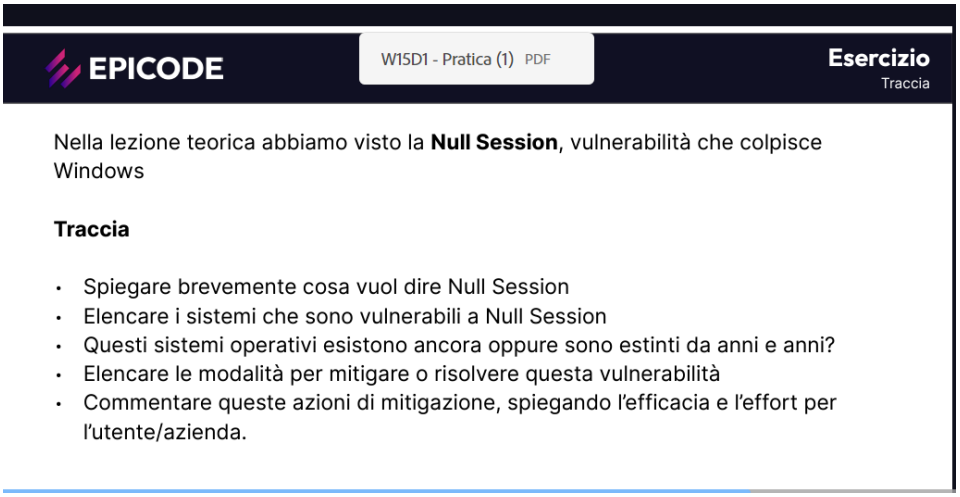
ESERCITAZIONE WEEK 15 DAY 2


EPICODE

W15D1 - Pratica (1) PDF

Esercizio
Traccia

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.

La Null Session è una vulnerabilità che colpisce i sistemi operativi **Windows**, consentendo un accesso non autorizzato alle informazioni di sistema tramite una sessione di rete senza credenziali di autenticazione. Questa vulnerabilità permette a un attaccante di ottenere informazioni sensibili sul sistema, come elenchi di utenti, gruppi, condivisioni di rete e altre risorse.

Gli attacchi *«null session»* si possono utilizzare per recuperare dalla macchina target molte informazioni. Un attaccante, infatti, può riuscire a recuperare informazioni quali:

- Password
- Utenti di un sistema
- Gruppi di un sistema
- Processi in esecuzione
- Programmi aperti

Le «null session» si possono sfruttare da remoto, questo significa che un attaccante può utilizzare il proprio PC per attaccare una macchina Windows vulnerabile. Inoltre, si può utilizzare questo tipo di attacco per eseguire azioni sulla macchina vittima tramite API o RPC (Remote Procedure Call).

Negli anni scorsi, la maggior parte dei sistemi Windows era vulnerabile alle «null session» e gli attacchi di questo tipo hanno avuto un impatto enorme su tutto l'ecosistema Windows. Ad oggi, sono ancora veramente pochi i sistemi vulnerabili, perlopiù sono sistemi legacy. Di per sé gli attacchi null session si basano su una vulnerabilità dell'autenticazione delle share amministrative di Windows, che permettevano ad un attaccante di collegarsi ad una share locale o remote senza autenticazione.

I sistemi operativi vulnerabili alla Null Session includono le versioni più vecchie di Windows, come Windows NT, 2000, XP e 2003. Tuttavia, è importante notare che le versioni più recenti di Windows hanno introdotto miglioramenti nella sicurezza, riducendo la vulnerabilità della Null Session.

Per mitigare o risolvere questa vulnerabilità, è possibile adottare le seguenti misure:

1. Disabilitare la Null Session: Disabilitare completamente le Null Session è un passo fondamentale. Questo può essere fatto mediante la configurazione delle impostazioni di sicurezza del sistema operativo.

2. Applicare le patch di sicurezza: Mantenere il sistema operativo aggiornato con le ultime patch di sicurezza è essenziale per correggere le vulnerabilità note, compresa la Null Session.

3. Utilizzare firewalls: Configurare firewall per filtrare il traffico di rete indesiderato e limitare l'accesso ai servizi solo a host autorizzati.

4. Implementare l'accesso basato sui ruoli: Limitare l'accesso alle risorse in base ai ruoli degli utenti, in modo che solo chi ha bisogno di determinate informazioni possa accedervi.

Commentando queste azioni di mitigazione:

- Disabilitare la Null Session: Questa è un'azione efficace ma richiede un certo sforzo iniziale per la configurazione e la verifica delle impostazioni di sicurezza.
- Applicare le patch di sicurezza: Mantenere il sistema operativo aggiornato è un'azione relativamente semplice, ma richiede una costante attenzione per le nuove patch e il loro tempestivo rilascio.
- Utilizzare firewalls: L'implementazione di firewalls aggiunge un livello di protezione, ma richiede la configurazione accurata per garantire che il traffico indesiderato venga bloccato senza compromettere la connettività legittima.
- Implementare l'accesso basato sui ruoli: Questa misura riduce il rischio fornendo accesso solo a chi ne ha bisogno, ma può richiedere una pianificazione approfondita per definire correttamente i ruoli e le autorizzazioni.

Complessivamente, la combinazione di queste azioni contribuirà significativamente a mitigare la vulnerabilità della Null Session, proteggendo il sistema da accessi non autorizzati e garantendo una migliore sicurezza complessiva del sistema operativo Windows.