## M4 D5

## ESERCIZIO

## GIORNO 2 – NULLSESSION

**Spiegazione Null session:**

La vulnerabilità **Null session** si riferisce a una situazione in cui un utente non autenticato può stabilire una connessione "sessione null" con un sistema operativo Windows o una risorsa di rete condivisa. Questa vulnerabilità può consentire a un potenziale attaccante di ottenere informazioni riservate o effettuare operazioni non autorizzate: password, utenti di un sistema, gruppi di un sistema, processi di esecuzione e programmi aperti.
Le null session si possono sfruttare da remoto.

**Sistemi vulnerabili ad attacchi Null session:**

I seguenti sistemi operativi Windows possono essere vulnerabili a null session: Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista (precedente a Service Pack 1), Windows Server 2008 (precedente a Service Pack 2), Windows 7 (precedente a Service Pack 1) e Windows Server 2008 R2 (precedente a Service Pack 1). Alcuni tra questi sistemi non sono più presenti ma estinti. È importante notare che questa vulnerabilità è stata affrontata e risolta nelle versioni più recenti di Windows, quindi se si utilizza un sistema operativo Windows aggiornato, la vulnerabilità null session non sarà presente.

**Modalità per mitigare o risolvere la vulnerabilità:**

Per mitigare o risolvere la vulnerabilità null session, è possibile adottare le seguenti misure: Applicare gli ultimi aggiornamenti di sicurezza e service pack disponibili per il sistema operativo Windows utilizzato. Questo garantirà che le patch di sicurezza siano state applicate correttamente. Limitare l'accesso alla rete e alle risorse condivise solo agli utenti autorizzati. È possibile utilizzare le impostazioni di sicurezza avanzate per configurare i permessi di accesso appropriati. Utilizzare una solida politica di password per evitare che gli utenti utilizzino password deboli o facili da indovinare. Impostare le autorizzazioni di condivisione e sicurezza corrette per le risorse condivise per limitare l'accesso non autorizzato. Utilizzare un firewall o altri meccanismi di protezione della rete per monitorare e bloccare eventuali tentativi di connessione non autorizzati.

**Azioni di migrazione, efficacia ed effort per utente-azienda:**

Le azioni di migrazione per mitigare la vulnerabilità null session possono richiedere sforzi sia per gli utenti che per le aziende.
Gli utenti potrebbero dover aggiornare o migrare i propri sistemi operativi a versioni più recenti che non siano vulnerabili alla null session. Questo potrebbe richiedere il trasferimento dei dati e la configurazione dei nuovi sistemi.
Per le aziende, la migrazione potrebbe comportare un processo di pianificazione più ampio, che include l'identificazione delle risorse e dei sistemi vulnerabili, la valutazione delle alternative, la pianificazione delle fasi di migrazione e l'esecuzione delle attività di migrazione.
L'efficacia della migrazione dipenderà dalla corretta pianificazione e implementazione delle contromisure. L'azienda dovrebbe anche fornire formazione e supporto agli utenti per agevolare la transizione verso i nuovi sistemi.
In generale, mitigare la vulnerabilità null session è essenziale per garantire la sicurezza delle reti e delle risorse condivise. L'implementazione di soluzioni appropriate ridurrà il rischio di accesso non autorizzato e proteggerà le informazioni sensibili.