ESERCIZIO M4 D5 - 1

NULL SESSION

NULL SESSION: Cos'è?

Una NULL SESSION si verifica quando è possibile accedere ad un sistema senza nome utente o password. Si tratta di una connessione anonima a condivisioni non protette di un sistema Windows; le NULL SESSION consentono agli aggressori di ottenere i dettagli della configurazione dell'host, come i nomi delle condivisioni e gli ID utente di Windows. Questo, a sua volta, consente di modificare alcune parti del registro remoto del sistema.
Una volta che un utente malintenzionato ha effettuato una connessione NetBIOS utilizzando una NULL SESSION a un sistema, può facilmente ottenere un elenco completo di tutti i nomi utente, gruppi, condivisioni, autorizzazioni, criteri, servizi e altro utilizzando l'account utente vuoto. Gli standard SMB e NetBIOS in Windows includono API che restituiscono informazioni su un sistema tramite la porta TCP 139.

Un metodo per connettere tramite una NULL SESSION NetBIOS ad un sistema Windows consiste nell'utilizzare la condivisione nascosta Inter-Process Communication (IPC$). Questa condivisione nascosta è accessibile utilizzando il comando net use.
Il comando "net use" è un comando integrato di Windows che si connette a una condivisione su un altro computer. Le virgolette vuote (" ") indicano che vuoi connetterti senza nome utente e senza password.
Per creare una NULL SESSION NetBIOS su un sistema con l'indirizzo IP 192.168.50.1 con l'account utente anonimo integrato e una password nulla utilizzando il comando net use, la sintassi è la seguente:

```
net use \\192.168.50.1 \IPC$ "" /u: “"
```

Una volta che il comando net use è stato completato con successo, l'aggressore dispone di un canale su cui utilizzare altri strumenti e tecniche di hacking.

NULL SESSION: Sistemi operativi interessati

- WINDOWS 95
- WINDOWS 98
- WINDOWS NT
- WINDOWS ME
- WINDOWS 2000
- WINDOWS XP
- WINDOWS SERVER 2003

Stato attuale dei sistemi operativi:

Le versioni menzionate sopra (Windows NT, Windows 2000, Windows XP, e Windows Server 2003) sono considerate obsolete e non supportate da Microsoft. Questo significa che non ricevono più aggiornamenti di sicurezza e sono considerate a rischio. È importante utilizzare versioni più recenti di Windows per garantire una maggiore sicurezza.

Modalità per mitigare o risolvere la vulnerabilità

Per mitigare la vulnerabilità Null Session, ecco alcune misure che possono essere adottate:

- Aggiornare il sistema operativo: Passare a una versione più recente del sistema operativo Windows, come Windows 10/11 o Windows Server 2016/2019, che hanno corretto la vulnerabilità Null Session.
- Disabilitare l'accesso anonimo: Configurare il sistema in modo da disabilitare l'accesso anonimo, impedendo connessioni Null Session non autorizzate.
- Applicare le corrette autorizzazioni: Assicurarsi che le autorizzazioni di accesso alle risorse di rete siano configurate correttamente, limitando l'accesso solo agli utenti autorizzati.

Commento sulle azioni di mitigazione:

- Efficacia: Aggiornare il sistema operativo e disabilitare l'accesso anonimo sono azioni molto efficaci per mitigare la vulnerabilità Null Session. Passare a una versione più recente del sistema operativo garantisce che gli aggiornamenti di sicurezza siano disponibili, mentre disabilitare l'accesso anonimo riduce il rischio di connessioni non autorizzate.

- Impegno per l'utente/azienda: L'aggiornamento del sistema operativo richiede tempo e risorse per pianificare e implementare correttamente il processo di aggiornamento. Inoltre, disabilitare l'accesso anonimo potrebbe richiedere una revisione delle impostazioni di sicurezza esistenti e la configurazione di autorizzazioni di accesso appropriate. Tuttavia, considerando i rischi associati alla vulnerabilità Null Session, l'impegno necessario per attuare queste azioni è giustificato per garantire la sicurezza delle reti e delle risorse aziendali.