1. **Report “Null Session” W15D1 Zanini Riccardo**

Legenda:

1.Cos'è una Null Session

2.Sistemi vulnerabili a Null Session

3.Esistenza dei sistemi operativi vulnerabili

4.Modalità per mitigare o risolvere la vulnerabilità

5.Commento sulle azioni di mitigazione

1.Cos'è una Null Session

Una sessione null è una connessione anonima ad un servizio di rete di comunicazione tra processi su computer basati su Windows. Consente agli utenti non autenticati di accedere a determinate informazioni e risorse di sistema, come elenchi di utenti, condivisioni di rete e servizi. Sebbene progettata per scopi legittimi, la sessione null può essere sfruttata da malintenzionati per raccogliere informazioni sensibili e compromettere la sicurezza del sistema.

Come avviene una null session:

- **Stabilimento della connessione:** L'attaccante invia una richiesta di connessione al servizio IPC del computer target utilizzando il protocollo SMB (Server Message Block).
- **Autenticazione null:** La richiesta non include credenziali di autenticazione, quindi il server la gestisce come una sessione null.
- **Accesso alle informazioni:** Se la sessione null è abilitata sul sistema target, l'attaccante ottiene un accesso limitato alle risorse di sistema. Può inviare comandi al server IPC per:
- Elencare gli utenti e i gruppi del sistema.
- Elencare le condivisioni di rete.
- Visualizzare i processi in esecuzione.
- Ottenere informazioni sui servizi attivi.
- **Sfruttamento delle informazioni:** L'attaccante può utilizzare le informazioni ottenute per:
- Identificare potenziali target per ulteriori attacchi.
- Pianificare attacchi mirati.
- Rubare dati sensibili.
- Compromettere la sicurezza del sistema.

Enum4Linux

Di seguito vedremo come ad esempio è possibile utilizzare un semplice tool Enum4Linux per sfruttare le vulnerabilità di un sistema.

Enum4Linux è uno strumento open source per sistemi Linux che permette di enumerare e raccogliere informazioni dettagliate su un sistema operativo.

Come usarlo?

- Installa Enum4Linux sul tuo sistema Linux.
- Esegui il comando `enum4linux` con gli switch appropriati:
    - `-S`: Elenca le condivisioni di rete, incluse quelle amministrative.
    - `-U`: Estrae i nomi utente.
    - `-P`: Controlla le policy password.
- Utilizza le informazioni ottenute per configurare un attacco all'autenticazione su rete tramite file Batch

Creare un file batch:

- Creare un file batch con estensione `.bat` sul proprio sistema Linux.
- Inserire il seguente codice nel file batch, sostituendo i nomi utente e le condivisioni di rete con quelli ottenuti nel passaggio 1:

```
net use \\192.168.1.100\share /user:username password
   1. copy C:\path\to\file \\192.168.1.100\share
net use \\192.168.1.100\share /delete
```

- Sostituire `192.168.1.100` con l'indirizzo IP del sistema target.
- Sostituire `share` con il nome della condivisione di rete con permessi di scrittura.
- Sostituire `username` con il nome utente con privilegi elevati.
- Sostituire `password` con la password dell'utente con privilegi elevati.
- Sostituire `C:\path\to\file` con il percorso del file da copiare sul sistema target.

Il primo comando `net use` stabilisce una connessione alla condivisione di rete specificata, utilizzando le credenziali dell'utente con privilegi elevati.

- Il secondo comando `copy` copia il file specificato sulla condivisione di rete.
- Il terzo comando `net use` elimina la connessione alla condivisione di rete.

2.Sistemi vulnerabili a Null Session

I sistemi principalmente vulnerabili alle sessioni null sono quelli che eseguono il sistema operativo Windows, in particolare:

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

Versioni più recenti di Windows, come Windows Vista, Windows 7 e versioni successive, hanno implementato misure di sicurezza che limitano o eliminano la vulnerabilità della sessione null.

3.Esistenza dei sistemi operativi vulnerabili

Mentre i sistemi operativi elencati in precedenza sono ancora in uso in alcuni casi, la loro diffusione è notevolmente diminuita con il tempo. La maggior parte delle organizzazioni e degli utenti ha adottato versioni più recenti di Windows che non sono vulnerabili alle sessioni null.

4.Modalità per mitigare o risolvere la vulnerabilità

Esistono diverse modalità per mitigare o risolvere la vulnerabilità della sessione null:

- **Disabilitare le sessioni null:** Questa è la soluzione più efficace e consiste nel disattivare completamente la funzionalità di sessione null a livello di sistema operativo.

- **Limitare l'accesso alle condivisioni di rete:** È possibile limitare l'accesso alle condivisioni di rete solo agli utenti autenticati, impedendo così agli utenti anonimi di accedervi tramite sessioni null.
- **Utilizzare firewall e software di sicurezza:** Implementare firewall e software di sicurezza in grado di filtrare e bloccare il traffico proveniente da sessioni null.
- **Aggiornare i sistemi operativi:** Aggiornare i sistemi operativi alle versioni più recenti di Windows che non sono vulnerabili alle sessioni null.

Come disabilitare le sessioni null per i principali sistemi operativi vulnerabili:

Windows XP:

1. Fare clic con il pulsante destro del mouse su **Risorse del computer** e selezionare **Gestisci**.
2. Espandere **Strumenti di sistema** e fare clic su **Criteri di gruppo locali**.
3. Nella console Criteri di gruppo locali, espandere **Configurazione del computer** > **Impostazioni di Windows** > **Impostazioni di sicurezza** > **Criteri locali** > **Assegnazione dei diritti utente**.
4. Fare doppio clic su **Non consentire connessioni guest** nel pannello di destra.
5. Nella finestra **Proprietà Non consentire connessioni guest**, selezionare la casella **Attiva**.
6. Fare clic su **OK** per salvare le modifiche.

Windows Server 2003:

1. Fare clic con il pulsante destro del mouse su **Risorse del computer** e selezionare **Gestisci**.
2. Espandere **Strumenti di sistema** e fare clic su **Criteri di gruppo**.
3. Nella console Criteri di gruppo, espandere **Configurazione del computer** > **Impostazioni di Windows** > **Impostazioni di sicurezza** > **Criteri locali** > **Assegnazione dei diritti utente**.
4. Fare doppio clic su **Non consentire connessioni guest** nel pannello di destra.
5. Nella finestra **Proprietà Non consentire connessioni guest**, selezionare la casella **Attiva**.
6. Fare clic su **OK** per salvare le modifiche.

Windows 7 e versioni successive:

Le sessioni null sono state disabilitate per impostazione predefinita in Windows 7 e versioni successive.

Tuttavia, è possibile riattivarle seguendo questi passaggi:

1. Aprire **Editor del Registro di sistema**.
2. Accedere alla chiave di registro seguente:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
```

3. Creare un nuovo valore DWORD (32 bit) denominato **NullSessionShares** e impostarne il valore su **0**.
4. Riavviare il computer.

5.Commento sulle azioni di mitigazione

Efficacia:

- La disabilitazione delle sessioni null offre la massima protezione, ma può comportare problemi di compatibilità con alcune applicazioni legacy.
- La limitazione dell'accesso alle condivisioni di rete è una soluzione efficace, ma richiede una configurazione accurata.

- I firewall e il software di sicurezza possono fornire un livello di protezione, ma potrebbero non essere in grado di bloccare tutti i tentativi di accesso anonimo.
- L'aggiornamento dei sistemi operativi è la soluzione più a lungo termine e garantisce la massima protezione contro le vulnerabilità note.

Effort:

- La disabilitazione delle sessioni null e la limitazione delle condivisioni di rete richiedono competenze tecniche e potrebbero comportare modifiche alla configurazione del sistema.
- L'implementazione di firewall e software di sicurezza richiede la selezione, l'installazione e la configurazione di strumenti adeguati.
- L'aggiornamento dei sistemi operativi può essere un processo semplice o complesso, a seconda del numero di sistemi coinvolti e della compatibilità con software e hardware esistenti.

Scelta della soluzione migliore:

La scelta della soluzione migliore dipende da diversi fattori, tra cui la gravità del rischio, le risorse disponibili e le competenze tecniche. In generale, si consiglia di disabilitare le sessioni null e limitare l'accesso alle condivisioni di rete, oltre a utilizzare firewall e software di sicurezza e aggiornare i sistemi operativi alle versioni più recenti.

Conclusione

Le sessioni null rappresentano una vulnerabilità di sicurezza che può essere sfruttata da malintenzionati per compromettere i sistemi Windows. Adottare le opportune misure di mitigazione, come la disabilitazione delle sessioni null, la limitazione dell'accesso alle condivisioni di rete, l'utilizzo di firewall e software di sicurezza e l'aggiornamento dei sistemi operativi, è fondamentale per proteggere i propri sistemi da attacchi informatici.