CS0424IT — ESERCITAZIONE S7L3
EXPLOIT VULNERABILITÀ MS08-067 CON METASPLOIT

Simone La Porta

GitHub

TRACCIA

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).

SERVIZIO SMB

Il protocollo Server Message Block (SMB) è utilizzato per la condivisione di file e stampanti in una rete locale. La vulnerabilità MS08-067 riguarda un'errata gestione delle richieste RPC da parte del servizio di rete di Windows, permettendo l'esecuzione di codice arbitrario da remoto.

METASPLOIT

Metasploit è una piattaforma utilizzata per sviluppare, testare e utilizzare exploit su vulnerabilità conosciute in vari software e sistemi. Metasploit contiene codice di exploit e payload ed altre funzionalità contenute nei suoi moduli. Ogni modulo mette a disposizione un vettore di attacco diverso. È possibile cercare un determinato modulo utilizzando il comando `search`; in questo caso si cerca il modulo `vsftpd` che sfrutta una vulnerabilità nota nel server FTP.

Exploit

Un exploit è un pezzo di software, un frammento di dati o una sequenza di comandi che sfrutta una vulnerabilità in un sistema informatico per causare un comportamento imprevisto o non desiderato. Nel contesto di Metasploit, un exploit è utilizzato per prendere il controllo di una macchina vulnerabile.

Le principali caratteristiche di un exploit includono:

- **Identificazione della vulnerabilità**: gli exploit sono progettati per sfruttare specifiche vulnerabilità nei software o nei sistemi.
- **Esecuzione di comandi**: permettono l'esecuzione di comandi non autorizzati sul sistema target.
- **Accesso non autorizzato**: possono fornire accesso non autorizzato a dati o funzionalità del sistema target.

Payload

Un payload è il codice che viene eseguito sul sistema target una volta che l'exploit ha avuto successo. Il payload può avere vari obiettivi, come aprire una shell di comando, creare una backdoor o raccogliere informazioni sensibili.

Le principali caratteristiche di un payload includono:

- **Tipo di attività**: i payload possono eseguire una varietà di attività, come l'apertura di una shell, il download di file o la raccolta di informazioni.
- **Compatibilità**: devono essere compatibili con l'exploit utilizzato per penetrare nel sistema target.
- **Obiettivo specifico**: sono progettati per raggiungere specifici obiettivi post-exploit.

La vulnerabilità MS08-067

La vulnerabilità MS08-067 è una falla critica di esecuzione di codice remoto nel servizio Server di Microsoft Windows, scoperta nel 2008. Questa vulnerabilità è dovuta a un errore nella gestione delle richieste di procedura remota (RPC) nel servizio di rete di Windows, che permette a un attaccante remoto di eseguire codice arbitrario sul sistema bersaglio inviando richieste RPC appositamente predisposte.

Le caratteristiche principali della vulnerabilità MS08-067 sono:

- **Gravità**: la vulnerabilità è classificata come critica da Microsoft, poiché consente l'esecuzione remota di codice con i privilegi del sistema.
- **Autenticazione**: non è richiesta autenticazione per sfruttare la vulnerabilità, rendendo possibile l'attacco da parte di utenti non autenticati.
- **Impatto**: un attaccante può ottenere il pieno controllo del sistema bersaglio, con la possibilità di eseguire qualsiasi comando, installare programmi, visualizzare, modificare o eliminare dati, e creare nuovi account con pieni diritti utente.
- **Diffusione**: la vulnerabilità ha colpito diverse versioni di Microsoft Windows, tra cui Windows 2000, Windows XP, Windows Server 2003, Windows Vista e Windows Server 2008.
- **Sfruttamento**: il modulo Metasploit `exploit/windows/smb/ms08_067_netapi` sfrutta questa vulnerabilità inviando una richiesta RPC malformata al servizio di rete di Windows, causando un buffer overflow che permette l'esecuzione di codice arbitrario.

A causa della sua gravità, la vulnerabilità MS08-067 è stata sfruttata in diversi attacchi informatici su larga scala, incluso il noto worm Conficker, che si è diffuso rapidamente sfruttando questa falla per infettare milioni di computer in tutto il mondo.

SVOLGIMENTO

Configurazione della rete

Per l'esercizio, è stata configurata una rete virtuale tra una macchina Kali Linux e una macchina Windows XP. Gli indirizzi IP assegnati sono:

- Kali Linux: `192.168.50.100`
- Windows XP: `192.168.50.105`

La configurazione degli indirizzi IP è stata verificata da un test di connettività con il comando `ping`.

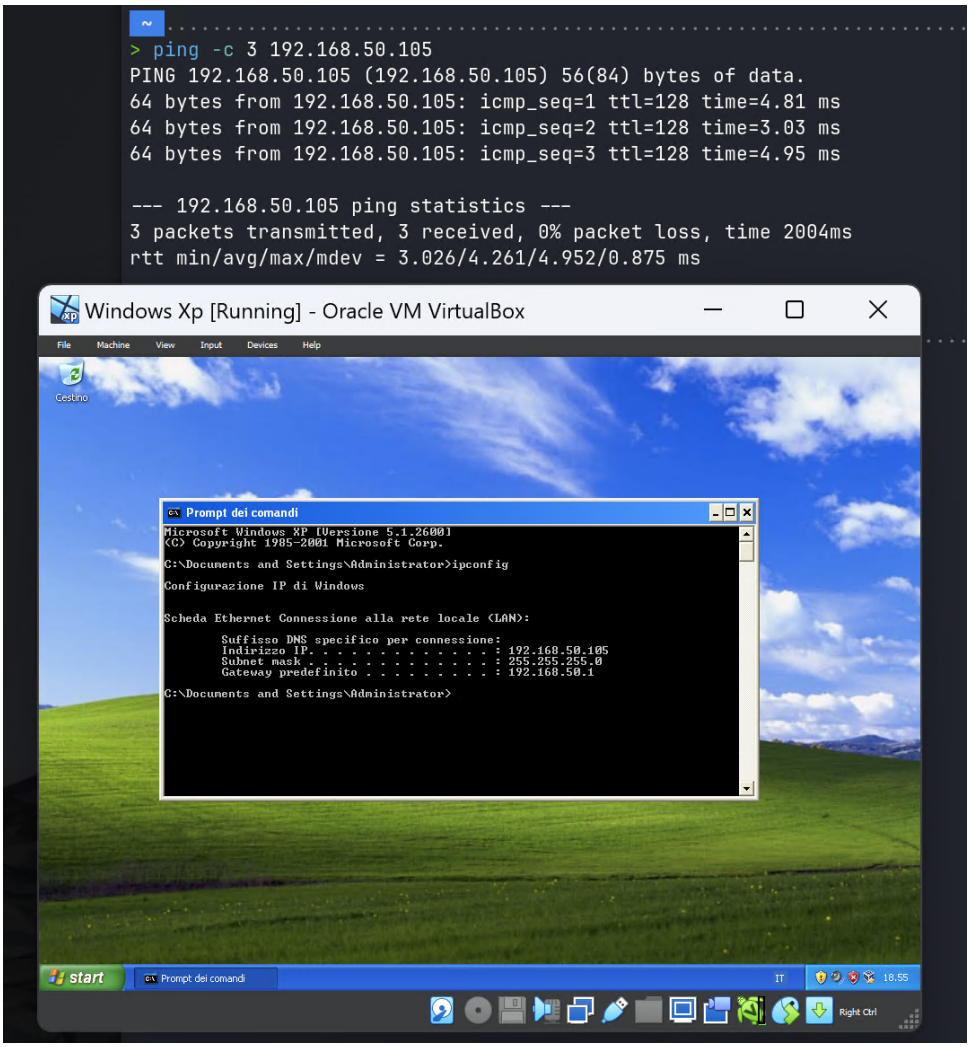

Figura 1: Configurazione IP su Windows XP e test di connettività

Avvio di Metasploit e ricerca/configurazione del modulo

Dopo aver avviato la console di Metasploit con il comando `msfconsole`, è stato cercato il modulo `exploit/windows/smb/ms08_067_netapi` con il comando `search ms08-067`.

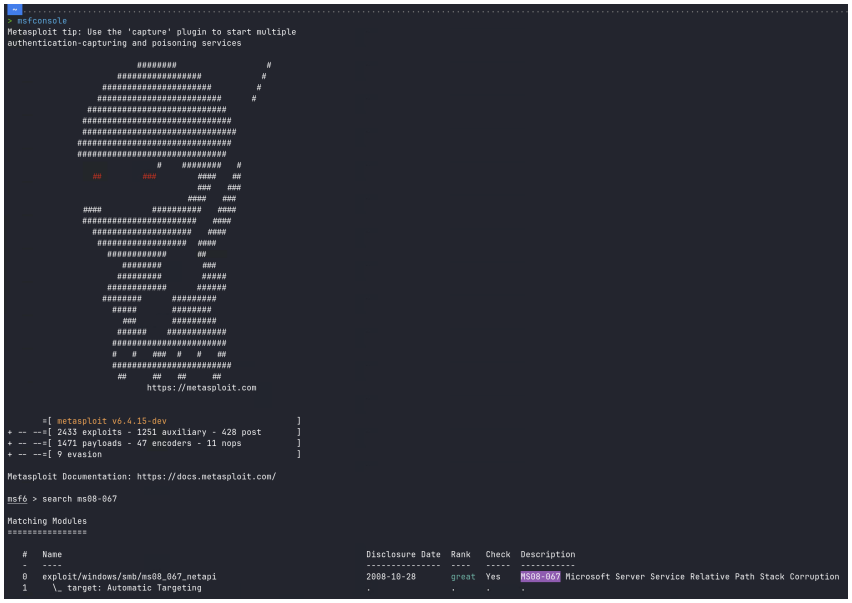

Figura 2: Ricerca del modulo MS08-067

Individuato il modulo corretto, è stato utilizzato con il comando `use 0`. Successivamente, sono state controllate le opzioni necessarie con il comando `show options`, notando che era necessario impostare `RHOSTS` con l'indirizzo target dove è in esecuzione il servizio SMB.

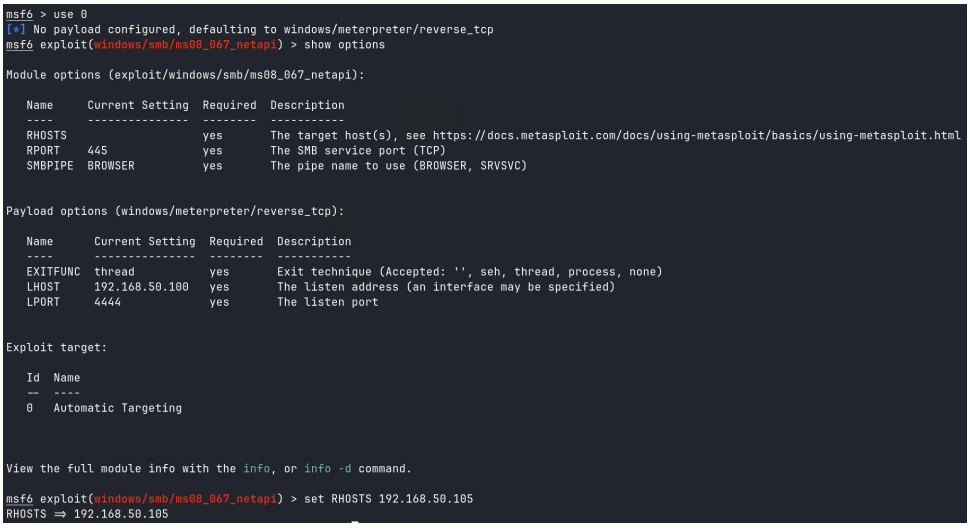

Figura 3: Configurazione del modulo MS08-067

Per configurare il modulo, è stata impostata l'opzione `RHOSTS` con l'indirizzo IP della macchina Windows XP utilizzando il comando `set RHOSTS 192.168.50.105`.

Esecuzione dell'attacco

Non essendo necessario specificare un payload per questo modulo, l'attacco è stato eseguito con il comando `exploit`.

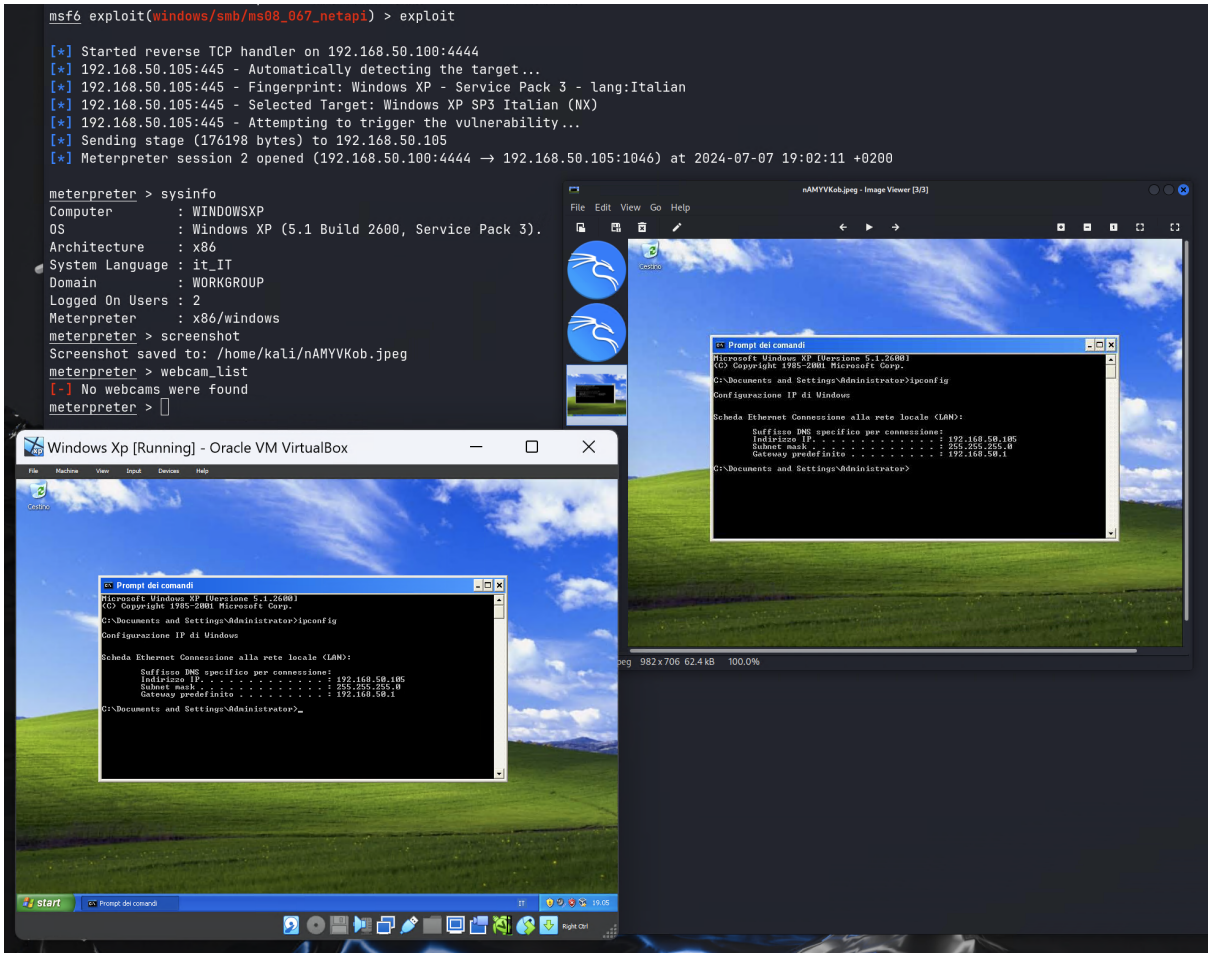

Figura 4: Esecuzione dell'attacco

Il modulo ha avviato con successo una sessione Meterpreter sulla macchina target, confermando che l'attacco ha avuto successo.

Recupero di uno screenshot

Dopo aver confermato che l'attacco è andato a buon fine, è stato eseguito il comando `screenshot` tramite la sessione Meterpreter per catturare uno screenshot della macchina target.

Verifica della presenza di Webcam

Infine, è stato eseguito il comando `webcam_list` per verificare la presenza di webcam sulla macchina Windows XP. Non è stata riscontrata la presenza di webcam.