Traccia

● Descrivere cos’è l’hardening dei sistemi.

● Produrre una checklist di hardening per Windows Server 2022 e per ogni voce descrivere le caratteristiche.

L'hardening dei sistemi è il processo di protezione e rafforzamento di un sistema informatico per ridurre le sue vulnerabilità e aumentare la sicurezza contro attacchi informatici o accessi non autorizzati. L'obiettivo è limitare il più possibile le opportunità di sfruttamento da parte di aggressori, applicando configurazioni, restrizioni e misure di protezione.

Principali attività di hardening

1. **Rimozione di software e servizi non necessari**: Disinstallare programmi, servizi o moduli non essenziali per ridurre la superficie di attacco.
2. **Aggiornamenti e patch**: Mantenere il sistema operativo e le applicazioni aggiornati per correggere vulnerabilità note.
3. **Configurazione di privilegi minimi**: Garantire che gli utenti e i processi abbiano solo i permessi strettamente necessari.
4. **Disabilitazione di porte e protocolli inutilizzati**: Chiudere le porte aperte o disattivare protocolli non necessari per limitare i punti di accesso.
5. **Firewall e controlli di rete**: Configurare regole per limitare il traffico di rete a ciò che è strettamente necessario.
6. **Autenticazione sicura**:
    - Implementare password forti e politiche di rotazione.
    - Utilizzare l'autenticazione a più fattori (MFA) dove possibile.
7. **Crittografia**:

    - Proteggere i dati in transito e a riposo con protocolli crittografici.
    - Evitare protocolli obsoleti come SSL 2.0/3.0 o cifrature deboli.
8. **Rafforzamento delle configurazioni di sistema**:
    - Limitare l'accesso al file system.
    - Configurare correttamente i log e il monitoraggio degli eventi.
9. **Protezione contro malware**: Utilizzare antivirus, sistemi di rilevamento delle intrusioni (IDS) e prevenzione (IPS).
10. **Policy di sicurezza rigorose**:
    - Impostare regole chiare per l'accesso remoto e locale.
    - Utilizzare configurazioni sicure per applicazioni e database.
11. **Disabilitazione delle funzionalità di debug o test**: Queste funzioni possono rivelare informazioni sensibili su un sistema.

1. Aggiornamenti e Patch

- **Caratteristica**: Mantenere il sistema operativo aggiornato con le ultime patch di sicurezza.
- **Dettagli**:
    - Configura Windows Update per il download automatico e l'installazione delle patch.
    - Controlla regolarmente eventuali aggiornamenti fuori banda per vulnerabilità critiche.

2. Configurazione del Firewall di Windows

- **Caratteristica**: Blocca traffico non autorizzato e permette solo quello necessario.
- **Dettagli**:
    - Configura regole specifiche per le porte e i protocolli richiesti dai servizi.
    - Attiva il firewall sia per il traffico in entrata che in uscita.
    - Implementa regole basate sull'indirizzo IP per restrizioni geografiche.

3. Gestione degli Account e delle Password

- **Caratteristica**: Impostazione di politiche rigide per utenti e credenziali.
- **Dettagli**:
    - Abilita l'autenticazione a due fattori (MFA) per gli

amministratori.
    - Applica criteri di password forti (lunghezza, complessità, scadenza).
    - Disabilita gli account inutilizzati o predefiniti (es. Guest).
    - Usa l'account amministratore solo quando necessario.

4. Crittografia e Protezione dei Dati

- **Caratteristica**: Protezione dei dati a riposo e in transito.
- **Dettagli**:
    - Abilita BitLocker per crittografare i dischi del server.
    - Usa TLS 1.2 o superiore per la crittografia delle comunicazioni.
    - Configura Windows SMB con crittografia, se usato per condivisione file.

5. Disabilitazione dei Servizi Non Necessari

- **Caratteristica**: Ridurre la superficie di attacco disabilitando componenti non usati.
- **Dettagli**:
    - Usa il comando Get-Service per elencare i servizi in esecuzione.
    - Disattiva servizi come "Server", "Print Spooler" o "Remote Desktop" se non necessari.

6. Protezione dei Ruoli e delle Funzionalità

- **Caratteristica**: Installare solo i ruoli e le funzionalità richiesti.
- **Dettagli**:
    - Usa Server Manager per selezionare solo ciò che serve (es. IIS, Hyper-V).
    - Controlla regolarmente eventuali componenti installati non utilizzati.

7. Configurazione del Registro Eventi

- **Caratteristica**: Monitoraggio dettagliato delle attività e degli eventi del sistema.
- **Dettagli**:
    - Configura la registrazione degli eventi di sicurezza, applicazioni e sistema.
    - Aumenta il limite delle dimensioni dei log per evitare sovrascritture.
    - Configura inoltro degli eventi (Event Forwarding)

verso un server centralizzato.

8. Controllo degli Accessi Basato su Ruoli (RBAC)

- **Caratteristica**: Limita i permessi secondo il principio del minimo privilegio.
- **Dettagli**:
  - Usa "Active Directory" per assegnare ruoli specifici agli utenti.
  - Configura politiche di accesso tramite Group Policy.
  - Impedisci agli utenti standard di eseguire script o software amministrativi.

9. Protezione del Desktop Remoto (RDP)

- **Caratteristica**: Rafforza la sicurezza delle connessioni RDP.
- **Dettagli**:
  - Cambia la porta RDP predefinita (3389) con una personalizzata.
  - Usa crittografia Network Level Authentication (NLA).
  - Restringi l'accesso RDP a indirizzi IP specifici tramite firewall.

10. Implementazione di Windows Defender

- **Caratteristica**: Protezione antivirus e anti-malware integrata.
- **Dettagli**:
  - Configura scansioni automatiche e aggiornamenti delle definizioni.
  - Usa il modulo Windows Defender Exploit Guard per mitigazioni avanzate.
  - Attiva il controllo di accesso controllato alle cartelle per proteggere i file da ransomware.

11. Disabilitazione del Protocollo SMBv1

- **Caratteristica**: Evitare vulnerabilità note come WannaCry.
- **Dettagli**:
  - Rimuovi SMBv1 dal server tramite PowerShell (Disable-WindowsOptionalFeature).
  - Usa SMBv2 o SMBv3 per una maggiore sicurezza.

12. Configurazione delle Politiche di Audit

- **Caratteristica**: Controllare e registrare eventi chiave per

rilevare attività sospette.

- **Dettagli**:
  - Configura auditing avanzato per modifiche ai file, accessi non riusciti e modifiche di configurazione.
  - Integra con un SIEM (Security Information and Event Management) per analisi centralizzate.

13. Protezione contro Attacchi Brute-Force

- **Caratteristica**: Limitare i tentativi di accesso falliti.
- **Dettagli**:
  - Configura il blocco dell'account dopo un numero specifico di tentativi falliti.
  - Imposta intervalli di sblocco lunghi per account bloccati.

14. Backup Regolari e Protetti

- **Caratteristica**: Pianifica backup completi e incrementali.
- **Dettagli**:
  - Usa Windows Server Backup o soluzioni di terze parti.
  - Conserva i backup in location sicure e isolati dalla rete principale.

15. Abilitazione di Secure Boot

- **Caratteristica**: Protezione del sistema all'avvio.
- **Dettagli**:
  - Abilita Secure Boot nel BIOS per evitare l'esecuzione di software non autorizzati.
  - Usa dispositivi con supporto TPM per maggiore sicurezza.