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.

Cos'è una Null Session

La Null Session è una connessione anonima a un sistema Windows, utilizzata per ottenere informazioni su quel sistema senza autenticarsi. Questo tipo di connessione sfrutta una caratteristica (o vulnerabilità) dei sistemi operativi Windows che permette a utenti non autenticati di stabilire una sessione di rete con il server, chiamata "null session". Questa sessione può essere utilizzata per enumerare utenti, gruppi, condivisioni di rete e altre informazioni sensibili.

Sistemi Vulnerabili

I sistemi vulnerabili alle null sessions sono principalmente le versioni precedenti di Microsoft Windows. Di seguito un elenco dei sistemi operativi storicamente vulnerabili:

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

Anche se questi sistemi operativi sono obsoleti, è possibile che alcune organizzazioni li utilizzino ancora per applicazioni legacy. Tuttavia, con l'avanzamento delle versioni di Windows e con l'introduzione di misure di sicurezza migliorate, la vulnerabilità delle null sessions è stata mitigata nelle versioni successive di Windows.

Sistemi Ancora in Uso

Nonostante i progressi tecnologici, alcuni sistemi vulnerabili potrebbero ancora essere in uso per vari motivi, tra cui:

- **Compatibilità con applicazioni legacy:** Alcune organizzazioni potrebbero continuare a utilizzare sistemi operativi più vecchi per mantenere la compatibilità con software non aggiornati.
- **Costi di aggiornamento:** L'aggiornamento dei sistemi operativi può essere costoso e complesso, specialmente per le grandi organizzazioni.
- **Mancanza di consapevolezza:** Alcune organizzazioni potrebbero non essere consapevoli delle vulnerabilità esistenti nei loro sistemi.
-

Mitigazione delle Null Sessions

Per mitigare le vulnerabilità legate alle null sessions, gli amministratori di rete possono adottare diverse misure. Di seguito, elenchiamo le soluzioni tecniche per prevenire tali attacchi:

1. Disabilitare le Null Sessions
2. Limitare le condivisioni accessibili tramite Null Session
3. Configurare la Group Policy
4. Disabilitare l'accesso anonimo alle risorse di rete
5. Utilizzare Firewall e Controlli di Accesso
6. Monitorare e Rivedere i Log di Sicurezza
7. Aggiornare i Sistemi Operativi

Conclusione

Le null sessions rappresentano una vulnerabilità significativa nei vecchi sistemi operativi Windows. Sebbene queste vulnerabilità possano essere sfruttate per raccogliere informazioni sensibili, esistono diverse tecniche e misure che possono essere adottate per mitigare questi rischi. È fondamentale per le organizzazioni rimanere aggiornate con le pratiche di sicurezza informatica e implementare regolarmente misure preventive per proteggere i loro sistemi e dati sensibili.