Pratica S7-L3

Hacking Windows XP

Traccia: Hacking MS08-067

Oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Report

Hacking al servizio SMB di Windows XP con Metasploit

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "SMB" sulla macchina target Windows XP.

INTRODUZIONE

SMB (**Server Message Block)** è un protocollo di rete che fornisce un servizio di condivisione di risorse, come file e stampanti, su una rete locale, consentendo il trasferimento di dati e l'accesso alle risorse condivise.

La **vulnerabilità MS08-067** (Server Service Buffer Overflow) è una vulnerabilità **di stack overflow** del servizio SMB, che può essere sfruttata da un attaccante, tramite invio di richieste SMB al relativo server, per ottenere accesso non autorizzato al sistema bersaglio, con conseguente esecuzione di codice sulla macchina target.

Una vulnerabilità di stack overflow si verifica quando un programma scrive oltre i limiti dello spazio di memoria dedicato allo stack, che è una regione di memoria temporanea utilizzata per l'esecuzione di funzioni e la gestione delle chiamate di ritorno.

La vulnerabilità MS08-067 è causata da un errore nella gestione delle richieste SMB nel servizio Server di Windows.
Un attaccante remoto può inviare una richiesta SMB appositamente creata che causa un overflow dello stack, permettendo all'attaccante di sovrascrivere l'indirizzo di ritorno della funzione e inserire del codice arbitrario che verrà poi eseguito dal sistema.
In termini più semplici, l'overflow dello stack consente a un attaccante di manipolare in modo non autorizzato il flusso di esecuzione del programma, eseguendo così del codice malevolo.

La vulnerabilità è identificata dalla **sigla MS08-067**.
Una volta trovata una vulnerabilità su un sistema proprietario Microsoft, Microsoft stessa rilascia quello che viene chiamato «Security Bulletin», che include una serie di aggiornamenti per risolvere la vulnerabilità trovata, ed assegna una convenzione sui nomi standard, ad esempio appunto MS08-067, dove:

- **MS** = indica Microsoft Security Bulletin
- **08** = l'anno di pubblicazione
- **067** = il numero progressivo del Bulletin pubblicato nel 2008

Un Microsoft Security Bulletin include:

- **Executive summary**: ovvero un riassunto ad alto livello delle integrazioni di sicurezza che vengono apportate al sistema per risolvere la vulnerabilità.
- La **lista dei sistemi impattati** dalla vulnerabilità, come ad esempio Windows XP, Windows Vista, Windows 10 o prodotti Microsoft, ad esempio Word, Excel.
- Dettaglio della vulnerabilità: una **descrizione approfondita** della vulnerabilità con gli impatti sui sistemi e la conseguente **criticità** della vulnerabilità.

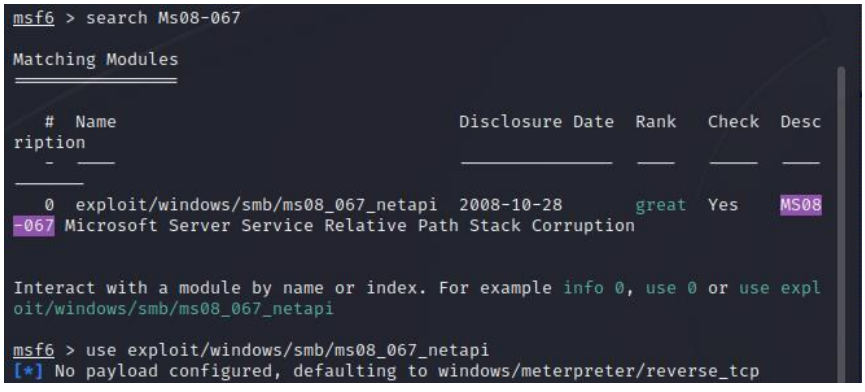
PROCEDURA EXPLOIT

1) Avvio console di Metasploit con comando “msfconsole”

2) individuazione modulo con “search” e configurazione dell’exploit individuato

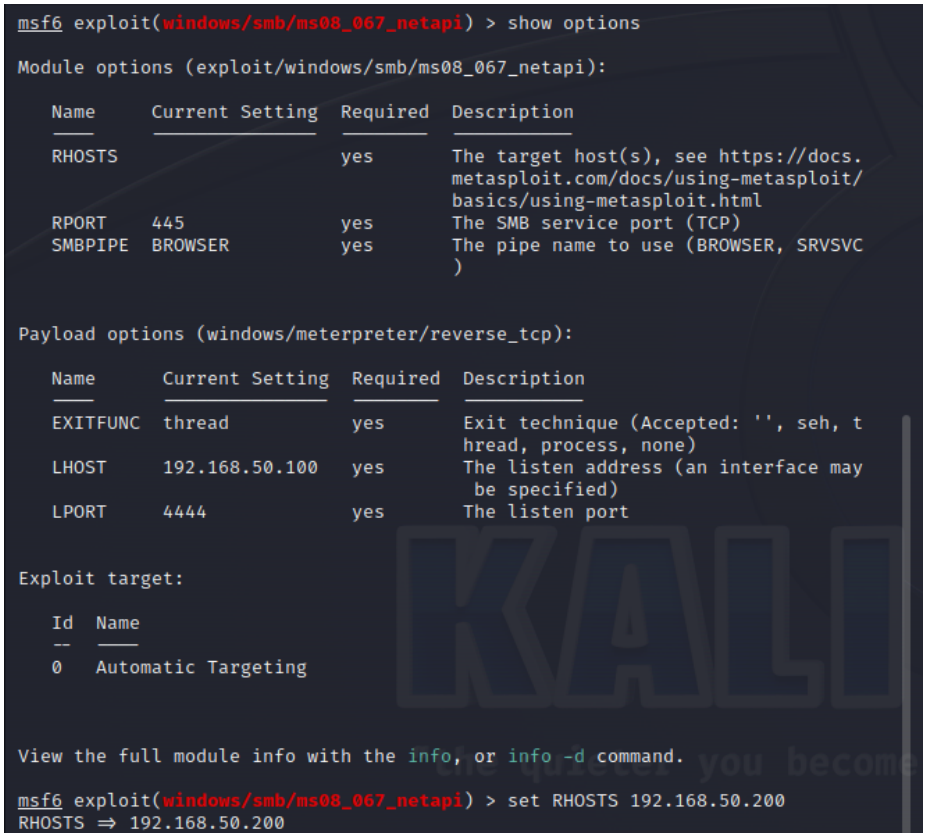
Con il comando “search”, seguito dalla sigla MS08-067, si cerca il modulo contenente l’exploit più adatto**.**
In questo caso è previsto un unico exploit per sfruttare la vulnerabilità MS08-067: **exploit/windows/smb/ms08_067_netapi.**

Per configurare l’exploit si usa il comando **use** seguito dal path dell’exploit



3) Individuazione parametri necessari per utilizzo exploit e inserimento degli stessi

Con il comando **show options,** si controllano quali parametri è necessario (required) configurare per l'esecuzione successiva dell'exploit**.**
In questo caso l'unico parametro required da configurare è **RHOSTS,** ovvero **L'IP** della macchina Target **Windows XP.**
La configurazione si effettua tramite il comando **"set RHOSTS 192.168.50.200".**



4) Lancio exploit e dimostrazione efficacia tramite shell Meterpreter

Il comando **“exploit”** da avvio all’**esecuzione dell’exploit selezionato.**
Questi gli step che costituiscono l’esecuzione dell’attacco**:**

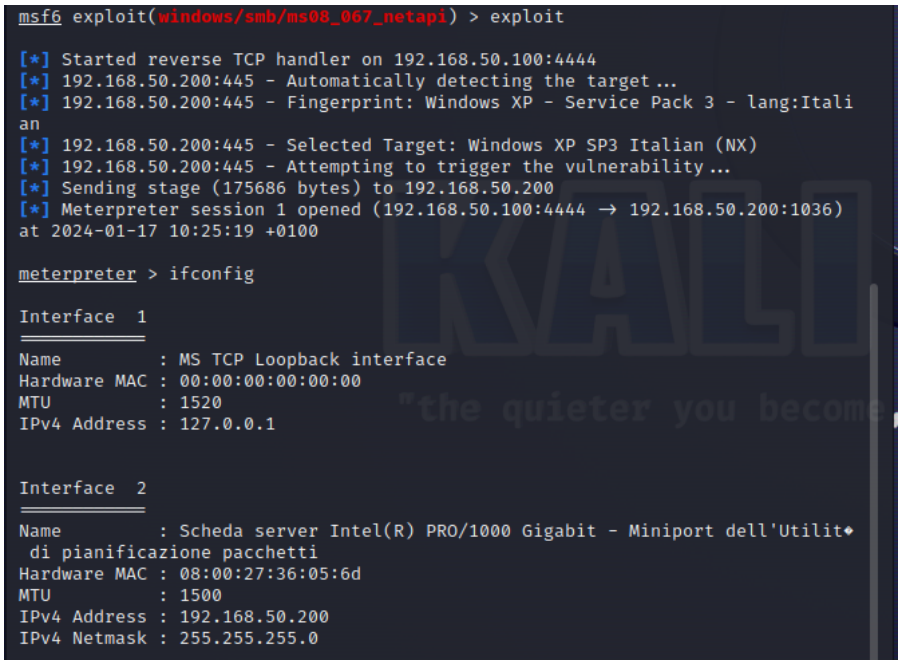
1. Creazione della connessione Reverse TCP:
Metasploit avvia un "handler" in ascolto sulla macchina Kali Linux alla porta di default 4444.

2. Esplorazione e Rilevamento del Target:
Metasploit rileva automaticamente le informazioni della macchina bersaglio, come il sistema operativo, la versione del servizio SMB e altre informazioni rilevanti.

3. Selezione del Target e Trigger della Vulnerabilità:
Basandosi sulle informazioni rilevate, Metasploit seleziona automaticamente il target corretto e avvia il tentativo di sfruttare la vulnerabilità MS08-067, attraverso la manipolazione del traffico SMB.

4. Invio dello Stage (Payload):
Dopo la riuscita identificazione del target, Metasploit invia uno "stage" (payload) alla macchina bersaglio. Questo stage è il codice malevolo che sarà eseguito sulla macchina bersaglio per stabilire la connessione inversa e aprire una sessione Meterpreter.

5. Apertura di una Sessione Meterpreter e dimostrazione efficacia exploit:
L'exploit ha avuto successo in quanto viene aperta una sessione di Meterpreter su Windows XP. che offre, sulla macchina attaccante, una shell per eseguire comandi sulla macchina compromessa. Infatti, tramite il comando ifconfig da terminale di Kali Linux, si ottiene la configurazione di rete di Windows XP.



5) **Tentativo rilevamento webcam di Windows XP, fallito.**

CONCLUSIONI

L'exploit del servizio SMB sulla macchina Windows XP è avvenuto con successo in quanto si è ottenuto l'accesso remoto e non autorizzato al sistema di Windows XP.
Sfruttando la vulnerabilità MS08-067, viene aperta una sessione Meterpreter con la possibilità di eseguire comandi sulla macchina bersaglio.