NULL SESSION - ESERCIZIO

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.

Esecuzione:

Spiegazione di NULL SESSION

Le **NULL SESSION** sono connessioni di rete anonime e senza autenticazione ad una risorsa condivisa presente in un sistema Windows. Essa effettua delle sessioni con accesso ad informazioni sul sistema senza dover richiedere dati di accesso validi ad esse. Sono una minaccia di tipo critico perché, oltre a poter accedere al sistema target senza una verifica di chi si sta connettendo, mette "a nudo" dati sensibili dell'azienda quali:

- Liste di account utente con relative password
- Risorse condivise
- Altre informazioni sensibili
- Gruppi di sistema
- Programmi presenti ed attivi e/o in esecuzione

Elenco di sistemi che sono vulnerabili a Null Session

I sistemi vulnerabili che (negli anni poi sono sparite o sono state sostituite) possono essere le seguenti:

- Sistemi Windows NT, Windows 2000 e XP
- Sistemi Windows Server < 2003

Tuttavia questi sistemi non sono più presenti ad oggi. Di fatto sono state sostituite da nuovi sistemi più "forti" oppure hanno aggiornato le stesse rendendo difficile che si verifichi una Null Session.

Modalità possibili per mitigare o risolvere una Null Session

1. **Aggiornare i sistemi:** sistemi operativi di qualsiasi macchina (switch, firewall, pc etc...) deve tenere il passo con gli aggiornamenti del proprio sistema operativo. Periodicamente vengono rilasciate release o patch che correggono le vulnerabilità o ne potenziano la difesa delle stesse.
2. **Configurazioni di sicurezza:** in particolare quelle relative alle connessioni di rete e disabilitare quelle inerenti alle Null Session. Su un Windows Server > 2003 queste impostazioni sono già disabilitate, ma meglio verificare.
3. **Registro degli eventi:** verificare periodica delle attività delle reti per controllare e individuare eventuali tentativi di Null Session.

4. **Monitoraggio delle attività di rete:** questa attività potrebbe tornare utile per sempre per l'individuazione di attività sospette e di possibili tentativi di sfruttamento di vulnerabilità.

Spiegazione sull'efficacia delle correzioni ed efforts

Ovviamente, oggi giorno, la Null Session è una vulnerabilità molto rara in quanto i sistemi operativi godono di ottime difese, come anche tutti gli altri device presenti in una rete aziendale. Qual ora vi fosse una azienda che avesse dei sistemi oramai deprecati o "obsoleti", sarebbe opportuno aggiornarli (se possibile) oppure sostituirli con sistemi più innovativi e con possibilità di aggiornamenti frequenti. Gli antivirus possono contribuire anche ad una forma di difesa preventiva.