Laboratorio 1.1 – Configurazione di un firewall

1. Panoramica del laboratorio

1.1 Descrizione del laboratorio

Benvenuto al tuo primo laboratorio pratico sulla sicurezza informatica!

In questo esercizio imparerai come abilitare e configurare un firewall di base per proteggere il tuo sistema da accessi non autorizzati. Che tu stia lavorando su Windows o Linux, questo laboratorio ti guiderà attraverso l'attivazione del firewall, l'aggiunta di regole per consentire o bloccare traffico specifico e il test dell'efficacia di tali regole.

Al termine del laboratorio, avrai compiuto il primo passo verso il controllo delle modalità di ingresso e uscita dei dati dal tuo sistema, una base essenziale nella difesa della sicurezza informatica.

1.2 Obiettivi di apprendimento

Dopo aver completato questo laboratorio, sarai in grado di:

- Comprendere lo scopo e la funzione di un firewall nella sicurezza informatica.
- Abilita e gestisci le impostazioni del firewall su sistemi Windows e Linux.
- Crea regole per consentire o bloccare il traffico di rete in base a porte, indirizzi IP o servizi.
- Verifica l'efficacia del firewall utilizzando tentativi SSH, ping e scansioni Nmap.
- Riconoscere l'importanza reale dei firewall negli ambienti personali e aziendali.

1.3 Prerequisiti

Per completare con successo questo laboratorio, è necessario disporre di:

- Conoscenza di base dei sistemi operativi per computer (Windows e/o Linux).
- Accesso a un PC Windows o a una macchina virtuale Linux (preferibilmente Ubuntu).
- Privilegi amministrativi sul sistema che stai utilizzando.
- Una connessione Internet per testare il traffico di rete (o un secondo dispositivo/VM per i test SSH).
- Opzionale: installazione di Nmap per i test di scansione delle porte.

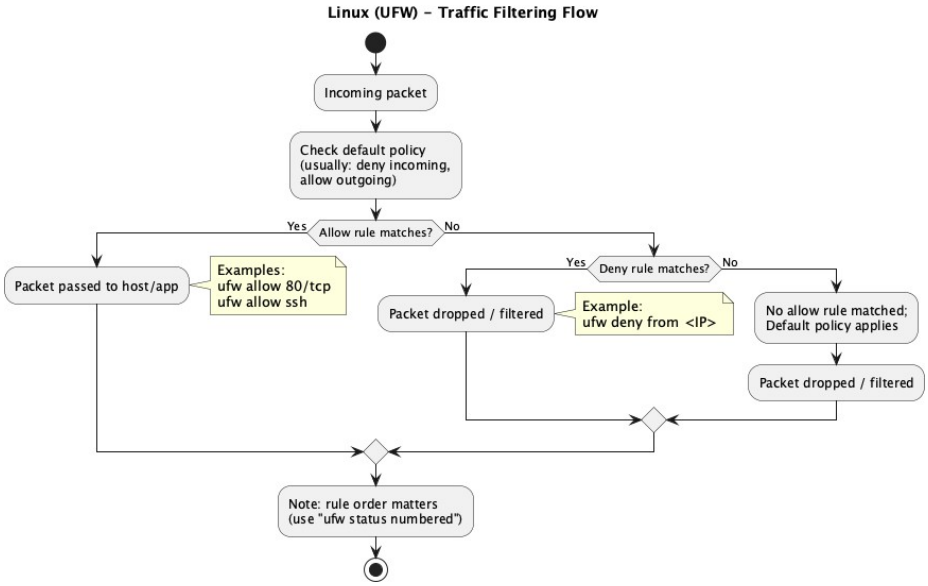
1.4 Tempo di completamento stimato

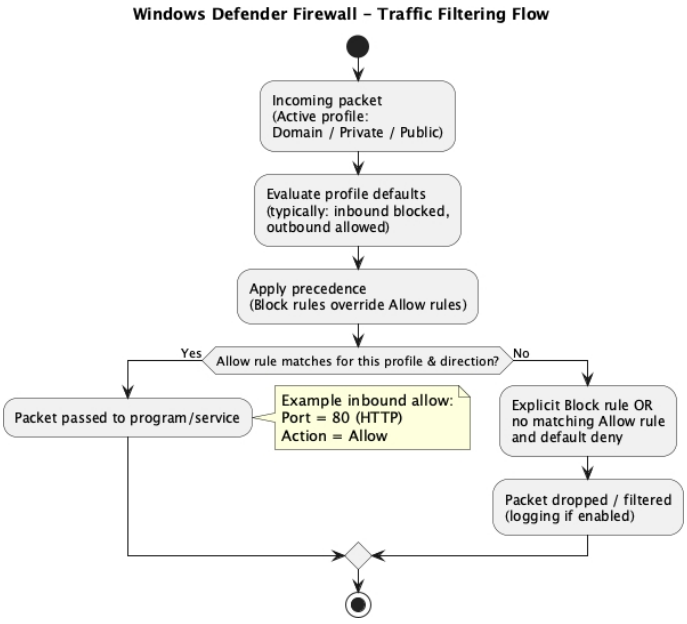
Attività	**Tempo stimato**
Lettura delle istruzioni Configurazione dell'ambiente C	10 minuti
Abilitazione del firewall (Windows e/o Linux)	15 minuti
Configurazione delle regole personalizzate (in entrata/in uscita, porte, IP)	30 minuti
Verifica della configurazione (SSH, Ping, Nmap, log)	35 minuti
Approfondimento: funzionalità avanzate del firewall di Windows (facoltativo)	25 minuti
Riflessione sul mondo reale: casi d'uso e scenari di minaccia	25 minuti
Sfida interattiva: consentire HTTP, bloccare tutto il resto	30 minuti
Documentazione C Scrivere il rapporto di configurazione del firewall	10 minuti
Tempo totale stimato	**3 ore**

2. Guida introduttiva

2.1 Che cos'è un firewall?

Un **firewall** è un sistema che monitora e controlla il traffico di rete in entrata e in uscita sulla base di regole predefinite. Funge da barriera tra la rete interna affidabile e il traffico esterno potenzialmente pericoloso (come Internet).





Esistono due tipi principali:

- **Firewall basati su host** (oggetto di questo laboratorio): installati su singoli computer (ad esempio, laptop o server).
- **Firewall di rete**: implementati a livello di rete per controllare il traffico su più dispositivi.

Perché è importante:
I firewall sono una delle prime linee di difesa in qualsiasi sistema sicuro e vengono utilizzati da aziende, governi e persino utenti domestici per proteggersi dagli attacchi.

Lo sapevate?
La maggior parte dei sistemi operativi include un firewall integrato che è disabilitato per impostazione predefinita o configurato in modo minimale. Questo laboratorio ti insegna a prenderne il controllo.

2.2 Elenco di controllo per la configurazione del laboratorio

Prima di iniziare, assicurati di avere a disposizione quanto

segue: Un computer funzionante con:

- **Windows 10/11** con accesso amministrativo
- **Ubuntu Linux (22.04 o versioni successive)** macchina fisica o virtuale

Accesso al terminale (Linux) o accesso GUI amministrativo (Windows)
Connessione Internet per testare la connettività e installare gli strumenti
Possibilità di installare software (se necessario: Nmap, OpenSSH)
(Facoltativo) Un secondo dispositivo o VM per simulare l'accesso SSH esterno

2.3 Note per gli utenti Windows e Linux

Questo laboratorio supporta **sia** gli utenti **Windows che Linux**. È possibile seguire entrambi i percorsi o scegliere quello adatto al proprio sistema.
Si consiglia di completare entrambi per una comprensione più

approfondita. Attività	**Windows**	**Linux (UFW)**
Abilita firewall	sudoufwabilita	Utilizza **Sicurezza di Windows → Firewall s Rete**
Crea regole	ufw allow / ufw deny comandi	Utilizza l'interfaccia grafica **delle impostazioni avanzate del firewall**
Prova il firewall bloccate	SSH, ping, Nmap	Ping, scansione delle porte, verifica delle app
Visibilità delle regole	Stato ufw verboso	Elenco delle regole GUI in Windows Defender Firewall

Suggerimento: se non sei sicuro di quale sistema operativo utilizzare, inizia con **Linux UFW**, quindi confrontalo con Windows per un'esperienza più ampia.

3. Passaggio 1: abilitazione del firewall

In questa sezione, abiliterai il firewall predefinito basato su host sul tuo sistema operativo.

Imparerai:

- Come attivare UFW (Uncomplicated Firewall) su Linux.
- Come controllare e abilitare il firewall utilizzando il Centro sicurezza di Windows.
- Come verificare che il firewall stia proteggendo il sistema.

3.1 Abilitazione del firewall su Windows

Passo dopo passo (Windows 10/11):

1. **Apri il Centro sicurezza Windows**
    - Fare clic sul **menu Start** o premere il **tasto Windows**
    - Digita: Sicurezza di Windows
    - Premi **Invio** o clicca sul primo risultato
2. **Passa alle impostazioni del firewall**
    - Nel menu a sinistra, clicca su **"Protezione rete firewall"**
3. **Controlla lo stato della rete attiva**
    - Sotto la **rete attiva** (di solito Privata o Dominio), cerca un segno di spunta verde e l'etichetta **"Firewall attivo"**
    - Se è **disattivato**, clicca e **attiva** il firewall
4. **Conferma l'operazione**
    - Quando il firewall è attivo, Windows mostra un segno di spunta verde
    - Ora sei protetto dal filtro di base basato sull'host

Suggerimento: alcuni strumenti antivirus di terze parti potrebbero disabilitare Windows Firewall. Se non vedi l'opzione, controlla le impostazioni del tuo antivirus.

3.2 Abilitazione del firewall su Linux (UFW)

Procedura dettagliata (sistemi basati su Ubuntu/Debian):

Queste istruzioni presuppongono che si stia utilizzando Ubuntu 22.04 LTS o simile.

1. **Apri il terminale**
    - Puoi usare **Ctrl + Alt + T** per aprire il terminale
2. **Verifica dello stato di UFW (facoltativo)**
3. sudo ufw status
    - Se UFW è **inattivo**, procedere per abilitarlo
    - Se UFW è **attivo**, passare alla sezione successiva
4. **Abilitare il firewall**
5. sudo ufw enable
    - Digita **la** tua **password utente** quando richiesto
    - UFW risponderà con:
      Il firewall è attivo e abilitato all'avvio del sistema
6. **Conferma stato**
7. sudo ufw status verbose
    - Questo comando mostra un riepilogo dettagliato delle regole e dello stato attuali

Suggerimento: UFW sta per "Uncomplicated Firewall" (firewall semplice) ed è progettato per essere intuitivo e facile da usare dalla riga di comando.

3.3 Breve riepilogo: configurazione Windows vs Linux

Sistema operativo	Passaggi per abilitare il firewall
Windows	Start → Cerca Sicurezza di Windows → Protezione rete firewall C → Attiva
Linux	Apri Terminale → sudo ufw enable → Controlla con sudo ufw status verbose

Punto di controllo

Prima di continuare:

- Il firewall è **abilitato**?
- **Vedi lo stato** che conferma che il firewall è in esecuzione?
- Sei pronto per iniziare a configurare le regole?

4. Passaggio 2 – Configurazione delle regole del firewall

Una volta abilitato, il firewall non svolge alcuna funzione fino a quando non si iniziano ad aggiungere regole per consentire o bloccare tipi specifici di traffico di rete.

In questa sezione:

- Consentire il traffico verso servizi essenziali (come SSH o HTTP).
- Blocca le connessioni indesiderate (ad esempio, da indirizzi IP specifici).
- Imparare a utilizzare sia gli strumenti a riga di comando (Linux) che quelli grafici (Windows).

4.1 Linux – Gestione delle regole con UFW

Esempio 1: consentire l'accesso SSH

Consenti le connessioni in entrata sulla porta 22 (impostazione predefinita per SSH):

```
sudo ufw allow ssh
```

Questo abilita il login remoto tramite SSH.

Esempio 2: consentire il traffico web (HTTP)

Consenti il traffico del server web sulla porta 80:

```
sudo ufw allow 80/tcp
```

Questo comando è comunemente usato per ospitare o accedere a siti web.

Esempio 3: Bloccare un indirizzo IP specifico

Bloccare le connessioni in entrata da un IP dannoso o sospetto:

```
sudo ufw deny from 192.168.1.100
```

Sostituire con qualsiasi indirizzo IP che si desidera bloccare.

Esempio 4: rivedere tutte le regole attuali

Visualizza le regole attive e la configurazione del firewall:

```
sudo ufw status numbered
```

oppure, per maggiori dettagli:

```
sudo ufw status verbose
```

Nota: le regole vengono applicate nell'ordine in cui sono elencate. È possibile eliminare o modificare regole specifiche in un secondo momento utilizzando i loro numeri.

4.2 Windows – Creazione di regole con il firewall avanzato

Passaggio 1: aprire le impostazioni avanzate del firewall

1. Apri **il menu Start**
2. Cerca: Windows Defender Firewall con sicurezza avanzata
3. Fare clic per avviare il pannello delle impostazioni avanzate

Passaggio 2: creare una nuova regola in entrata

1. Nel riquadro sinistro, clicca su **Regole in entrata**
2. A destra, seleziona **Nuova regola...**
3. Scegliere **Porta**, quindi fare clic su **Avanti**
4. Inserisci una porta (ad esempio 80), seleziona **Consenti** o **Blocca**
5. Applica ai profili corretti (Dominio, Privato, Pubblico)
6. Assegna un nome alla regola (ad esempio, "Consenti HTTP"), quindi termina

Passaggio 3: Altri tipi di regole

È inoltre possibile:

- Consentire o bloccare programmi specifici
- Filtrare in base agli indirizzi IP
- Scegliere tra TCP o UDP
- Impostare condizioni basate sull'autenticazione o sui servizi

Suggerimento: è possibile duplicare e modificare le regole esistenti per creare rapidamente varianti personalizzate.

4.3 Riepilogo rapido: Riepilogo delle regole del firewall

Piattaforma	Azione	Comando / Passaggi
Linux (UFW)	Consenti SSH	`sudo ufw allow ssh`
Linux (UFW)	Consenti HTTP	`sudo ufw allow 80/tcp`
Linux (UFW)	Blocca indirizzo IP	`sudo ufw deny from 192.168.1.100`
Linux (UFW)	Controlla le regole	`sudo ufw status verbose`
Windows avanzate	Apri Impostazioni avanzate	Start → Cerca Windows Defender Firewall con sicurezza avanzata
Windows es.	Consenti porta (ad es. HTTP)	Impostazioni → Regole in entrata → Nuova regola → Porta → 80 → Consenti
Windows specifica	Blocca app o IP	Nuova regola → Programma / Personalizzata → Blocca

Checkpoint

Prima di proseguire:

- Hai creato almeno due regole (una **di autorizzazione** e una **di blocco**)?
- Hai provato a creare regole su **entrambe le piattaforme**, se applicabile?
- Sai come **visualizzare e gestire** le regole esistenti?

5. Passaggio 3 – Testare il firewall

Creare regole firewall è solo metà del lavoro: è necessario anche **testarle** per assicurarsi che funzionino come previsto.

In questa sezione:

- Tenterai di connetterti utilizzando SSH e osserverai il comportamento del firewall.
- Utilizzerai il comando ping per testare l'accesso di base alla rete.
- Eseguire una scansione **Nmap** per visualizzare quali porte sono visibili dall'esterno.

Nota: potrebbe essere necessario un secondo dispositivo o una macchina virtuale per simulare l'accesso esterno. Il test funziona meglio quando un sistema è protetto dal firewall e un altro funge da "aggressore" o client esterno.

5.1 Test di blocco SSH

Obiettivo:

Verificare se l'accesso SSH è bloccato o consentito dalle regole del firewall.

Procedura:

1. Sul **secondo computer**, aprire un terminale o un client SSH.
2. Provare a connettersi utilizzando:

```
ssh tuo-nome-utente@tuo-server-ip
```

3. Se SSH è **bloccato**, dovresti vedere:
    - Connessione rifiutata
    - Timeout
    - Nessuna rotta verso l'host
4. Se SSH è **consentito**, ti verrà richiesta la password e potrai effettuare l'accesso.

Suggerimento: su Linux, blocca SSH utilizzando `sudo ufw deny ssh`, quindi riprova a stabilire la connessione.

5.2 Test Ping (raggiungibilità ICMP)

Obiettivo:

Verificare se il sistema risponde alle **richieste di eco ICMP** di base (ping).

Procedura:

1. Su un altro computer, apri un terminale.
2. Eseguire:

```
ping your-server-ip
```

3. Osserva il risultato:
    - Risposte = ICMP **consentito**
    - Richiesta scaduta = ICMP **bloccato**

Nota: alcuni sistemi bloccano ICMP per impostazione predefinita; ciò è configurabile utilizzando le impostazioni avanzate del firewall.

5.3 Scansione delle porte Nmap

Obiettivo:

Utilizzare **Nmap** per eseguire la scansione delle porte aperte e vedere quali servizi sono esposti.

Passaggi:

1. Sul secondo sistema (o da una macchina di scansione), installare Nmap se necessario:

```
sudo apt install nmap          # Su Debian/Ubuntu
brew install nmap              # Su macOS
```

2. Esegui la scansione del sistema protetto:

```
nmap your-server-ip
```

3. Esamina i risultati:
    - Le porte consentite (ad esempio 22, 80) appariranno come **aperte**
    - Le porte bloccate non verranno visualizzate o appariranno come **filtrate**
4. Per maggiori dettagli:

```
nmap -v il-tuo-server-ip
```

Suggerimento di sicurezza: anche gli hacker utilizzano strumenti come Nmap. Imparare a testare i propri sistemi aiuta a difendersi da scansioni e sondaggi.

5.4 Tabella riassuntiva – Metodi di test del firewall

Test funziona	Comando o azione	Risultato previsto se la regola
Test di blocco SSH	`ssh utente@ip`	Connessione rifiutata / timeout
Test ping	`ping your-server-ip`	Risposte (consentite) o timeout (bloccati)
Scansione delle porte con Nmap	`nmap il-tuo-server-ip`	Solo porte consentite (ad es. 22, 80) visibili
Scansione dettagliata Nmap	`nmap -v il-tuo-server-ip`	Elenco dettagliato dei servizi filtrati/bloccati

Punto di controllo

Conferma prima di procedere:

- Hai testato **almeno una porta bloccata e una consentita**?
- Sei riuscito a confermare il comportamento del firewall con **ping o SSH**?
- Hai provato a eseguire una **scansione delle porte** utilizzando Nmap?

6. Rilevanza nel mondo reale

Configurare un firewall può sembrare semplice, ma è uno dei **passaggi** più **critici nella difesa dei sistemi reali**, dai laptop ai data center aziendali.

In questa sezione imparerai:

- Perché i firewall sono importanti nel mondo reale.
- Come gli aggressori vengono bloccati da regole ben configurate.
- Dove si inseriscono i firewall a casa e al lavoro.

6.1 Perché i firewall sono importanti nella sicurezza informatica

I firewall non sono opzionali. Sono **strumenti di difesa essenziali** utilizzati oggi in quasi tutti i sistemi sicuri.

I firewall proteggono i sistemi:

- Bloccando scansioni e tentativi di connessione non autorizzati.
- Prevenire l'accesso a servizi vulnerabili.
- Filtraggio del traffico dannoso **prima** che raggiunga il sistema.

6.2 Firewall in uso – Casi d'uso

Utente domestico:

- **Il router di casa** tua ha un firewall integrato che blocca silenziosamente la maggior parte del traffico Internet in entrata.
- Questo protegge i tuoi dispositivi (laptop, TV, telefono) da attacchi diretti.

Sistemi aziendali:

- Le grandi organizzazioni implementano **firewall multistrato** per segmentare le reti interne e controllare l'accesso a database, applicazioni e dispositivi dei dipendenti.
- Questi firewall sono monitorati attentamente e aggiornati costantemente.

Dispositivi personali:

- I firewall su laptop o workstation bloccano le app pericolose, prevengono le backdoor e isolano il malware.

6.3 Riepilogo visivo – Il firewall come barriera

Funzione firewall in 3 passaggi:

1. **Controlla** tutto il traffico in entrata e in uscita.
2. **Confronta** il traffico con le regole configurate.
3. **Consenti o blocca** in base alla politica.

Punto di controllo

Rifletti sul tuo sistema:

- Quali servizi desideri **rendere accessibili** a Internet?
- Quali servizi devono essere sempre **bloccati**?
- In che modo un firewall configurato in modo errato potrebbe esporre il tuo sistema?

7. Sfida di laboratorio

7.1 Scenario: consentire HTTP, bloccare tutto il resto

Il tuo compito:
Configurare il sistema in modo che sia consentito **solo** il traffico **HTTP (porta 80)**; tutto il resto del traffico in entrata deve essere bloccato.

Questo simula uno scenario di server web di base in cui si desidera che gli utenti possano accedere al proprio sito web, ma si desidera bloccare tutti gli altri accessi (SSH, ping, ecc.).

Istruzioni per Linux (UFW)

1. **Impostare la politica predefinita per bloccare tutto il traffico in entrata:**

```
sudo ufw default deny incoming
```

2. **Consenti solo HTTP (porta 80):**

```
sudo ufw allow 80/tcp
```

3. **(Facoltativo) Negare esplicitamente tutti gli altri servizi:**

```
sudo ufw deny ssh
```

4. **Controlla le tue regole:**

```
sudo ufw status verbose
```

Istruzioni per Windows

1. **Aprire le impostazioni avanzate del firewall**
2. **Crea una nuova regola in entrata:**
    - Tipo: **Porta**
    - Porta: 80
    - Azione: **Consenti**
    - Nome: Consenti HTTP
3. **Blocca tutto il resto del traffico in entrata (facoltativo):**

- Vai a **Regole in entrata** → Fai clic su **Nuova regola**
- Tipo: **Tutti i programmi**
- Azione: **Blocca**
- Ambito: Applica a tutte le porte o a quelle specifiche come la 22 per SSH

4. **Riorganizza o modifica le regole in conflitto, se necessario**

7.2 Lista di controllo: hai completato con successo l'operazione?

Attività	**Completata?**
Impostare il rifiuto predefinito per il traffico in entrata	[ ]
Consentito solo HTTP (porta 80)	[ ]
Stato/output della regola verificata	[ ]
Confermato che SSH o ping sono bloccati	[ ]
Confermato che la porta 80 è aperta (tramite Nmap)	[ ]

7.3 Test facoltativi

Prova ad accedere al tuo sistema da un altro dispositivo o da una macchina virtuale:

- Visita http://your-server-ip → Dovrebbe caricarsi un servizio web (se ne è in esecuzione uno)
- Prova SSH o Nmap → Dovrebbe essere

bloccato Non hai un server web in esecuzione?

Prova:

sudo apt install apache2

sudo systemctl start apache2

7.4 Domande di riflessione

Rispondi a queste domande nel tuo quaderno di laboratorio o inviale come parte della tua relazione:

1. Quali comandi o passaggi hai utilizzato per configurare il tuo firewall?

2. Come hai verificato che il traffico non HTTP fosse bloccato?
3. C'erano ancora servizi accessibili che non intendevi consentire?
4. Cosa potrebbe accadere se consentissi accidentalmente una porta vulnerabile?

Sfida completata!

Hai simulato il profilo firewall di un **server web pubblico**, uno dei casi d'uso più comuni nelle operazioni di sicurezza informatica.

8. Conclusioni e prossimi passi

8.1 Punti chiave

Congratulazioni, hai completato il tuo primo laboratorio sulla sicurezza

informatica! Ecco cosa hai realizzato in questa sessione:

Abilitato un firewall basato su host sia su Linux (UFW) che su Windows.
Creazione di regole in entrata e in uscita per consentire o bloccare il traffico.
Testate le regole utilizzando strumenti come SSH, ping e Nmap.
Esplorazione di **casi d'uso reali** dei firewall nelle reti domestiche e aziendali.
Configurato un profilo firewall limitato per simulare un server web nella sfida.

Perché è importante:
Ogni sistema sicuro, dal tuo laptop personale a un'infrastruttura cloud globale, dipende da firewall ben configurati. Hai compiuto un passo professionale verso la comprensione e il controllo delle difese digitali.

8.2 Competenze acquisite

Completando questo laboratorio, ora hai acquisito esperienza pratica con:

- Configurazione della sicurezza a livello di sistema operativo.
- Strumenti di rete da riga di comando (ufw, ping, ssh, nmap).
- Pensiero difensivo: ridurre al minimo la superficie di attacco limitando l'accesso.
- Gestione della GUI del firewall e logica delle regole (Windows Advanced Firewall).

Queste sono competenze che utilizzerai durante il tuo percorso nella sicurezza informatica, nei laboratori, nelle competizioni o sul posto di lavoro.

8.3 Prossimamente: Laboratorio di scansione del malware

Successivamente, cambieremo marcia e vedremo **come rilevare e rimuovere il software dannoso** da un sistema utilizzando strumenti antivirus.

Nel **laboratorio 1.2 - Scansione malware**, imparerai a:

- Eseguire una scansione utilizzando strumenti integrati o open source.
- Esamina come si comporta e si nasconde il malware.
- Scopri come funzionano il rilevamento e la riparazione nel mondo reale.

Suggerimento per la preparazione: preparati a installare uno scanner antimalware (Windows Defender, ClamAV, ecc.) ed esegui scansioni rapide e complete sui file di prova.

Passaggi successivi

- Completa **le domande di riflessione** della sfida.
- Invia il **log/rapporto di configurazione del firewall,** se richiesto.
- Rivedi i **comandi utilizzati** e riprova a eseguirli a memoria.
- Inizia a preparare il tuo sistema per **la scansione antimalware**. **Hai creato uno scudo: ora imparerai a rilevare gli intrusi.**

6. Appendice

6.1 Riferimento ai comandi Linux (UFW)

Comando	Descrizione
`sudo ufw status`	Visualizza lo stato di base
del firewall `sudo ufw status verbose`	Visualizza il set di regole
dettagliato `sudo ufw enable`	Attiva il firewall
`sudo ufw disable`	Disattiva il firewall
`sudo ufw default deny incoming`	Blocca tutto il traffico in entrata per impostazione predefinita
`sudo ufw default allow outgoing`	Consenti tutto il traffico in uscita
`sudo ufw allow ssh`	Consenti SSH (porta 22)
`sudo ufw allow 80/tcp`	Consenti HTTP (porta 80)
`sudo ufw deny from [IP]`	Blocca tutto il traffico proveniente da un IP specifico
`sudo ufw delete [numero-regola]`	Rimuovi una regola specifica in base al numero

6.2 Suggerimenti per Windows Firewall

- Utilizza il pannello **Impostazioni avanzate** per avere il controllo completo sulle regole.
- **Prova** sempre **le nuove regole** prima di implementarle in ambienti critici.
- **Utilizza le regole "Personalizzate"** per individuare con precisione porte, app o protocolli.
- **I profili predefiniti** (Dominio, Privato, Pubblico) possono comportarsi in modo diverso: verifica sempre quale è attivo.
- Utilizza **Visualizzatore eventi > Registri di sicurezza** per tenere traccia delle connessioni bloccate/consentite (utenti esperti).

6.3 Risoluzione dei problemi comuni

Problema	Possibile causa	Soluzione
Impossibile connettersi tramite SSH	La regola blocca la porta 22	sudo ufw allow ssh o verificare
Il ping restituisce "Richiesta scaduta"	ICMP bloccato	Regola di Windows Consenti ICMP (avanzato) o conferma la raggiungibilità della rete
Nmap mostra tutte le porte chiuse/filtrate	Tutte le porte bloccate o firewall abilitato	Consentire porte specifiche secondo necessità
La regola di Windows non è applicabile	Profilo selezionato errato (Privato/Pubblico)	Controllare il profilo di rete attivo e applicare quello corretto
Il firewall non funziona su Linux	UFW non abilitato o mancante	Eseguire sudo ufw enable e assicurarsi che sia installato

6.4 Strumenti opzionali e risorse

🛠 **Strumenti consigliati**

- **Nmap** – https://nmap.org
- **Wireshark** – https://www.wireshark.org
- **ClamAV (antivirus Linux)** – https://www.clamav.net

Ulteriori letture

- Manuale UFW: man ufw o https://help.ubuntu.com/community/UFW
- Microsoft Defender Firewall: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall
- Guida ai firewall OWASP: https://owasp.org/www-community/Firewalls