

ChatGPT - EXTRA

Prompt 1:

Ok, oggi devo insegnare ai miei studenti come possono proteggersi da attacchi di malintenzionati sulla macchina virtuale con Sistema Operativo Windows 10. Puoi elencarmi in modo specifico e professionale quali sono le vulnerabilità di questo sistema operativo?

Risposta:

Troppo Generica non mi soddisfaceva

Prompt 2:

Ok ma sono riportate online anche vulnerabilità note come porte aperte, bug etc?

Risposta

EternalBlue (CVE-2017-0144)

- **Descrizione:** Questa vulnerabilità riguarda il protocollo **SMBv1** (Server Message Block version 1) e fu sfruttata nel famoso attacco ransomware **WannaCry**. L'attacco sfrutta un bug nell'implementazione di SMBv1 in Windows per consentire l'esecuzione di codice remoto.
- **Porte aperte:** **Porta 445 (SMB)**.
- **Protezione:** Disabilitare **SMBv1** e bloccare la **porta 445** nel firewall. Aggiornare Windows con le ultime patch di sicurezza per correggere la vulnerabilità.

2. PrintNightmare (CVE-2021-34527)

- **Descrizione:** Questa vulnerabilità nel **Windows Print Spooler** consente a un attaccante di eseguire codice arbitrario con privilegi di sistema. Un attaccante potrebbe sfruttare questa vulnerabilità per ottenere il controllo totale di una macchina vulnerabile.
- **Porte aperte:** **Porta 139 (NetBIOS), Porta 445 (SMB)**.
- **Protezione:** Disabilitare il **Windows Print Spooler** se non è necessario, applicare l'ultima patch di sicurezza di Microsoft.

3. BlueKeep (CVE-2019-0708)

- **Descrizione:** Una vulnerabilità critica nel **Remote Desktop Protocol (RDP)** che permette l'esecuzione di codice remoto non autenticato. È una vulnerabilità di **esecuzione di codice remoto (RCE)** che può essere sfruttata senza interazione dell'utente.
- **Porte aperte:** **Porta 3389 (RDP)**.
- **Protezione:** Disabilitare il **Remote Desktop Protocol (RDP)** se non necessario. Applicare le patch di sicurezza e bloccare la **porta 3389** tramite firewall.

4. CVE-2020-0601 (CurveBall)

- **Descrizione:** Questa vulnerabilità riguarda l'**API criptografica Windows CryptoAPI** e permette agli attaccanti di creare certificati falsificati per eseguire attacchi **Man-in-the-Middle** (MitM), ingannando i sistemi di validazione del certificato.
- **Protezione:** Assicurarsi di applicare tutti gli aggiornamenti relativi alla sicurezza rilasciati da Microsoft. Utilizzare solo certificati affidabili.

5. CVE-2020-1472 (Zerologon)

- **Descrizione:** Una vulnerabilità nel **Netlogon Remote Protocol** che consente agli attaccanti di elevare i privilegi a livello di dominio in Windows Server, con il rischio di compromettere l'intero dominio.
- **Porte aperte:** **Porta 445 (SMB)**, **Porta 135 (MS RPC)**.
- **Protezione:** Aggiornare immediatamente i sistemi che utilizzano **Netlogon** per ridurre il rischio. Microsoft ha rilasciato patch specifiche per questa vulnerabilità.

6. CVE-2021-36934 (HiveNightmare)

- **Descrizione:** Una vulnerabilità che riguarda il **Windows Security Account Manager (SAM)**, che consente a un attaccante locale di leggere le informazioni degli account utente, compresi gli hash delle password.
- **Protezione:** Microsoft ha rilasciato una patch che risolve il problema. Assicurarsi che il sistema sia aggiornato con l'ultima versione della patch. Proteggere la cartella **C:\Windows\System32\config** tramite **permessi** di accesso.

7. CVE-2018-8453 (Windows DNS Server)

- **Descrizione:** Questa vulnerabilità è nel **Windows DNS Server** e consente a un attaccante di eseguire **remote code execution** (RCE) attraverso l'invio di richieste DNS dannose.
- **Porte aperte:** **Porta 53 (DNS)**.
- **Protezione:** Applicare gli aggiornamenti di sicurezza e limitare l'accesso alle porte **DNS** per ridurre il rischio di attacchi.

8. Elevazione dei privilegi tramite DLL hijacking

- **Descrizione:** Windows permette a un programma di caricare file DLL (Dynamic Link Library). Un attaccante può sfruttare questo comportamento caricando una DLL malevola in una directory vulnerabile, consentendo l'esecuzione di codice arbitrario con privilegi elevati.
- **Porte aperte:** Nessuna porta aperta specifica, la vulnerabilità è più legata alla **gestione dei file**.
- **Protezione:** **Monitorare** le directory di sistema e **bloccare** l'accesso non autorizzato. Configurare il sistema per evitare l'esecuzione di file DLL sconosciuti.

9. Vulnerabilità di configurazione della rete (Windows SMB, RDP, Netlogon)

- **Descrizione:** Una configurazione errata nelle impostazioni di rete di Windows può esporre vulnerabilità note, come SMB, RDP o altri servizi di condivisione di rete. Queste porte possono essere facilmente individuate e sfruttate da attaccanti.
- **Porte aperte:** **Porta 445 (SMB), Porta 3389 (RDP), Porta 135 (MS RPC).**
- **Protezione:** Utilizzare un **firewall** per limitare le porte aperte alle necessità specifiche. Disabilitare i protocolli di rete non necessari (SMBv1, RDP, Netlogon, ecc.).

10. Vulnerabilità nel controllo dell'account utente (UAC)

- **Descrizione:** Un attaccante può sfruttare un bug nel sistema di controllo dell'account utente (UAC) per eseguire codice con privilegi di amministratore.
- **Protezione:** Configurare **UAC** per richiedere sempre l'autorizzazione per l'esecuzione di programmi con privilegi elevati