Laboratorio 2.1 – Configurazione delle politiche di sicurezza su una macchina virtuale

1. Panoramica del laboratorio

1.1 Descrizione del laboratorio

In questo laboratorio, ti eserciterai nel **rafforzamento del sistema** configurando criteri di sicurezza all'interno di una macchina virtuale (VM). Le VM forniscono un ambiente sandbox sicuro in cui è possibile applicare criteri reali senza mettere a rischio il sistema host.

Imparerai come:

- Creare e gestire account utente con privilegi adeguati.
- Applicare politiche di password complesse.
- Limitare i diritti amministrativi.
- Abilitare la registrazione di sistema per il monitoraggio e il controllo.

Al termine di questo laboratorio, avrai uno **snapshot della VM rafforzato**, una base di riferimento sicura a cui potrai ricorrere ogni volta che sarà necessario.

1.2 Obiettivi di apprendimento

Al termine di questo laboratorio, sarai in grado di:

- Spiegare l'importanza del rafforzamento del sistema nella sicurezza informatica.
- Configurare un ambiente di macchina virtuale per testare le politiche di sicurezza.
- Configurare le politiche relative alle password su Windows e Linux.
- Limitare i privilegi amministrativi e applicare il principio del privilegio minimo.
- Abilitare e verificare i sistemi di registrazione e controllo.
- Documentare e salvare un'istantanea sicura della VM per poterla riutilizzare.

1.3 Prerequisiti

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

- Un computer funzionante con **almeno 8 GB di RAM** e **20 GB di spazio libero su disco**.

- Uno strumento di virtualizzazione installato (VirtualBox, VMware Workstation o Hyper-V).
- Un'immagine ISO di installazione di Windows (10/11) o Linux (consigliato Ubuntu Server).
- Conoscenza di base dell'uso della riga di comando (Linux) e dell'amministrazione di sistema.
- Diritti amministrativi sul sistema host (per installare/configurare le VM).

1.4 Tempo di completamento stimato

Attività	**Tempo stimato**
Configurazione della VM (installazione + account utente)	90 minuti
Configurazione delle politiche relative alle password	60 minuti
Limitazione dei privilegi amministrativi	45 minuti
Abilitazione e verifica della registrazione	45 minuti
Sfida di laboratorio: snapshot VM rinforzato + riflessione	60 minuti
Tempo totale stimato	**~5 ore**

Punto di controllo
Prima di proseguire, assicurati di:

- Comprendi che questo laboratorio richiede circa 5 ore.
- Hai installato una piattaforma VM.
- Hai scelto un sistema operativo (Windows o Linux) con cui esercitarti.

2. Per iniziare

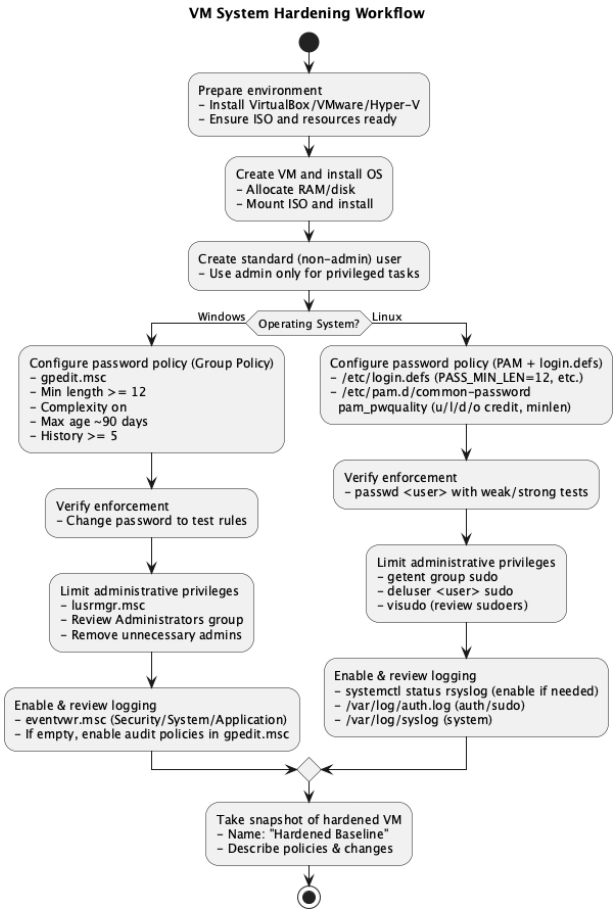
2.1 Che cos'è il rafforzamento del sistema?

Il rafforzamento del sistema è il processo di protezione di un sistema informatico attraverso la riduzione della sua superficie di attacco. Ciò significa eliminare account non necessari, applicare politiche rigorose e abilitare funzioni di monitoraggio per individuare tempestivamente comportamenti sospetti.

Esempi di azioni di rafforzamento:

- Applicazione **di password complesse**
- Limitazione **dei privilegi di amministratore**
- Abilitazione **della registrazione e del controllo**
- Rimozione o disabilitazione dei servizi inutilizzati

Idea chiave: meno "punti deboli" ha un sistema, più difficile sarà per un aggressore avere successo.



2.2 Perché utilizzare macchine virtuali per i laboratori di sicurezza?

Le macchine virtuali (VM) forniscono un **ambiente protetto** per esercitarsi nella sicurezza informatica:

- **Isolamento**: le modifiche apportate non influiscono sulla macchina host.
- **Capacità di ripristino**: è possibile ripristinare uno snapshot se qualcosa non funziona correttamente.
- **Supporto di più sistemi operativi**: esercitati a rafforzare la sicurezza sia su Windows che su Linux.
- **Realismo**: le VM si comportano come sistemi reali, quindi le competenze acquisite sono direttamente trasferibili agli ambienti di produzione.

2.3 Lista di controllo per la configurazione del laboratorio

Prima di iniziare, assicurati di avere:

Software di virtualizzazione installato

- VirtualBox (gratuito, multipiattaforma)
- VMware Workstation Player (gratuito per uso personale)
- Hyper-V (incluso con Windows Pro/Enterprise)

ISO del sistema operativo

- Windows 10/11 (è sufficiente la versione di valutazione)
- Ubuntu Server (opzione Linux leggera)

Requisiti del sistema host

- Minimo: 8 GB di RAM e 20 GB di spazio libero su disco
- Connessione Internet (per aggiornamenti e download)

Configurazione di base della VM completata

- Creazione di una nuova macchina virtuale
- Installazione del sistema operativo scelto
- Creazione di almeno **un account utente standard (non amministratore)**

Punto di controllo
Prima di proseguire:

- Hai già un ambiente VM funzionante?
- Hai installato Windows o Linux all'interno della VM?
- Hai creato un **account utente standard** (non solo admin/root)?

3. Configurazione della macchina virtuale

3.1 Scelta di una piattaforma di virtualizzazione

Per eseguire la VM è necessario un software di virtualizzazione. Scelte popolari:

- **VirtualBox** (gratuito, multipiattaforma)
- **VMware Workstation Player** (gratuito per uso personale)
- **Hyper-V** (integrato nelle edizioni Windows Pro/Enterprise)

Suggerimento: se non sei sicuro, scegli **VirtualBox**: è ampiamente supportato e facile da usare.

3.2 Creazione di una nuova macchina virtuale

Segui la procedura guidata "Nuova VM" della tua piattaforma. I passaggi tipici includono:

1. **Selezione del nome e del sistema operativo**
    - Esempio: "Ubuntu Hardened VM" o "Windows Security Lab"
    - Seleziona il tipo e la versione del sistema operativo
2. **Allocazione delle risorse**
    - Memoria: almeno **2 GB per Linux**, **4 GB per Windows**
    - Disco: minimo 20 GB
3. **Collegare il supporto di installazione**
    - Montare il file ISO per l'installazione di Windows o Linux
4. **Installare il sistema operativo**
    - Avvia la VM e segui la normale procedura di installazione del sistema operativo

3.3 Creazione di account utente standard

Una volta installato il sistema operativo della VM:

- **Su Windows**
    - Aprire **Impostazioni → Account → Altri utenti della famiglia**
    - Aggiungere un nuovo account **utente standard** (non amministratore)
    - Utilizza l'account amministratore solo per attività privilegiate
- **Su Linux**
    - Aggiungi un nuovo utente con:
    - sudo adduser studentuser
    - Assegna una password quando richiesto
    - Verifica che l'account funzioni effettuando l'accesso

Principio del privilegio minimo: utilizzare sempre account standard per le attività quotidiane. L'accesso come amministratore/root deve essere utilizzato solo quando necessario.

3.4 Riepilogo: Elementi essenziali per la configurazione delle VM

Passaggio	**Windows**	**Linux**
Creare una VM	VirtualBox/VMware/Hyper-V procedura guidata	Procedura guidata VirtualBox/VMware/Hyper-V
Installa sistema operativo		Windows 10/11 Ubuntu Server/Desktop
Crea standard Utente `studentuser`	Impostazioni → Account → Aggiungi utente	`sudo adduser`
Verifica privilegio minimo	Accedi come utente standard, non come amministratore	Confermare che l'accesso sudo sia limitato

Punto di controllo

Prima di continuare:

- La tua VM è installata e in esecuzione?
- Hai almeno un **account utente standard**?
- È possibile effettuare l'accesso senza utilizzare l'account amministratore/root?

4. Applicazione delle politiche relative alle password

Le password sono spesso la prima linea di difesa contro gli intrusi. Password deboli rendono vulnerabile anche un sistema rinforzato. In questa sezione, applicherai regole che richiedono password più forti e sicure.

4.1 Windows: utilizzo dell'Editor criteri di gruppo

1. **Apri l'Editor criteri di gruppo**
    - Premere **il tasto Windows + R**
    - Digita:
    - gpedit.msc
    - Premere **Invio**
2. **Passa a Criteri password**
    - Configurazione computer → Impostazioni di Windows → Impostazioni di sicurezza → Criteri account → Criteri password
3. **Imposta regole rigorose**
    - Lunghezza minima della password: **12 caratteri**
    - La password deve soddisfare i requisiti di complessità (maiuscole, minuscole, numeri, simboli)
    - Durata massima della password: **G0 giorni**
    - Durata minima della password: **1 giorno**
    - Applica cronologia password: **ricorda le ultime 5 password**

Suggerimento: dopo aver applicato le modifiche, disconnettiti e prova a creare una nuova password per verificare l'applicazione.

4.2 Linux: configurazione di PAM e login.defs

Linux utilizza **PAM (Pluggable Authentication Modules)** per le regole di autenticazione.

A. Modifica /etc/login.defs

1. Aprire il file in un editor di testo:
2. sudo nano /etc/login.defs
3. Modificare questi valori:
4. PASS_MAX_DAYS 90
5. PASS_MIN_DAYS 1
6. PASS_MIN_LEN 12
7. PASS_WARN_AGE 7
    - **PASS_MAX_DAYS** = forza la modifica della password dopo 90 giorni
    - **PASS_MIN_LEN** = lunghezza minima della password

B. Modifica delle politiche relative alle password PAM

1. Aprire la configurazione password PAM:
2. sudo nano /etc/pam.d/common-password
3. Aggiungere o modificare la seguente riga:
4. password requisite pam_pwquality.so retry=3 minlen=12 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
    - minlen=12 → Lunghezza minima 12
    - ucredit=-1 → Almeno una lettera maiuscola
    - lcredit=-1 → Almeno una lettera minuscola
    - dcredit=-1 → Almeno una cifra
    - ocredit=-1 → Almeno un carattere speciale

Provalo: prova a cambiare una password con passwd studentuser — le password deboli dovrebbero essere rifiutate.

4.3 Linee guida per password sicure

Anche se le regole sono applicate, ricordate agli utenti le buone pratiche:

- Utilizzate **frasi di accesso** invece di singole parole.
- Evita parole presenti nel dizionario o schemi prevedibili.
- Non riutilizzare mai le password su più account.
- Utilizzate un **gestore di password** per un'archiviazione sicura.

4.4 Tabella riassuntiva: politiche relative alle password per piattaforma

Criterio	**Windows (Criteri di gruppo)**	**Linux (PAM/login.defs)**
Lunghezza minima	12 caratteri	PASS_MIN_LEN 12 / pam_pwquality minlen=12
Complessità	Richiede maiuscole, minuscolo, simbolo	pam_pwquality con ucredit/lcredit/dcredit/ocredit
Età massima 90 giorni		PASS_MAX_DAYS 90
Cronologia password	Ricorda le ultime 5 password	Gestito tramite moduli PAM

Punto di controllo

Prima di continuare:

- Hai configurato le politiche relative alle password in Windows o Linux?
- Hai verificato l'applicazione delle politiche modificando una password?
- Comprendi perché la scadenza e la complessità delle password sono importanti?

5. Limitazione dei privilegi amministrativi

Non tutti gli utenti dovrebbero avere il controllo completo di un sistema. Il **principio del privilegio minimo**
consiste nel concedere agli utenti solo l'accesso necessario per svolgere il proprio lavoro. Ciò riduce il rischio di configurazioni errate accidentali o azioni dannose.

5.1 Windows: gestione di utenti e gruppi locali

1. **Aprire Utenti e gruppi locali**
    - Premere **il tasto Windows + R**
    - Digita:
    - lusrmgr.msc
    - Premi **Invio**
2. **Controlla i membri del gruppo amministratori**
    - Nel pannello di sinistra, fai clic su **Gruppi**
    - Fai doppio clic su **Amministratori**
    - Controlla quali account sono elencati
3. **Rimuovi gli amministratori non necessari**
    - Seleziona tutti gli utenti che non devono avere diritti di amministratore
    - Fai clic su **Rimuovi**
4. **Verifica gli utenti standard**
    - Assicurati che **il** tuo **account di uso quotidiano** faccia parte solo del gruppo **Utenti**

Suggerimento: lascia sempre abilitato un account amministratore di emergenza, ma non utilizzarlo per il lavoro quotidiano.

5.2 Linux: Configurazione del file sudoers

1. **Controlla gli utenti sudo attuali**
   ```
   # Questo comando elencherà tutti gli utenti con
   privilegi sudo getent group sudo
   ```
2. **Rimuovere i diritti sudo non necessari**
   ```
   #Per rimuovere un utente dal gruppo sudo:
   sudo deluser nome utente sudo
   ```
3. **Modifica il file sudoers (se necessario)**
   ```
   # Apri con visudo (più sicuro che modificarlo
   direttamente) sudo visudo
   ```
4. Assicurarsi che solo gli account affidabili abbiano privilegi ALL=(ALL:ALL) ALL

Suggerimento: mantenere sempre un account amministratore, ma utilizzare un **account standard separato** per il lavoro quotidiano.

5.3 Best practice per la gestione dei privilegi

Creare **account amministratore e standard** separati. Utilizzare **i diritti di amministratore solo quando necessario**.
Controllare regolarmente gli account amministrativi.
Disattiva o rimuovi gli account inutilizzati.
Non condividere mai gli account amministrativi tra più utenti.

5.4 Riepilogo: controlli di accesso amministratore

Controllo dei diritti di amministratore della piattaforma		**Limitare i diritti di amministratore**
Windows	lusrmgr.msc → Gruppi → Amministratori	Rimuovere gli utenti non necessari dal gruppo Amministratori
Linux	getent group sudo	sudo deluser nome utente sudo / visudo

Punto di controllo
Prima di proseguire:

- Hai verificato chi ha i privilegi di amministratore/sudo?
- Hai rimosso gli account amministratore non necessari?
- Hai almeno un account standard per l'uso quotidiano?

6. Abilitazione della registrazione e del monitoraggio

I log sono **il** tuo **sistema di allerta precoce**. Registrano le attività di sistema come accessi, errori ed eventi di sicurezza, aiutandoti a rilevare attacchi o violazioni delle politiche.

In questa sezione, abiliterai e verificherai la registrazione sia su **Windows** che su **Linux**.

6.1 Windows: configurazione del Visualizzatore eventi

1. **Apri il Visualizzatore eventi**
    - Premere **il tasto Windows + R**
    - Digita:
    - eventvwr.msc
    - Premere **Invio**
2. **Controllare i registri di sicurezza, di sistema e delle applicazioni**
    - Nel menu a sinistra, espandi **Registri di Windows**
    - Controllare:
        - **Sicurezza** (tentativi di accesso, utilizzo dei privilegi)
        - **Sistema** (avvisi/errori a livello di sistema operativo)
        - **Applicazione** (attività dei programmi)
3. **Verificare che la registrazione di sicurezza sia attiva**
    - Se i registri di sicurezza sono vuoti, è possibile che il controllo non sia abilitato.
    - Per abilitare il controllo, aprire:
      gpedit.msc → Configurazione computer → Impostazioni di Windows → Impostazioni di sicurezza → Configurazione avanzata dei criteri di controllo → Criteri di controllo

Suggerimento: prestare attenzione ai tentativi di accesso ripetuti non riusciti, poiché potrebbero indicare un attacco di forza bruta.

6.2 Linux: Syslog e Auth.log

I sistemi Linux utilizzano in genere **rsyslog** o **syslog-ng** per gestire i log.

1. **Verificare se rsyslog è in esecuzione**
2. sudo systemctl status rsyslog
    - Se non è attivo, avvialo:
      sudo systemctl start rsyslog sudo
      systemctl enable rsyslog
3. **Visualizza i log di autenticazione**
    - I tentativi di accesso e l'attività sudo vengono registrati qui:
    - sudo less /var/log/auth.log
4. **Visualizza i registri generali di sistema**
    - Gli eventi a livello di sistema sono memorizzati qui:
    - sudo less /var/log/syslog

Suggerimento: utilizzare grep per cercare nei log, ad esempio:

grep "Password errata" /var/log/auth.log

6.3 Perché i log sono importanti

- **Rilevamento**: i tentativi di accesso non riusciti o di escalation dei privilegi risaltano.
- **Analisi forense**: i log forniscono prove dopo un incidente.
- **Conformità**: molti standard (ISO 27001, PCI DSS) richiedono la registrazione di sistema.

6.4 Tabella riassuntiva: log chiave da monitorare

Log della piattaforma da controllare	Scopo
Sicurezza Windows, sistema, applicazione	Monitoraggio di accessi, errori ed eventi del programma
Linux	/var/log/auth.log Autenticazione e attività sudo

Registri della piattaforma da controllare	Scopo
Linux /var/log/syslog	Eventi generali del sistema

Punto di controllo

Prima di proseguire:

- Hai abilitato e verificato la registrazione sulla tua VM?
- Riesci a individuare **i tentativi di accesso** nei tuoi registri?
- Capisci perché i registri sono fondamentali per il rilevamento degli attacchi?

7. Sfida di laboratorio

Ora è il momento di mettere insieme tutti gli elementi. Applicherai le politiche relative alle password, limiterai i privilegi di amministratore, abiliterai la registrazione e salverai il tuo sistema rafforzato come snapshot riutilizzabile.

7.1 Rafforza la tua VM

Applica le seguenti modifiche all'interno della tua VM:

- Applica **criteri di password** complessi (lunghezza, complessità, scadenza).
- Limita **i privilegi amministrativi** in modo che solo gli account affidabili abbiano diritti elevati.
- Abilita e verifica **la registrazione e il monitoraggio** (Visualizzatore eventi in Windows, auth.log e syslog in Linux).

7.2 Crea uno snapshot della tua VM protetta

Le istantanee consentono di salvare lo stato corrente della VM. Se in seguito si commettono errori, è possibile ripristinare questa baseline rafforzata.

Passaggi (esempio VirtualBox):

1. Spegnere o mettere in pausa la VM.
2. In VirtualBox, fai clic con il pulsante destro del mouse sulla tua VM → **Crea istantanea**.
3. Assegna un nome: *Base di riferimento rafforzata*
4. Aggiungi una descrizione (ad esempio, "Configurazione delle politiche relative alle password, delle restrizioni amministrative e della registrazione").

In VMware o Hyper-V, utilizzare la funzione **Snapshot/Checkpoint**.

7.3 Domande di riflessione

Annota le tue risposte nel tuo quaderno di laboratorio o inviale se richiesto:

1. Quali regole per le password hai configurato e come le hai testate?

2. Quali account hanno privilegi di amministratore/sudo dopo le modifiche apportate?
3. Quali log hai esaminato e quali eventi hai riscontrato?
4. In che modo gli snapshot ti aiuterebbero nella gestione della sicurezza nel mondo reale?
5. Quale sarebbe il **prossimo passo di rafforzamento** se questa VM entrasse in produzione?

Sfida completata!

Ora disponete di uno **snapshot VM consolidato**, ovvero una baseline sicura e riutilizzabile a cui potete ricorrere in qualsiasi momento. Questo rispecchia il modo in cui i professionisti IT preparano le "immagini golden" per l'implementazione aziendale.

8. Conclusioni e prospettive future

8.1 Punti chiave

In questo laboratorio hai **rafforzato** con successo **una macchina virtuale** applicando politiche di sicurezza reali. Nello specifico, hai:

Configurato un ambiente VM sicuro utilizzando VirtualBox, VMware o Hyper-V.
Applicato **regole di password complesse** per proteggere gli account.
Hai limitato **i privilegi amministrativi** solo agli utenti fidati.
Abilitato e verificato **la registrazione di sistema** per il monitoraggio e il rilevamento tempestivo degli attacchi. Creato **un'istantanea della VM**, che costituirà la vostra base di riferimento rafforzata per i laboratori futuri.

8.2 Competenze acquisite

Completando questo laboratorio, ora sei in grado di:

- Spiegare il principio del **privilegio minimo** e applicarlo.
- Configurare **criteri relativi alle password** su Windows e Linux.
- Gestire in modo efficace **gli account amministrativi e quelli standard**.
- Utilizzare **il Visualizzatore eventi** (Windows) e /var/log (Linux) per il monitoraggio della sicurezza.
- Creare e documentare **istantanee** per preservare gli stati di rafforzamento.

Queste sono le competenze amministrative fondamentali che ogni professionista della sicurezza informatica deve padroneggiare.

8.3 Argomento successivo: Nozioni fondamentali sulla sicurezza di rete

Ora che la tua VM è protetta, la sfida successiva è quella di proteggere **le** sue **connessioni con il mondo esterno**.

Nel prossimo **modulo Fondamenti di sicurezza di rete**, esplorerai:

- I protocolli di rete di base e come vengono sfruttati dagli hacker.
- Difese basate sulla rete come firewall, IDS/IPS e segmentazione.
- Laboratori pratici in cui analizzerai il traffico e proteggerai le comunicazioni.

Passaggi successivi

- Salva o invia le risposte alle domande di riflessione sul laboratorio.
- Conserva **lo snapshot della** tua **VM rinforzata** per utilizzarlo nei laboratori futuri.
- Preparati per il modulo **Fondamenti di sicurezza di rete**.

Hai creato una base solida e sicura a livello di sistema. Ora imparerai come proteggere quel sistema quando comunica in rete.

6. Appendice

6.1 Comandi Linux principali

Comando	Scopo
sudo adduser nome utente	Crea un nuovo utente standard
sudo deluser nome utente sudo	Rimuove un utente dal sudo (amministratore) .
sudo nano /etc/login.defs delle password	Modifica le impostazioni predefinite della politica
sudo nano /etc/pam.d/common-password	Configurare la complessità delle password PAM
sudo visudo	Modifica in modo sicuro il file sudoers
sudo systemctl status rsyslog	Verifica se il servizio di registrazione
è in esecuzione sudo less /var/log/auth.log	Esamina i registri di autenticazione
sudo less /var/log/syslog	Rivedere i registri generali del sistema
grep "Password errata" /var/log/auth.log	Cerca i tentativi di accesso non riusciti nei registri

6.2 Percorsi di accesso rapido di Windows

Attività	Percorso / Strumento
Apri l'Editor criteri di gruppo	gpedit.msc → Configurazione computer → Impostazioni di Windows → Impostazioni di sicurezza → Criteri account → Criteri password
Gestisci utenti e gruppi locali	lusrmgr.msc → Gruppi → Amministratori / Utenti
Visualizza registri di sicurezza	eventvwr.msc → Registri di Windows → Sicurezza
Abilita criteri di controllo avanzati	gpedit.msc → Impostazioni di sicurezza → Configurazione criteri di controllo avanzati

6.3 Suggerimenti per la risoluzione dei problemi

Problema	Possibile causa	Soluzione
Criteri password non applicati (Windows)	Ambito della politica errato / non ancora applicato	Eseguire gpupdate /force per applicare i criteri di gruppo
Password deboli ancora accettate (Linux)	Modulo PAM non configurato correttamente	Verificare che la password comune includa pam_pwquality
L'utente standard può ancora utilizzare le funzionalità di amministrazione	Utente rimasto in Amministratori o gruppo sudo	Rimuovere con lusrmgr.msc (Windows) / deluser (Linux)
I registri sono vuoti (Windows)	Controllo di sicurezza non abilitato	Configurare i criteri di controllo nell'Editor criteri di gruppo
Nessun auth.log su Linux	Servizio di registrazione disabilitato	Avvia rsyslog: sudo systemctl enable --now rsyslog

6.4 Risorse aggiuntive

Documentazione

- Microsoft Docs – Impostazioni dei criteri password: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy
- Documentazione sulla sicurezza di Ubuntu: https://ubuntu.com/security
- Guida al modulo PAM per la qualità delle password: http://www.linux-pam.org/Linux-PAM-html/sag-pam_pwquality.html

Strumenti e best practice

- Standard CIS (standard di rafforzamento del settore): https://www.cisecurity.org/cis-benchmarks
- Linee guida NIST sulle password (SP 800-63): https://pages.nist.gov/800-63-3/sp800-63b.html