ESERCIZIO W15D1

L’esercizio va ad esporre NULL session, la vulnerabilità che ha colpito gli utenti Windows con le versioni precedenti.

Traccia:

• Spiegare brevemente cosa vuol dire Null Session

• Elencare i sistemi che sono vulnerabili a Null Session

• Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?

• Elencare le modalità per mitigare o risolvere questa vulnerabilità

• Commentare queste azioni di mitigazione, spiegando l’efficacia e l’effort per l’utente/azienda.

Spiegazione Null Session

È una vulnerabilità storica propria dei vecchi sistemi Windows, utilizzabile sia in locale che in remoto. Il Null Session permette ad un attaccante di entrare in una share locale senza autenticazione.

Sistemi vulnerabili Null Session

Windows server 2000, Windows XP, Windows 7, Windows 8.

Questi sistemi esistono ancora?

Windows 2000: Vista l’età e le limitazioni d’uso, è improbabile che esista ancora sul mercato.

Windows XP: è morto nel 2014, ma molte organizzazioni continua ancora ad usarlo.

Windows 7: Finito in end of life nel 2020, Windows 7 ha continuato a ricevere supporto fino all'anno scorso. Molto probabile quindi che alcune aziende ancora lo usino.

Windows 8: Avendo falle nella sicurezza, Windows 8 è passato a miglior vita nell'anno 2016. Windows ha chiesto agli utenti di aggiornare il sistema alla versione 8.1, che ha terminato il supporto lo scorso anno.

Elenco remediation action

Registro di sistema, autorizzazioni condivisioni, monitoring, soluzioni di terze parti, aggiornamento.

Azioni di mitigazione

1. **Bloccare l'accesso anonimo tramite il Registro di sistema**:
    - Modificare le chiavi del Registro di sistema per impedire l'accesso anonimo tramite SMB.
    - Andare su HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters.
    - Impostare il valore DWORD RestrictAnonymous su 2 per disabilitare l'accesso anonimo.
    - Riavviare il servizio Server o il sistema per applicare le modifiche.

2. **Configurare le autorizzazioni delle condivisioni**
    - Assicurarsi che le condivisioni di rete siano configurate correttamente.
    - Limitare l'accesso alle condivisioni solo agli utenti autorizzati.
    - Evitare di concedere autorizzazioni di lettura o scrittura a "Everyone" o "Guest".
3. **Monitorare gli eventi di accesso anonimo**:
    - Configurare il monitoraggio degli eventi di accesso anonimo nei log di sicurezza.
    - Monitorare gli accessi anonimi per individuare eventuali attività sospette.
4. **Utilizzare soluzioni di sicurezza di terze parti**:
    - Esistono strumenti di sicurezza che possono rilevare e mitigare le sessioni null.
    - Valutare l'implementazione di soluzioni come **IDS/IPS**, **firewall avanzati** o **sistemi di rilevamento delle intrusioni**.
5. **Aggiornare il sistema operativo e le patch di sicurezza**:
    - Mantenere il sistema operativo Windows aggiornato con le ultime patch di sicurezza.
    - Le patch spesso risolvono vulnerabilità note, inclusa quella delle sessioni null.