# Modulo 1 – Quiz finale: Introduzione alla sicurezza informatica

## 1 - Quale delle seguenti definizioni descrive meglio la sicurezza informatica?

A) La protezione dei beni fisici dai furti
B) Il processo di protezione dei sistemi digitali, delle reti e dei dati da accessi non autorizzati o attacchi
C) Installazione di software antivirus su un personal computer
D) Solo la protezione dei dati personali sui social media

## 2 - Chi ha bisogno della sicurezza informatica?

A) Solo i governi e le grandi aziende
B) Solo banche e istituzioni finanziarie
C) Tutti, dai singoli individui alle organizzazioni globali
D) Solo i professionisti IT

## 3 - Quale dei seguenti è un esempio comune di attacco informatico?

A) Formattazione di un disco rigido
B) Installazione di aggiornamenti software
C) E-mail di phishing che richiedono credenziali di accesso
D) Eliminazione dei file temporanei

## 4 - Che cos'è il ransomware?

A) Software che esegue la scansione alla ricerca di malware nel sistema
B) Malware che blocca i file e richiede un pagamento per ripristinarne l'accesso
C) Un attacco di phishing tramite e-mail
D) Un attacco brute-force contro una password

## 5 - Quale dei seguenti attacchi prende di mira il livello umano della sicurezza?

A) Denial-of-Service
B) Attacco di forza bruta
C) Phishing e ingegneria sociale
D) Exploit zero-day

## 6 - Cosa significa la "C" nella triade CIA?

A) Controllo
B) Crittografia
C) Riservatezza
D) Comunicazione

## 7 - Quale principio garantisce che gli utenti ottengano solo l'accesso strettamente necessario?

A) Difesa in profondità
B) Privilegio minimo
C) Zero Trust
D) Sicurezza fin dalla progettazione

## 8 - Un firewall protegge principalmente un sistema tramite:

A) Crittografando tutti i file presenti sul computer
B) Filtraggio del traffico di rete in entrata e in uscita in base a regole
C) Rilevando e rimuovendo i virus
D) Bloccando l'accesso ai siti web dei social media

## 6 - Quale di queste attività viene svolta dal software antivirus?

A) Crittografia del traffico Internet
B) Rilevamento e messa in quarantena dei file dannosi
C) Blocco degli indirizzi IP sospetti
D) Monitoraggio delle regole del firewall

## 10 - Perché spesso si consiglia di utilizzare sia un firewall che un software antivirus?

A) Svolgono esattamente la stessa funzione, quindi la ridondanza è utile
B) I firewall bloccano le intrusioni, gli antivirus rimuovono le infezioni
C) Il software antivirus rende obsoleti i firewall
D) I firewall funzionano solo su Linux, gli antivirus solo su Windows

## 11 - Quale comando Linux abilita il firewall utilizzando UFW?

A) sudo firewall on
B) ufw allow all
C) sudo ufw enable
D) abilita firewall ufw

## 12 - Negli strumenti antivirus, mettere in quarantena un file significa:

A) Eliminarlo automaticamente in modo permanente
B) Crittografarlo con una password complessa
C) Isolarlo in modo che non possa danneggiare il sistema
D) Inviarlo a un server di backup

## 13 - Ricevi un'e-mail dalla tua "banca" che ti chiede di confermare la tua password cliccando su un link. Quale concetto ti aiuta a identificare questa come una tentata frode?

A) Riservatezza
B) Difesa approfondita
C) Consapevolezza dell'ingegneria sociale
D) Zero Trust

### 14 - Quale delle seguenti opzioni illustra meglio l'architettura Zero Trust?

A) I dipendenti hanno accesso illimitato una volta entrati nella rete
B) I dispositivi e gli utenti devono essere continuamente verificati prima di accedere alle risorse
C) L'azienda utilizza un solo firewall potente
D) Tutta la sicurezza si basa esclusivamente sulle scansioni antivirus

### 15 - I log del firewall mostrano ripetuti tentativi da un IP sconosciuto sulla porta 22 (SSH). Qual è la migliore azione immediata da intraprendere?

A) Ignoralo, poiché si tratta solo di rumore di fondo
B) Bloccare l'IP e rivedere le regole del firewall SSH
C) Disinstallare il firewall e reinstallare l'antivirus
D) Consentire la connessione per vedere cosa succede

## Laboratorio 1.1 – Domande sul firewall

### 16 - Quale delle seguenti definizioni descrive meglio un firewall?

A) Uno strumento per crittografare i file
B) Una barriera che filtra il traffico di rete in base a regole
C) Uno scanner che rileva i virus
D) Un programma che monitora l'utilizzo della CPU

### 17 - Quale strumento di Windows viene utilizzato per configurare le regole avanzate del firewall?

A) Task Manager
B) Prompt dei comandi
C) Firewall di Windows Defender con sicurezza avanzata
D) Gestione dispositivi

### 18 - Qual è lo scopo del blocco della porta 22 (SSH) in una configurazione firewall?

A) Per prevenire lo spam via e-mail
B) Per impedire accessi remoti non autorizzati
C) Per disabilitare la navigazione web
D) Per migliorare le prestazioni del sistema

### 16 - Quale comando elenca le regole attive del firewall in Linux UFW?

A) ufw rules list
B) sudo ufw status
C) elenco firewall
D) netstat --ufw

### 20 - Nella sfida di laboratorio (consentire HTTP, bloccare tutto il resto), quale porta deve rimanere aperta?

A) 22
B) 25
C) 80
D) 443

## Laboratorio 1.2 – Domande sull'antivirus

### 21 - Qual è il primo passo da compiere prima di eseguire una scansione antivirus?

A) Disattivare il firewall
B) Aggiornare le definizioni dei virus
C) Reinstallare lo strumento antivirus
D) Eseguire un ripristino del sistema

## 22 - In Microsoft Defender, quale opzione esegue il controllo più approfondito?

A) Scansione rapida
B) Scansione personalizzata
C) Scansione completa
D) Scansione cronologica

## 23 - Quale comando Linux aggiorna il database dei virus ClamAV?

A) sudo freshclam
B) sudo update-av
C) clamav --update
D) av-refresh

## 24 - Se un file sospetto viene rilevato dall'antivirus, qual è la prima azione più sicura da intraprendere?

A) Eliminarlo immediatamente senza esaminarlo
B) Metterlo in quarantena per impedirne l'esecuzione
C) Ignorare l'avviso se il file sembra innocuo
D) Inviarlo a tutti i colleghi per un'ispezione

## 25 - Qual è la procedura migliore da seguire dopo aver esaminato i risultati della scansione antivirus?

A) Disattiva l'antivirus per risparmiare energia della CPU
B) Esamina i registri e conferma i falsi positivi prima di intraprendere qualsiasi azione
C) Esegui una sola scansione all'anno
D) Presumere che non siano necessarie ulteriori azioni

# Risposte

1. **B** – Cybersecurity = protezione dei sistemi digitali e dei dati.
2. **C** – Tutti hanno bisogno della sicurezza informatica.
3. **C** – Le e-mail di phishing sono classici attacchi informatici.
4. **B** – Il ransomware blocca i file e richiede un riscatto.
5. **C** – Il social engineering prende di mira le persone, non le macchine.
6. **C** – "C" = Riservatezza.
7. **B** – Privilegio minimo = accesso minimo necessario.
8. **B** – I firewall filtrano il traffico, non i file.
9. **B** – Gli antivirus rilevano/mettono in quarantena i file dannosi.
10. **B** – Si completano a vicenda: intrusione contro infezione.
11. **C** – Comando corretto: sudo ufw enable.
12. **C** – Quarantena = isolare i file sospetti.
13. **C** – La consapevolezza del social engineering previene il phishing.
14. **B** – Zero Trust = verifica continua.
15. **B** – Azione migliore: bloccare l'IP, controllare le regole del firewall.
16. **B** – Firewall = filtro del traffico.
17. **C** – Strumento Windows: Defender Firewall con sicurezza avanzata.
18. **B** – Il blocco di SSH impedisce gli accessi remoti.
19. **B** – sudo ufw status mostra le regole attive.
20. **C** – HTTP utilizza la porta 80.
21. **B** – Aggiornare sempre prima le definizioni dei virus.
22. **C** – La scansione completa è la più accurata.
23. **A** – sudo freshclam aggiorna il database ClamAV.
24. **B** – Metti prima in quarantena, poi controlla.
25. **B** – Controllare sempre i registri, confermare prima di eliminare.