Informe Tecnico

Room Ice

5 de Mayo del 2020

Indice

1. Antecendentes

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

Figura 1: Detalles de la maquina

2. Objetivos

Conocer el estado de seguridad actual del servidor **Ice**, enumerando posibles vectores de explotacion y determinando el alcance e impacto que un atacante podria ocasionar sobre el sistema en produccion.

2.1. Consideraciones

Una vez finalizadas las jornadas de auditoria, se llevara a cabo una fase de saneamientos y buenas practicas con el objetivo de securizar el servidor y evitar ser victimas de un futuro ataque en base a los vectores explotados.

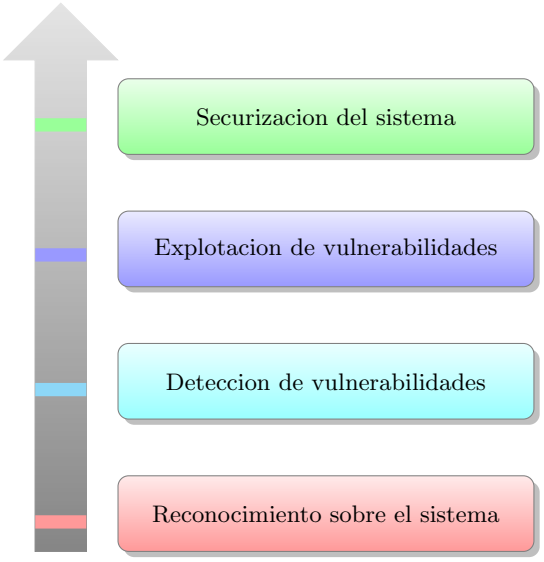

Figura 2: Flujo de trabajo

3. Analisis de vulnerabilidades

3.1. 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 10.10.157.153 (10.10.157.153) 56(84) bytes of data.
64 bytes from 10.10.157.153: icmp_seq=1 ttl=127 time=227 ms

--- 10.10.157.153 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 226.915/226.915/226.915/0.000 ms
```

3.2. Reconocimento por Servicios

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

```
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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
8000/tcp  open  http         Icecast streaming media server
|_http-title: Site doesn't have a title (text/html).
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: DARK-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

3.3. Reconocimento Especifico

Al ser uno de los servicios mas usados siempre es conveniente para el atacante mostrar las vulnerabilidades que puede o no puede tener este servicio.

```
8000/tcp  open  http-alt
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
```

3.4. Vulnerabilidades

Para tener una amplia cantidad de servicios que atacar analizo las vulnerabilidades con el script de la herramienta **nmap**

```
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
```

4. Explotacion

4.1. Metodo 1

4.2. Metodo 2

4.3. Metodo 3

5. Post-Explotacion

5.1. Escala de Privilegios

5.2. Persistencia

6. Soluciones

6.1. Actividades Post Pentest