**Report dell'Attacco di Sicurezza su Windows XP Utilizzando Metasploit**

**Introduzione**

In questo report, descrivo in dettaglio il processo che ho seguito per configurare un ambiente di test virtuale, eseguire un attacco sfruttando la vulnerabilità MS08-067 su un sistema Windows XP e testare alcune funzionalità post-sfruttamento tramite Meterpreter. L'obiettivo è quello di ottenere una comprensione pratica di come possono essere sfruttate le vulnerabilità note e come gli strumenti di post-sfruttamento possano essere utilizzati per raccogliere informazioni da un sistema compromesso.

**Installazione e Configurazione di Metasploit**

Metasploit è stato installato sul mio sistema Kali Linux, che utilizzo come stazione di attacco. Ho assicurato che la macchina virtuale e il mio sistema Kali Linux fossero sulla stessa rete isolata per facilitare l'attacco e minimizzare qualsiasi interferenza esterna.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, design

Descrizione generata automaticamente

**Esecuzione dell'Attacco con Metasploit**

Scelta dell'Exploit e Configurazione:

All'interno di Metasploit, ho cercato l'exploit per MS08-067 e ho configurato l'ambiente di attacco specificando l'IP del sistema target (Windows XP) e l'IP del sistema attaccante (Kali Linux). Ho scelto un payload adatto che mi avrebbe permesso di ottenere una sessione Meterpreter sul sistema target.

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Lancio dell'Exploit**

Dopo aver configurato tutti i parametri necessari, ho lanciato l'exploit. Una volta sfruttata la vulnerabilità, sono stato in grado di ottenere una sessione Meterpreter, che mi ha dato il controllo sul sistema Windows XP.

**Operazioni Post-Sfruttamento**

**Cattura di uno Screenshot**

Una delle prime cose che ho fatto dopo aver ottenuto l'accesso è stata la cattura di uno screenshot del desktop del sistema compromesso. Questo è stato realizzato semplicemente con il comando “screenshot” all'interno della sessione Meterpreter, che ha salvato l'immagine localmente sul mio sistema Kali.

Immagine che contiene testo, elettronica, schermata, software

Descrizione generata automaticamente



**Verifica della Presenza di Webcam**

Immagine che contiene testo, schermata, Carattere, nero

Descrizione generata automaticamente

Successivamente, ho tentato di verificare la presenza di una webcam utilizzando il comando “webcam\_list” in Meterpreter. Tuttavia, questo tentativo non ha rilevato alcuna webcam, probabilmente perché la macchina virtuale non era configurata per accedere alla webcam del computer host o perché non erano presenti i driver necessari in Windows XP.

**Conclusione**

Questo esercizio mi ha permesso di apprezzare l'efficacia degli strumenti di attacco moderni contro sistemi vulnerabili e non aggiornati come Windows XP. Inoltre, mi ha fornito un'esperienza pratica significativa nell'uso di Metasploit per sfruttare le vulnerabilità ed eseguire azioni post-sfruttamento.