Nella lezione teorica abbiamo visto la **Null Session**, vulnerabilità che colpisce Windows

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.

Null Session: Una Breve Spiegazione

Una Null Session è una connessione non autenticata a un sistema Windows che consente a un attaccante di accedere a determinate informazioni di rete e di sistema senza bisogno di credenziali. Questo tipo di connessione sfrutta una vulnerabilità nei protocolli SMB (Server Message Block) e NBT (NetBIOS over TCP/IP), permettendo l'accesso a risorse come l'elenco degli utenti, gruppi, e condivisioni di rete.

Sistemi Vulnerabili a Null Session

I sistemi operativi principalmente vulnerabili a Null Session sono:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

Questi sistemi operativi sono progettati per permettere, per impostazione predefinita, connessioni Null Session, offrendo così un'ampia superficie di attacco.

Stato Attuale di Questi Sistemi Operativi

Questi sistemi operativi esistono ancora ma sono considerati obsoleti. Microsoft ha cessato il supporto ufficiale per questi sistemi anni fa:

- Windows NT 4.0: Fine del supporto nel 2004.
- Windows 2000: Fine del supporto nel 2010.
- Windows XP: Fine del supporto nel 2014.
- Windows Server 2003: Fine del supporto nel 2015.

Anche se non sono più supportati, potrebbero essere ancora in uso in ambienti legacy o sistemi non aggiornati, rappresentando un rischio significativo.

Modalità di Mitigazione o Risoluzione della Vulnerabilità Null Session

1. Aggiornamento del Sistema Operativo: Aggiornare a versioni più recenti di Windows (come Windows 10 o Windows Server 2019) che non sono vulnerabili a Null Session.
2. Configurazioni di Sicurezza: Modificare le impostazioni di sicurezza per disabilitare le Null Session:
    - Utilizzare il registro di sistema per disabilitare l'accesso anonimo.
    - Configurare le politiche di sicurezza locali per restringere l'accesso anonimo alle risorse.
3. Firewall e Filtri di Rete: Utilizzare firewall per bloccare il traffico SMB e NBT non autorizzato e limitare l'accesso alle reti fidate.
4. Strumenti di Rilevamento delle Vulnerabilità: Impiegare strumenti di scansione delle vulnerabilità per identificare e mitigare le Null Session.
5. Segregazione delle Reti: Separare i sistemi legacy vulnerabili dalle reti principali per limitare l'esposizione.

Commento sulle Azioni di Mitigazione

1. Aggiornamento del Sistema Operativo
    - Efficacia: Altissima, in quanto risolve definitivamente il problema delle Null Session.
    - Effort: Alto, può richiedere significativi investimenti in tempo e risorse, oltre a potenziali problemi di compatibilità con applicazioni legacy.
2. Configurazioni di Sicurezza
    - Efficacia: Elevata, poiché riduce notevolmente la possibilità di sfruttare Null Session.
    - Effort: Moderato, richiede conoscenze tecniche specifiche e una gestione accurata delle configurazioni di sicurezza.
3. Firewall e Filtri di Rete
    - Efficacia: Alta, impedisce l'accesso non autorizzato dall'esterno.
    - Effort: Moderato, necessita di una configurazione accurata e gestione continua per garantire che le regole siano sempre aggiornate.
4. Strumenti di Rilevamento delle Vulnerabilità
    - Efficacia: Variabile, dipende dalla frequenza e dall'accuratezza delle scansioni.
    - Effort: Moderato, richiede l'implementazione di strumenti e l'analisi dei risultati, ma offre una buona visibilità sui rischi.
5. Segregazione delle Reti
    - Efficacia: Alta, limita l'accesso ai sistemi vulnerabili.
    - Effort: Moderato, può richiedere una riorganizzazione delle reti e la gestione di segmenti di rete separati.

La mitigazione delle vulnerabilità di Null Session richiede un bilanciamento tra efficacia e effort, con le soluzioni più sicure (aggiornamenti di sistema) che richiedono maggiori risorse e pianificazione, mentre altre misure (configurazioni e firewall) offrono una buona protezione con un effort più contenuto.