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?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
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 24.93 seconds
```

Scansione con firewall attivo:

```
(raul@192)-[~]
$ nmap -sV 192.168.50.102
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 13:44 GMT
Nmap scan report for 192.168.50.102
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 4A:90:0C:A6:9B:76 (Unknown)
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 39.71 seconds
```

PARTE EXTRA:

1. Business Continuity (BC)

La Business Continuity è l'approccio proattivo e strategico che permette a un'organizzazione di continuare a erogare i propri servizi critici anche durante (o immediatamente dopo) un evento avverso.

Non riguarda solo l'informatica, ma l'intera azienda: persone, processi, sedi fisiche e comunicazioni. L'obiettivo è la sopravvivenza operativa riducendo al minimo l'impatto economico e reputazionale.

2. Disaster Recovery (DR)

Il Disaster Recovery è invece un sottoinsieme della Business Continuity, più focalizzato sull'aspetto tecnico e tecnologico. Rappresenta l'insieme delle misure logistiche e organizzative destinate a ripristinare sistemi, dati e infrastrutture a fronte di eventi gravi (attacchi ransomware, incendi, alluvioni).

Mentre la BC guarda al "come continuiamo a lavorare?", il DR risponde a "come recuperiamo i nostri server e i dati?".

Caratteristica	Business Continuity (BC)	Disaster Recovery (DR)
Obiettivo	Mantenere le operazioni aziendali attive durante una crisi.	Ripristinare l'infrastruttura IT e i dati dopo un evento.
Focus	Strategico e organizzativo (processi, persone, logistica).	Tecnico e operativo (server, backup, connettività).
Tempistica	Si attiva non appena si verifica l'evento (approccio continuo).	Si attiva dopo che il danno è avvenuto (approccio reattivo).
Esempio	Lavorare da casa se l'ufficio è inagibile.	Ripristinare un database da un backup dopo un attacco.
Indicatori Chiave	Analisi dell'impatto sul business (BIA).	RTO (Tempo di ripristino) e RPO (Punto di ripristino).