Windows Server 2022

Sommario

Traccia esercizio

- Descrivere cos'è l'hardening dei sistemi.
- Produrre una checklist di hardening per Windows Server 2022 e per ogni voce descrivere le caratteristiche.

Svolgimento esercizio

Cos'è l'hardening dei sistemi

L'hardening dei sistemi è il processo di configurazione, protezione e ottimizzazione di un sistema operativo o di un'applicazione per ridurne al minimo la superficie d'attacco e le vulnerabilità. Questo processo prevede l'eliminazione o la limitazione di servizi, funzionalità e configurazioni non necessarie, rafforzando così la sicurezza complessiva. L'obiettivo è ridurre il rischio di compromissione da parte di attaccanti minimizzando i punti di ingresso per potenziali exploit.

Il processo di hardening prevede diverse attività, tra cui:

- Disabilitare servizi inutili
- Applicare politiche di sicurezza rigorose
- Aggiornare e patchare regolarmente il sistema
- Configurare logging e monitoraggio
- Implementare controlli di accesso e autenticazione forti
- Adottare il principio del minimo privilegio

Checklist di Hardening per Windows Server 2022

Ecco una checklist con descrizione dettagliata delle voci:

1. Aggiornamenti e Patch

- **Caratteristiche:**
  - Verifica che il sistema operativo e i software installati siano aggiornati con le ultime patch di sicurezza.
  - Automatic Updates deve essere configurato per applicare aggiornamenti critici.
- **Perché è importante:** Gli aggiornamenti correggono vulnerabilità note e riducono il rischio di exploit.

2. Disabilitazione dei Servizi Non Necessari

- **Caratteristiche:**
  - Identifica e disabilita i servizi di Windows non essenziali per le funzionalità richieste, come Telnet, FTP, Remote Desktop Gateway (se non utilizzato), ecc.
- **Perché è importante:** Riduce la superficie d'attacco eliminando vettori inutili.

3. Configurazione delle Politiche di Gruppo (Group Policy)

- **Caratteristiche:**
  - Configura le GPO per applicare politiche di sicurezza come blocco degli account dopo diversi tentativi di accesso falliti, scadenza delle password e restrizioni per l'accesso remoto.
- **Perché è importante:** Rafforza il controllo sugli account e impedisce attacchi di brute force.

4. Firewall e Networking

- **Caratteristiche:**
  - Configura il firewall di Windows Defender per consentire solo il traffico necessario.
  - Chiudi tutte le porte non utilizzate e monitora il traffico di rete.
- **Perché è importante:** Protegge il sistema da connessioni non autorizzate.

5. Antivirus e Protezioni Anti-Malware

- **Caratteristiche:**
  - Installa e configura Windows Defender o un antivirus di terze parti.
  - Attiva la protezione in tempo reale e pianifica scansioni periodiche.
- **Perché è importante:** Protegge il sistema da malware e altre minacce.

6. Gestione delle Password

- **Caratteristiche:**
  - Imposta requisiti di complessità e lunghezza per le password.
  - Applica politiche di scadenza delle password.
- **Perché è importante:** Le password complesse riducono il rischio di compromissione degli account.

7. Controllo degli Account e dei Privilegi

- **Caratteristiche:**
  - Rimuovi account utente non necessari.
  - Applica il principio del minimo privilegio per gli account amministrativi.
- **Perché è importante:** Limita il potenziale di danneggiamento in caso di compromissione di un account.

8. Auditing e Logging

- **Caratteristiche:**
  - Configura il registro eventi di Windows per monitorare accessi, modifiche di sistema e attività sospette.
  - Conserva i log in un server centralizzato per evitare manipolazioni.
- **Perché è importante:** Consente rilevamento e risposta rapida alle attività anomale.

9. Crittografia dei Dati

- **Caratteristiche:**
  - Abilita BitLocker per proteggere i dati sui dischi.
  - Utilizza certificati SSL/TLS per proteggere le comunicazioni di rete.
- **Perché è importante:** Protegge i dati sensibili in caso di furto o accesso non autorizzato.

10. Protezione RDP (Remote Desktop Protocol)

- **Caratteristiche:**
  - Disabilita RDP se non necessario.
  - Se utilizzato, configura Network Level Authentication (NLA) e limita gli accessi con whitelist di IP.
- **Perché è importante:** RDP è un vettore comune di attacchi brute force; una configurazione sicura riduce il rischio.

11. Disabilitazione di SMBv1

- **Caratteristiche:**
  - Disabilita il protocollo SMBv1, noto per avere vulnerabilità gravi (ad esempio, exploit EternalBlue).
- **Perché è importante:** Migliora la sicurezza della condivisione dei file.

12. Protezione del BIOS/UEFI

- **Caratteristiche:**
  - Configura una password per l'accesso al BIOS/UEFI.
  - Abilita Secure Boot per prevenire l'esecuzione di firmware o sistemi operativi non autorizzati.
- **Perché è importante:** Previene attacchi a basso livello sul sistema.

13. Disabilitazione dell'Esecuzione di Script Non Sicuri

- **Caratteristiche:**
  - Configura PowerShell per eseguire solo script firmati digitalmente.
  - Disabilita l'esecuzione di script non necessari.
- **Perché è importante:** Riduce la possibilità di esecuzione di script dannosi.

14. Backup Sicuri e Testati

- **Caratteristiche:**
  - Implementa backup regolari e conserva copie offline.
  - Testa periodicamente il ripristino dei dati.
- **Perché è importante:** Garantisce il recupero dei dati in caso di attacco ransomware o guasto.

15. Blocchi per USB e Dispositivi Esterni

- **Caratteristiche:**
  - Configura restrizioni per l'uso di dispositivi USB e periferiche.
  - Usa soluzioni DLP (Data Loss Prevention) per monitorare e bloccare trasferimenti non autorizzati.
- **Perché è importante:** Riduce il rischio di furto di dati o introduzione di malware.

Conclusione

Questa checklist copre i principali aspetti dell'hardening per Windows Server 2022. Ogni organizzazione dovrebbe adattare queste misure in base al contesto specifico, alle esigenze aziendali e ai requisiti normativi. Dopo aver applicato queste misure, è consigliabile condurre un penetration test per verificare l'efficacia del processo di hardening.