Pratica S7-L2
Exploit Telnet con Metasploit

Traccia:

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito:

Configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40.
Mettere tutto su un **report**, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Bonus aggiuntivi:

- Exploit smb
- Exploit java_RMI
- Hacking con Windows XP

Report

Hacking del servizio «Telnet» vulnerabile sulla macchina Metasploitable tramite il modulo auxiliary di Metasploit

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "telnet" sulla macchina target Metasploitable.

INTRODUZIONE

- L'**exploit**, nel contesto di un Penetration Testing, è la **fase** nella quale si usa una tecnica o uno strumento, nel nostro caso Metasploit, per sfruttare una vulnerabilità presente sulla macchina target, al fine di ottenere, generalmente, l'accesso non autorizzato ed eseguire azioni non previste sul sistema remoto.
  Da notare che la parola "exploit" si usa anche per riferirsi alla **vera e propria attività svolta per ottenere l'accesso non autorizzato (o più in generale per compiere azioni dannose contro il) al sistema della macchina target**.

- **Metasploit**, strumento per la conduzione dell'attacco riportato, è un framework open source usato, nell'ambito dei PT, per la creazione e l'esecuzione automatizzata degli exploit su sistemi informatici.
  Infatti, fornisce un'ampia gamma di exploit, più di 2000, e quasi 600 payloads nel suo database che possono essere utilizzati per i vari sistemi operativi target (Windows, Linux etc..).
  Metasploit offre **moduli** che contengono varie funzionalità tra le quali codici di Exploit e Payload.
  Ogni modulo mette a disposizione un vettore di attacco diverso.

  Il **payload** è necessario per utilizzare un exploit nella pratica.
  Il termine, nel contesto di Metasploit e degli exploit di un PT, indica un insieme di istruzioni o codice che viene eseguito da un software dannoso o da un exploit dopo che questo ha sfruttato con successo una vulnerabilità del sistema.
  I payload sono progettati per eseguire una serie di azioni dannose, come ottenere l'accesso non autorizzato a un sistema, rubare dati sensibili, danneggiare o bloccare il funzionamento di un sistema o altro ancora.

- **N.B**. Per l'exploit del servizio "telnet" di Metasploitable si è utilizzato un **modulo ausiliario**, **telnet_version**, di Metasploit.
  I moduli ausiliari in Metasploit sono progettati per svolgere funzioni di supporto durante il test della sicurezza, come la scansione della rete, la raccolta di informazioni e altro ancora.
  La differenza, rispetto ai moduli "normali", è che questi moduli non eseguono necessariamente attacchi diretti, ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza del sistema e della rete target.
  Quasi mai utilizzano un payload
  Infatti, il modulo telnet_version **effettua** la **scansione e l'identificazione delle versioni del servizio Telnet** in esecuzione su un sistema remoto e, come si vedrà, non contiene un payload che conduce un attacco diretto al sistema target ma consente di **ottenere informazioni sul sistema target**.

- La **vulnerabilità** che è stata sfruttata è relativa al **servizio "telnet"** di Metasploitable.

Telnet è un protocollo di rete che fornisce un servizio di accesso da remoto a sistemi informatici , garantendo la comunicazione testuale bidirezionale in una rete per mezzo del protocollo TCP (Transmission Control Protocol).
Specificamente, Telnet sfrutta il protocollo di trasporto **TCP**, affidabile e orientato alla connessione, che garantisce una trasmissione e consegna ordinata e senza errori dei dati scambiati tra il client Telnet e il server Telnet.
Il servizio Telnet è in ascolto sulla **porta 23/TCP** per le connessioni in arrivo, stabilite da parte di client Telnet specificando l'indirizzo IP del dispositivo e la porta 23.
In sintesi, Telnet si presenta come un servizio di accesso su sistemi remoti e, simultaneamente, come un protocollo che utilizza il TCP per facilitare la trasmissione di dati testuali tra dispositivi connessi su una rete.
La **vulnerabilità** del protocollo consiste nell'**assenza di meccanismi di cifratura durante la trasmissione dei dati** che rende le informazioni vulnerabili ad attacchi di intercettazione (sniffing della comunicazione) con conseguente furto di informazioni sensibili.

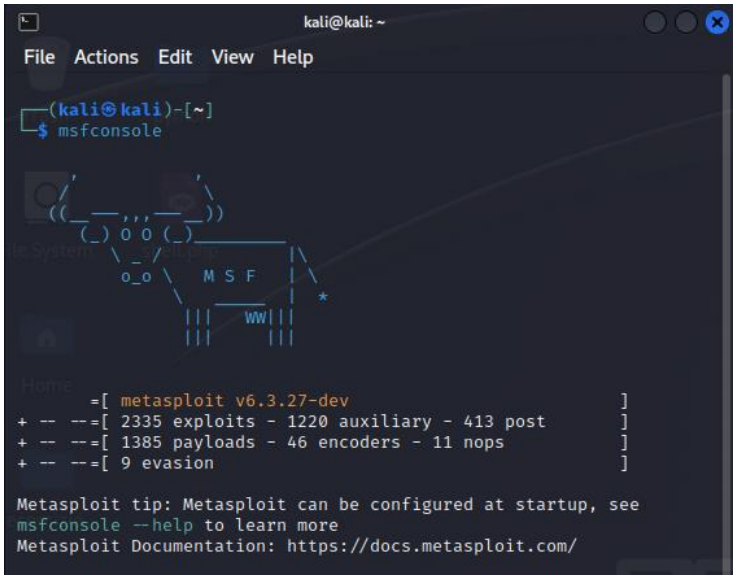
- **Conclusione**: Il presente report conferma che l'exploit è andato a buon fine.

Da terminale di Kali Linux, tramite Metasploit, si è realizzata la connessione con il servizio telnet di Metasploitable riuscendo ad accedere all'interfaccia della macchina e al prompt dei comandi dal quale si sono potuti inviare comandi da remoto, quali l'ifconfig che ha consentito di visualizzare le configurazioni di rete.

PROCEDIMENTO DELL' ATTACCO DA METASPLOIT

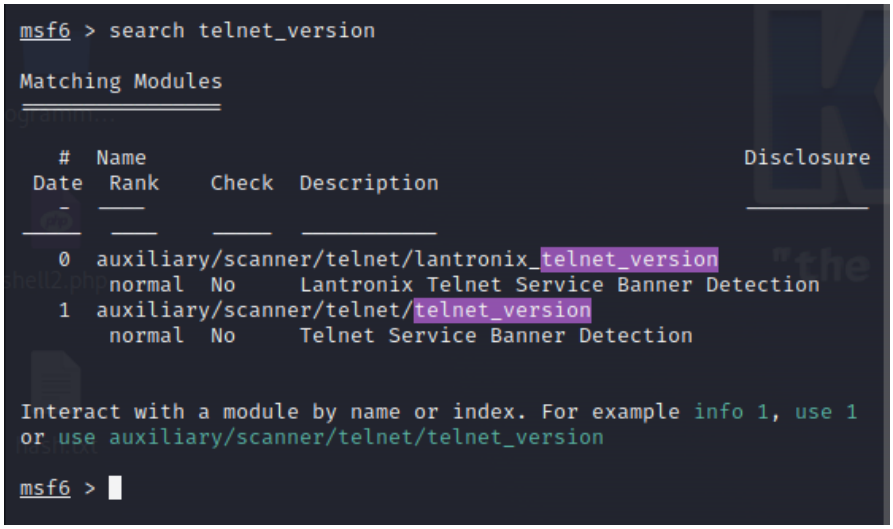
Ipotizziamo di aver effettuato una scansione sul sistema di Metasploitable attraverso nmap e di aver individuato il servizio «telnet» quale servizio che gira sulla macchina Metasploitable

1) **Avvio della console, msfconsole, di Metasploit**



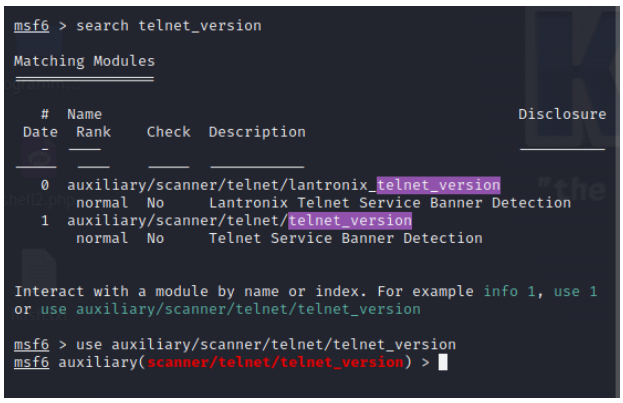
2) **Individuazione del modulo più adatto all'esecuzione dell'exploit con il comando "search"**

Tramite il comando **"search telnet_version"** si cerca e **il modulo ausiliario "auxiliary/scanner/telnet/telnet_version**" che si utilizzerà per l'exploit**.**



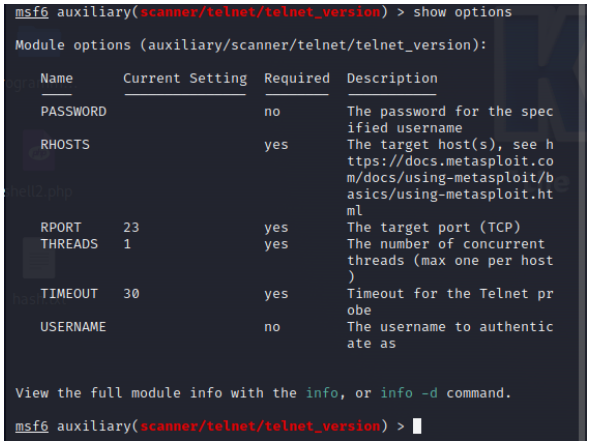
3) **Abilitazione del modulo individuato con il comando “use”**

Con il comando **“use auxiliary/scanner/telnet/telnet_version”** si abilita il modulo scelto per l’esecuzione dell’exploit.
Notare che per utilizzare il modulo, il comando “use” deve essere seguito dal path del modulo.



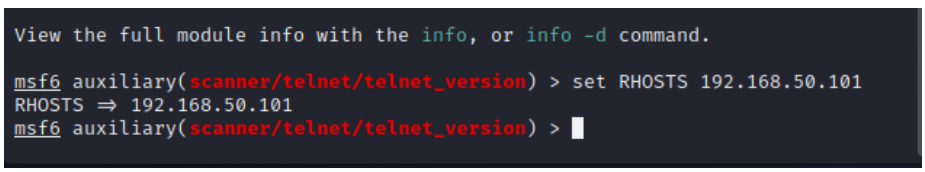
4) **Individuazione dei parametri “required” con il comando “show options”**

Per controllare quali parametri devono essere obbligatoriamente configurati per l’utilizzo del modulo, si usa il comando “show options”**.**
Notiamo che **per il modulo telnet_version è necessario configurare il solo:**
RHOSTS: con **l’IP della macchina Metasploitable** di cui si vuole hackerare il servizio telnet**.**
La porta 23 su cui il servizio telnet è in ascolto è invece prevista di default, come altri parametri**.**



5) **Configurazione dei parametri required con il comando “set”**

Il comando **“set RHOSTS 192.168.50.101**” indica a Metasploit l’ IP della macchina Metasploitable target.



6) “Exploit”, connessione al servizio telnet e Dimostrazione efficacia attacco

Con il comando **“telnet 192.196.50.101”,** Metasploit stabilisce una **connessione con il servizio Telnet** alla porta 23/TCP della macchina Metasploitable specificata con l’indirizzo IP 192.196.50.101**.**
Il modulo **telnet_version, sfruttando il fatto che Telnet trasmette dati in chiaro,** ha recuperato i dati di login del servizio.
Le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».
Con l’inserimento delle stesse si ha accesso al sistema target.

Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «telnet» seguito dall’ip della macchina Metasploitable.

Il servizio ci richiede una login. Proviamo con le informazioni che ci ha restituito Metasploit, quindi username «msfadmin», password «msfadmin» per confermare che l’attacco ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto abbiamo ottenuto accesso non autorizzato alla macchina.

CONCLUSIONI

L'"exploit" con il modulo ausiliario telnet_version di Metasploit è avvenuto con successo, sfruttando la vulnerabilità del servizio telnet che, non prevedendo meccanismi di cifratura durante la connessione, consente al framework Metasploit l'accesso non autorizzato al sistema remoto di Metasploitable.

Si noti che, vista la falla di sicurezza di Telnet, ad oggi si preferisce usare un protocollo più sicuro come SSH per l'accesso da remoto in quanto utilizza la crittografia per la tutela della riservatezza delle informazioni.

Report

Exploit smb con il modulo usermap_script

Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio "telnet" sulla macchina target Metasploitable

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.
Il servizio SMB, in ascolto sulla parta 445 di Metasploitable, è vulnerabile ad attacchi di tipo command execution.
Infatti SMB presenta una vulnerabilità legata ad un parametro di configurazione (mal configurato) che consente ad un attaccante di sfruttarla eseguire comandi non autorizzati sulla macchina bersaglio attraverso la connessione SMB.

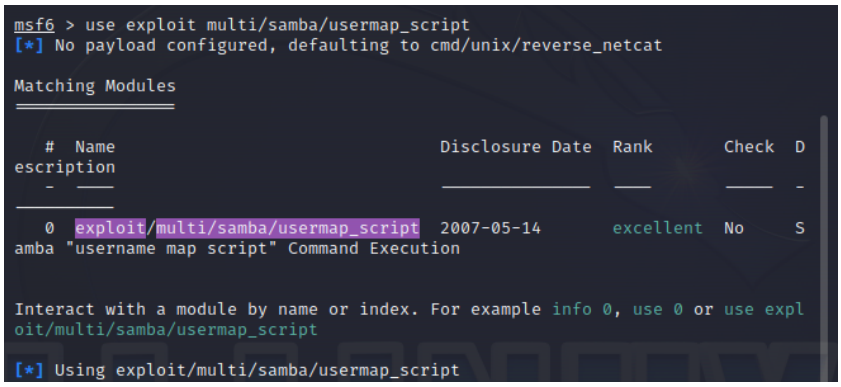
PROCEDURA EXPLOIT CON L'UTILIZZO DEL MODULO USERMAP

1) **Avvio console e ricerca del modulo per l'attacco con "search"**

Il modulo previsto per l'esecuzione dell'attacco al servizio SMB è "**exploit multi/samba/usermap_script**"

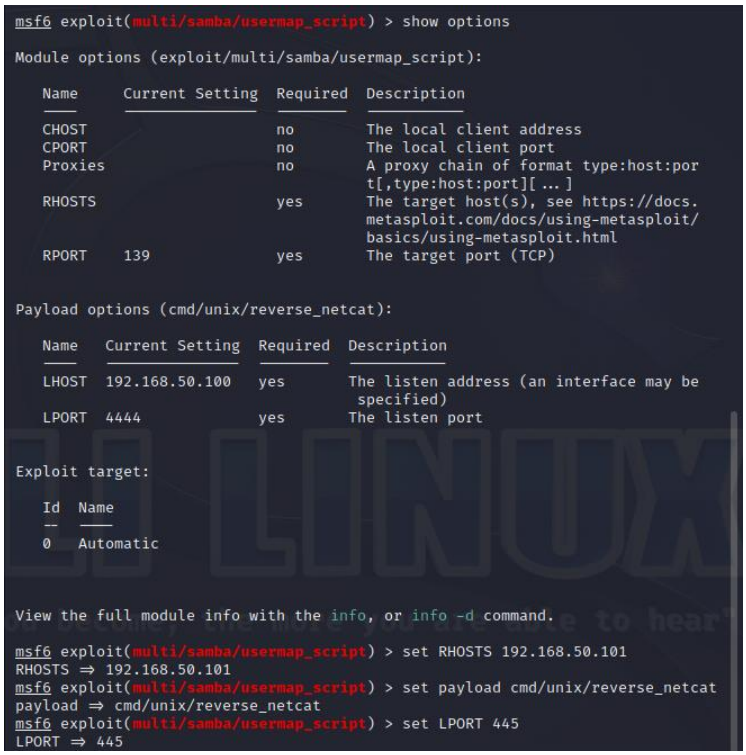
2) Abilitazione dell'exploit individuato con il comando "use"

Con il comando "use exploit multi/samba/usermap_script" si abilita l'exploit.



3) Individuazione e inserimento dei parametri required per l'utilizzo del modulo e abilitazione del payload

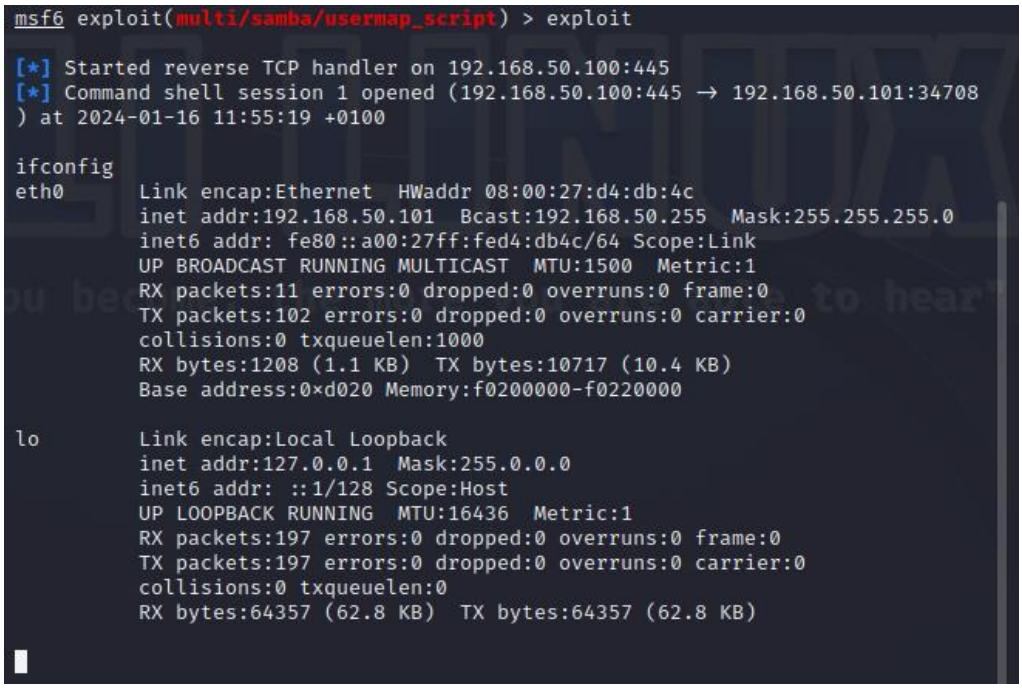
Il comando show options mostra le configurazioni dell'exploit**.**
È necessario settare L' RHOSTS con IP di Metasploitable e il payload previsto di default "payload/cmd/unix/reverse_netcat".



4) Lancio attacco e creazione di una shell reverse Meterpreter su Metasploitable con l'esecuzione del payload

Tramite accesso al sistema remoto, viene creata la reverse Shell di Meterpreter con l'esecuzione del payload.
In questo modo sarà la macchina attaccata a stabilire la connessione con la macchina attaccante.

L'attacco è andato a buon fine perché da remoto riusciamo a vedere la configurazione di rete della macchina Metaspoitable.



Report

Exploit java_RMI code execution

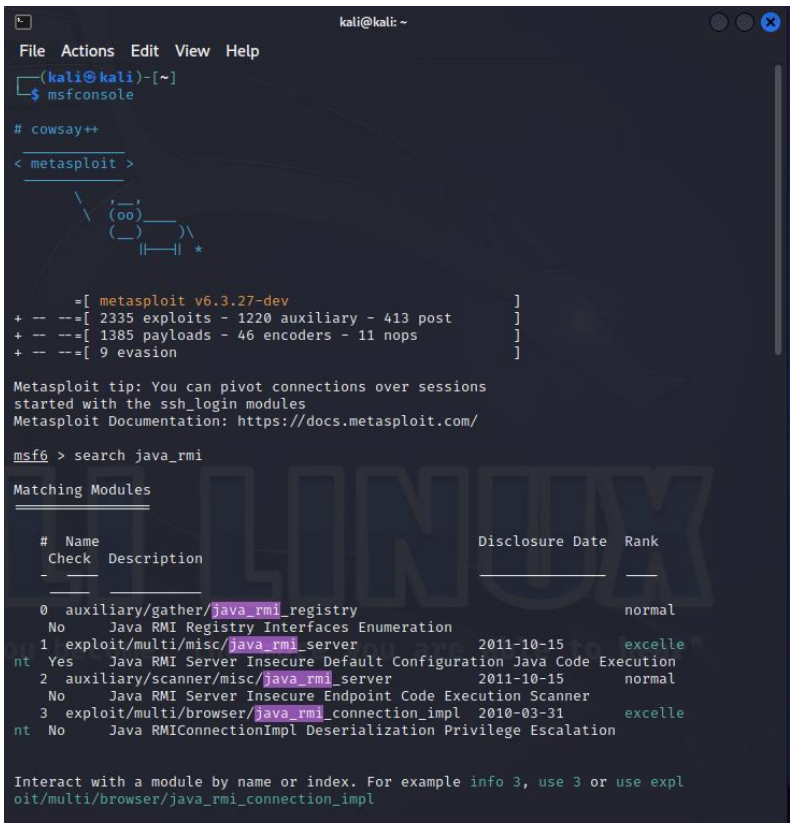
Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al servizio Java-RMI sulla macchina target Metasploitable

Sulla porta 1099 TCP di Metasploitable è attivo un **servizio Java-RMI**, che è una tecnologia che consente a diversi processi Java di comunicare tra di loro attraverso una rete.
La **vulnerabilità** "**java_RMI_code_execution**" è dovuta ad una configurazione di default errata che permette ad un potenziale attaccante di iniettare codice arbitrario per ottenere accesso amministrativo alla macchina target.

PROCEDURA EXPLOIT

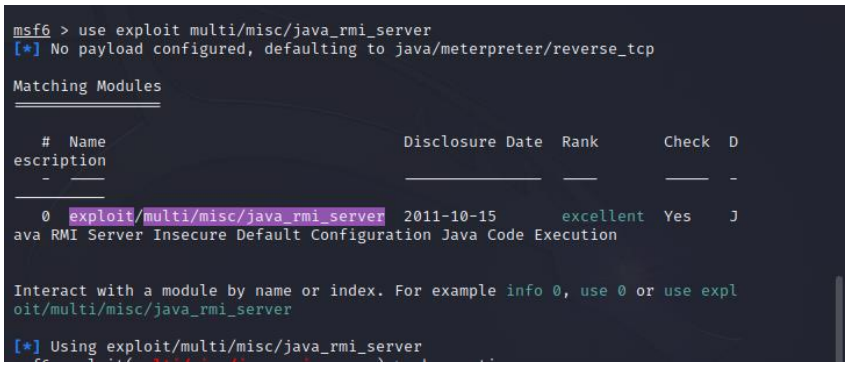
1) Avvio console e individuazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando "**search java_rmi**".
L'exploit scelto è **exploit multi/misc/java_rmi_server.**



2) **Abilitazione dell'exploit individuato con il comando "use"**

Con il comando **"use exploit multi/misc/java_rmi_server" si abilita l'exploit.**



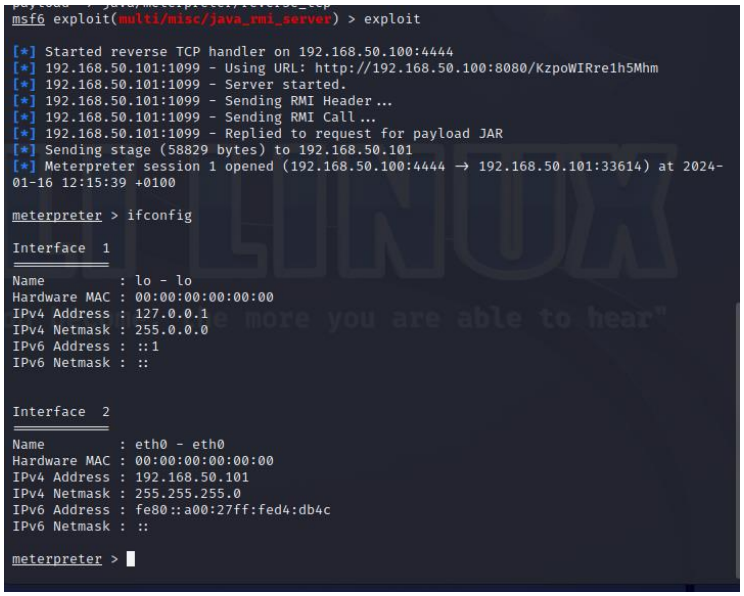
3) **Individuazione e inserimento dei parametri required per l'utilizzo del modulo e abilitazione del payload**

Il comando show options mostra le configurazioni dell'exploit**.**
È necessario settare **L' RHOSTS** con **IP di Metasploitable e il payload** previsto di default **"java/meterpreter/reverse_tcp".**

5) **Lancio attacco e creazione di una shell reverse Meterpreter su Metasploitable con l'esecuzione del payload**

Tramite accesso al sistema remoto, viene creata la reverse Shell di Meterpreter con l'esecuzione del payload.
Meterpreter, un componente di Metasploit, sfrutta Java per stabilire una connessione "reverse TCP" per cui è Metasploitable, la macchina target, stabilisce una connessione in uscita con il sistema controllato da noi, Kali Linux.
Questo è utile quando il sistema bersaglio si trova dietro a un firewall o a un NAT, poiché consente di superare le limitazioni delle connessioni in ingresso.

L'attacco è andato a buon fine perché da remoto tramite una sessione della shell di Meterpreter riusciamo a vedere la configurazione di rete della macchina Metaspoitable con il comando ifconfig.



Report

Hacking al servizio SMB di Windows XP con Metasploit

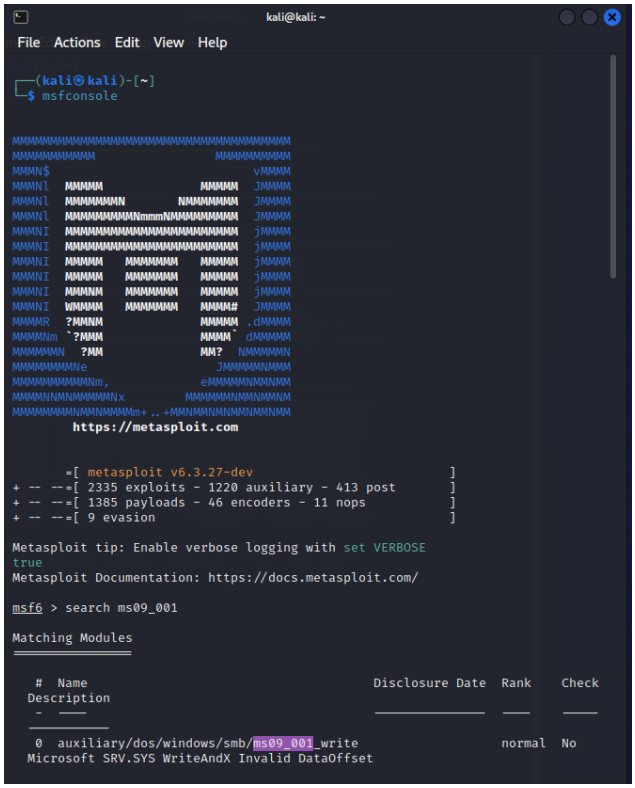
Il seguente report dettaglia l'attacco condotto tramite il framework Metasploit al **servizio SMB**, sfruttando due diverse vulnerabilità, sulla macchina target Metasploitable.

Le **vulnerabilità** "**SMB remote code execution**" e "**SMB code execution**" sono associate al protocollo **SMB** (Server Message Block), utilizzato per la condivisione di file e risorse in una rete locale.
Entrambe le vulnerabilità sono sfruttate per eseguire codice malevolo in remoto al fine di ottenere accesso non autorizzato sul sistema target.
La principale differenza tra le due potrebbe risiedere nella modalità di sfruttamento.
"SMB Remote Code Execution" sottolinea l'esecuzione di codice da remoto, mentre "SMB Code Execution" potrebbe essere più ampio e includere scenari in cui l'attaccante interagisce localmente con risorse SMB per eseguire codice.

PROCEDURA EXPLOIT DOS SFRUTTANDO VULNERABILITA' "SMB remote code execution"

1) Avvio console e individuazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando "**search ms09_001**" si cerca il modulo.
Il modulo ausiliario scelto, "**auxiliary/dos/windows/smb/ms09_001_write, sarà utilizzato per causare un DOS, cioè denial of service sul sistema remoto.**

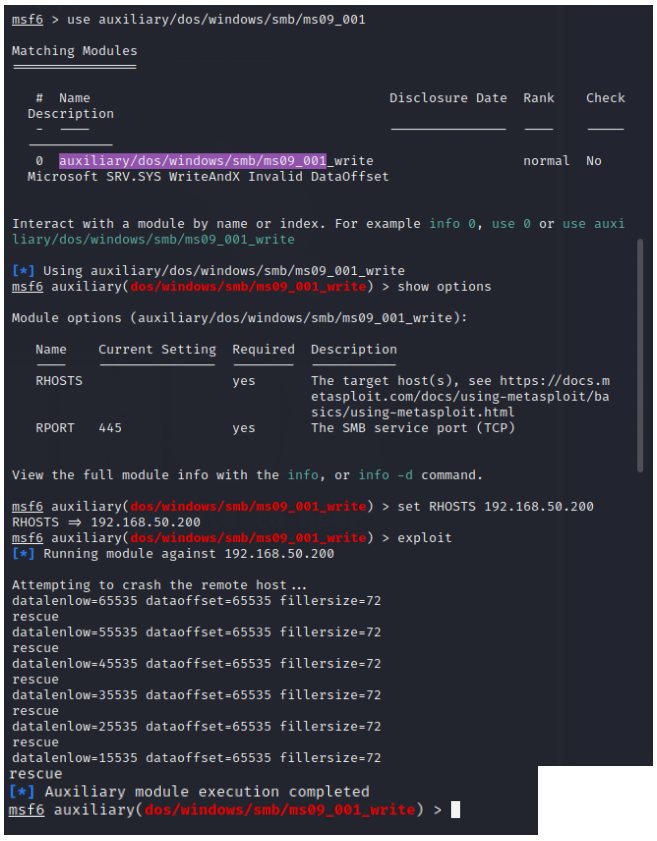


2) **Individuazione Modulo, inserimento dei parametri required, abilitazione del payload e lancio attacco di DOS**

Con il comando **“use auxiliary/dos/windows/smb/ms09_001_write” si abilita il modulo per l’attacco.**
Il comando show options mostra le configurazioni del modulo**.**
È necessario settare **il solo parametro L’ RHOSTS** con **IP di Windows XP.**
Il payload non è previsto nel modulo ausiliario.

Con il comando “exploit”, si fa partire il modulo che inizierà ad inviare pacchetti alla destinazione.
Il modulo «auxiliary» ci permette (in questo caso) di eseguire un attacco DoS sul target, ma di fatto non ottenendo nessuna sessione sul sistema target.

L’attacco va a buon fine se Windows XP da schermata di errore per poi riavviarsi in automatico.
Così non è stato.

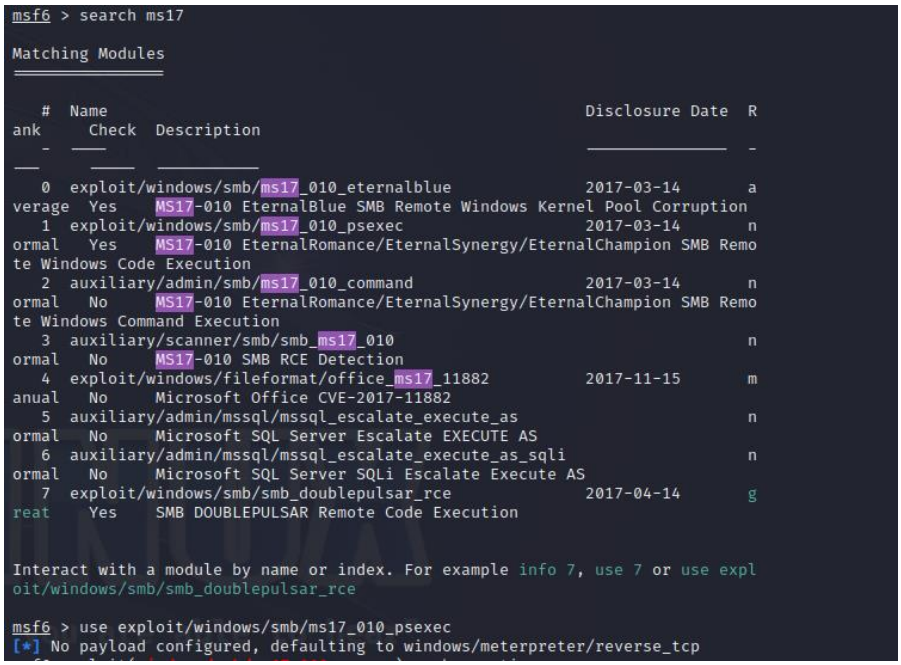


PROCEDURA EXPLOIT DOS SFRUTTANDO VULNERABILITA' "SMB code execution"

1) Avvio console, individuazione e abilitazione del modulo per l'attacco

Dopo l'avvio della console di Metasploit, tramite comando "**search ms17**" si cerca il modulo.
Il modulo ausiliario scelto, "**exploit/windows/smb/ms17_010_psexec".**

Si abilita il modulo per l'esecuzione dell'attacco con il comando **"set exploit/windows/smb/ms17_010_psexec".**



2) Individuazione dei parametri required per l'utilizzo del modulo con il comando "show options"

L'unico parametro necessario per l'attacco è **RHOSTS**, ovvero IP macchina target.

Vediamo anche che il **payload** previsto di default dal modulo scelto è "**windows/meterpreter/reverse_tcp**""

3) Impostazione Parametro modulo e lancio attacco

Una volta settato l'IP di Windows XP, si procede direttamente a lanciare l'attacco che, una volta ottenuto l'accesso al sistema remoto di Metasploitable, esegue il payload, il quale apre una sessione della shell Meterpreter attraverso una connessione reverse_tcp (è la macchina attaccata che stabilisce la connessione con la macchina attaccante).

L'attacco è andato a buon fine perché tramite comando da Kali Linux otteniamo la configurazione di rete di Metasploitable.