Write Up – Máquina Bizness

Entorno

Nombre: Crafty

Dificultad: Easy

Sistema Operativo: Windows

Target: 10.10.11.249

Plataforma: Hack The Box

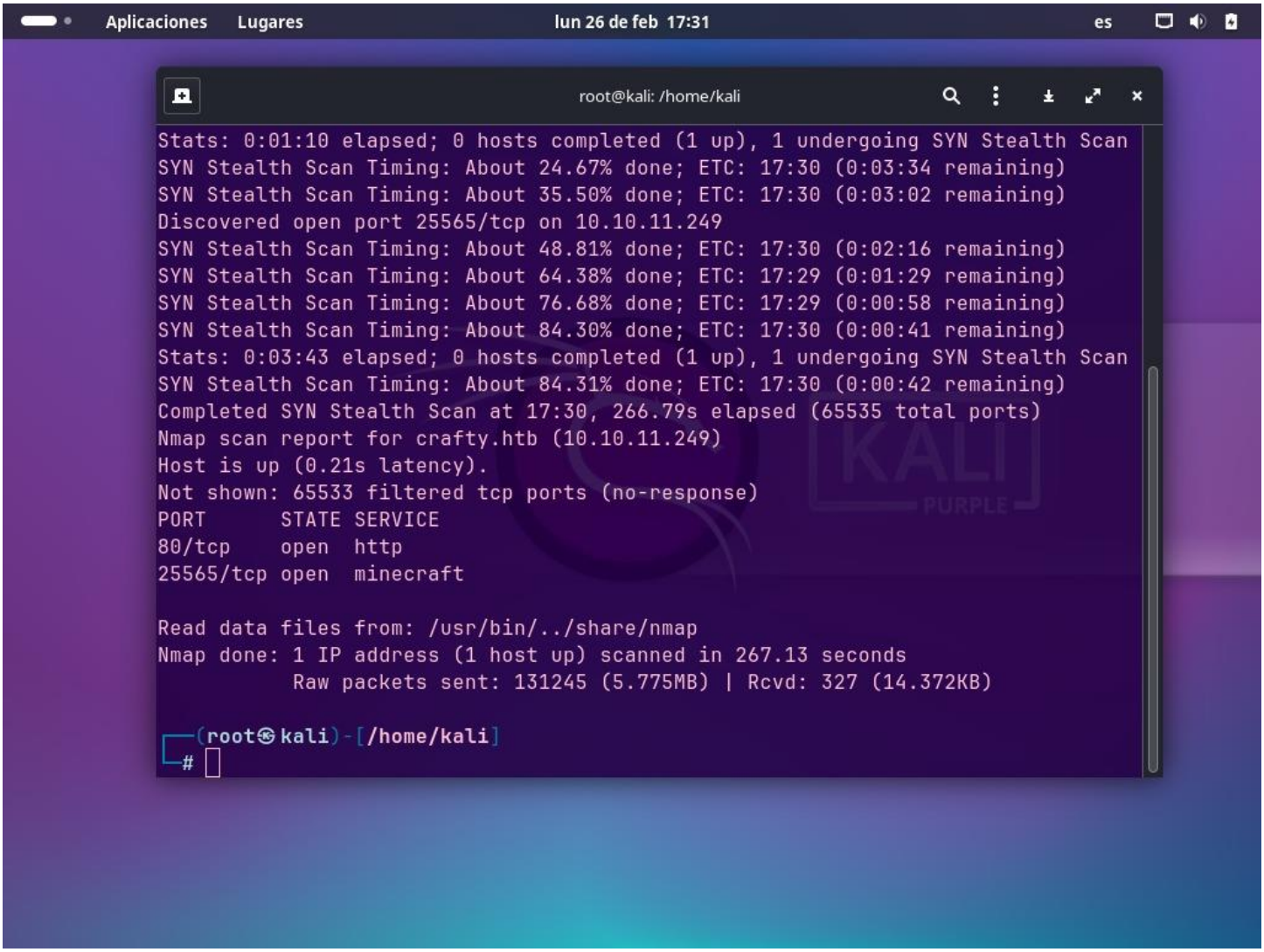
Autora: Ingrid K.

Índice

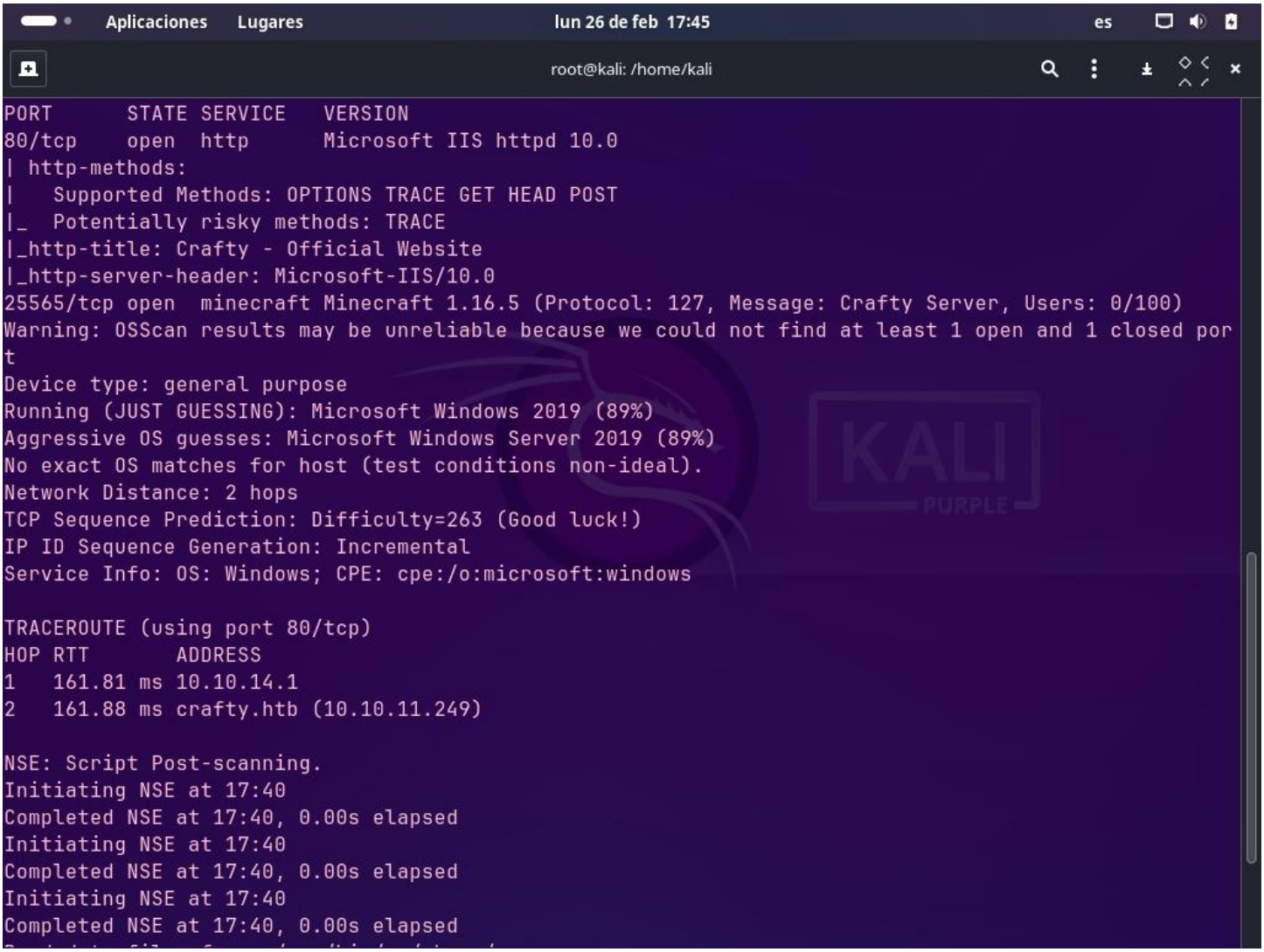
1. Reconocimiento
2. Identificación de la vulnerabilidad
3. Explotación
4. Escalada de privilegios
5. Obtención de Shell de Administrador
6. Resumen final

1. Reconocimiento

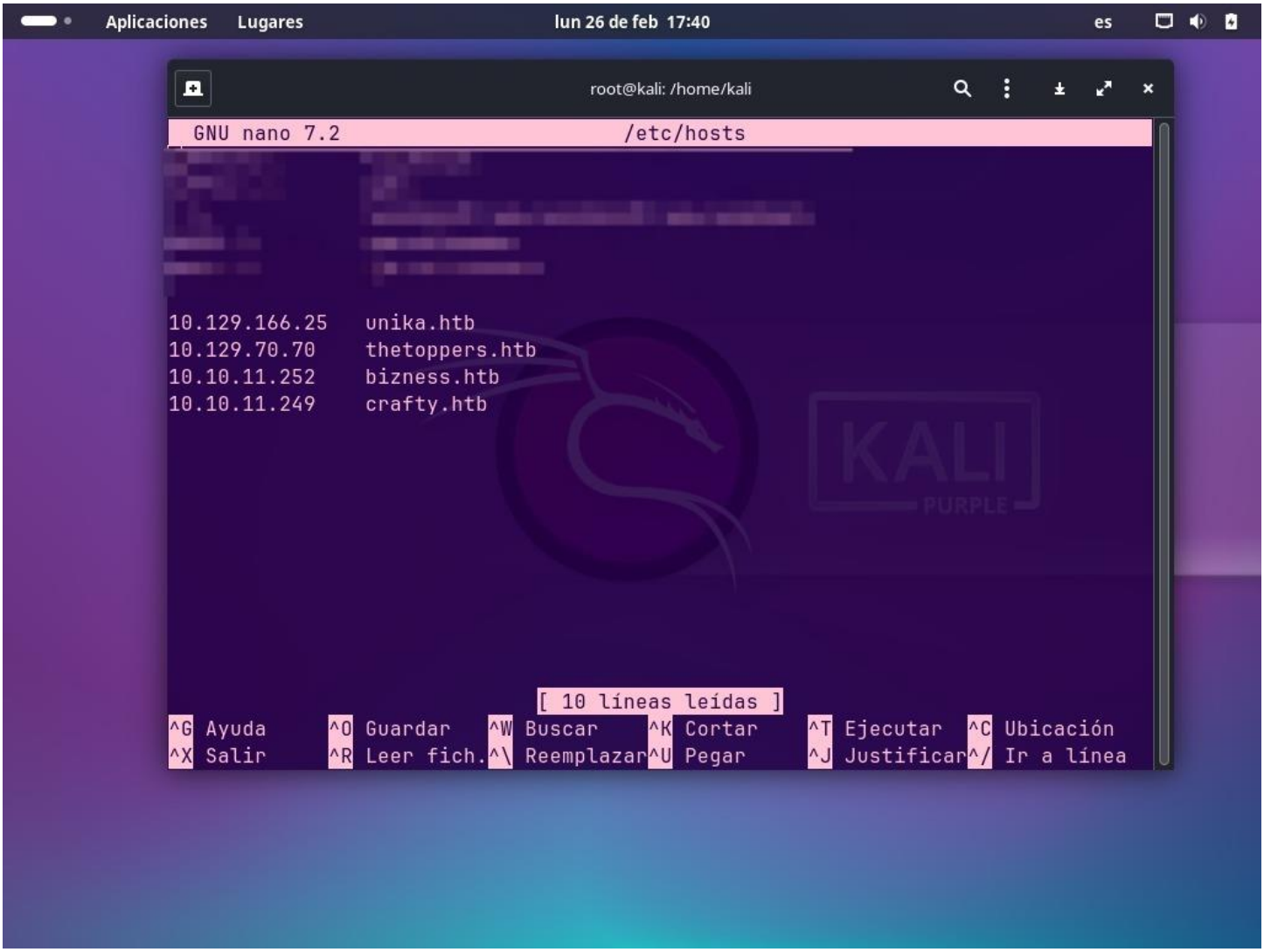
Se realizó un primer escaneo con Nmap que reveló dos puertos clave



Posteriormente, mediante un segundo escaneo, se identificó el servicio en el puerto 25565, utilizado por Minecraft



Para acceder correctamente a la web, se agregó la IP al archivo



2. Identificación de la vulnerabilidad

El servicio en 25565 ejecutaba una versión vulnerable al exploit Log4Shell:

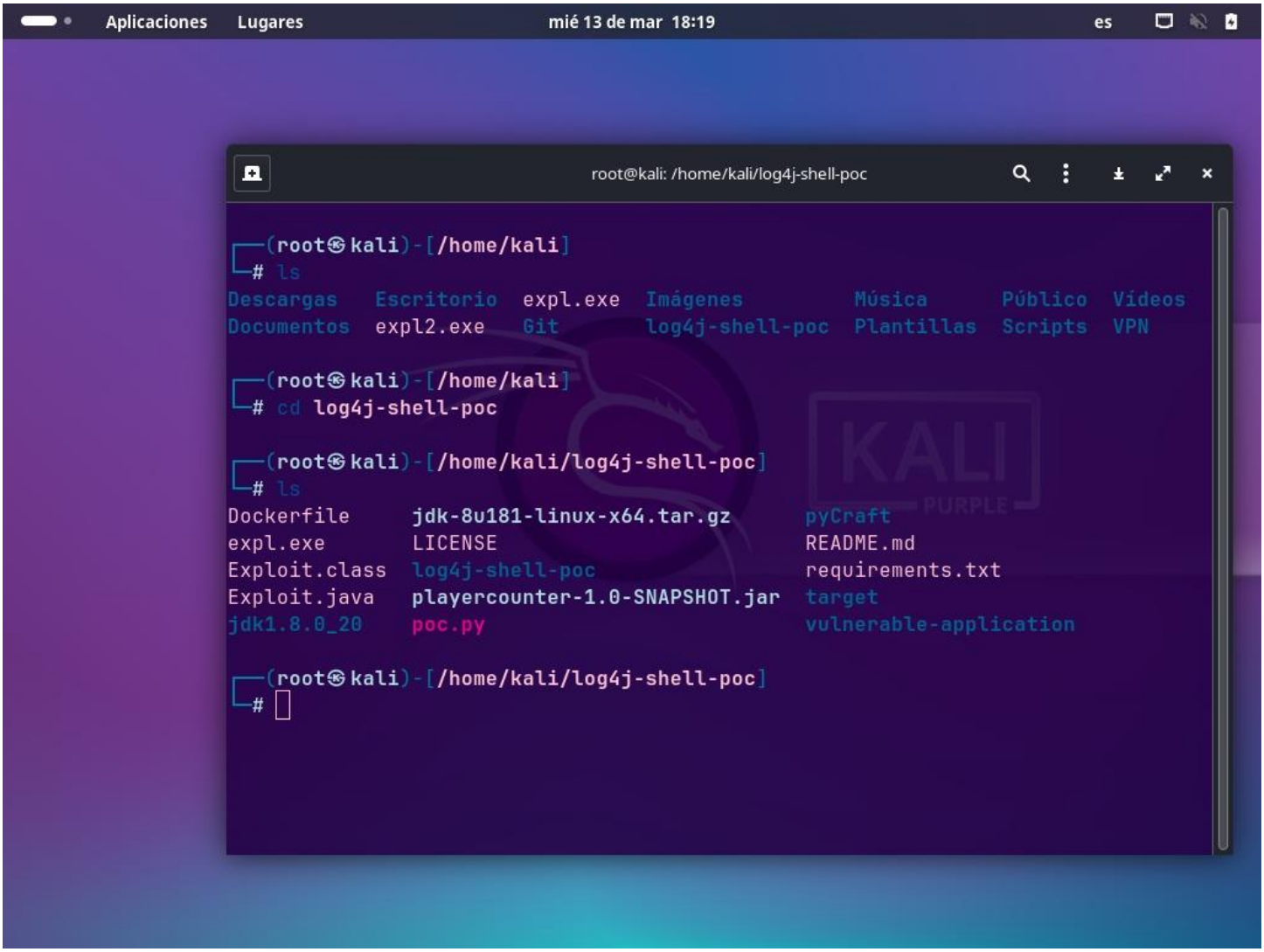
- CVE-2021-44228: ejecución remota de código (RCE) enviando cadenas manipuladas
- Permite cargar código malicioso desde un servidor LDAP del atacante

3. Explotación

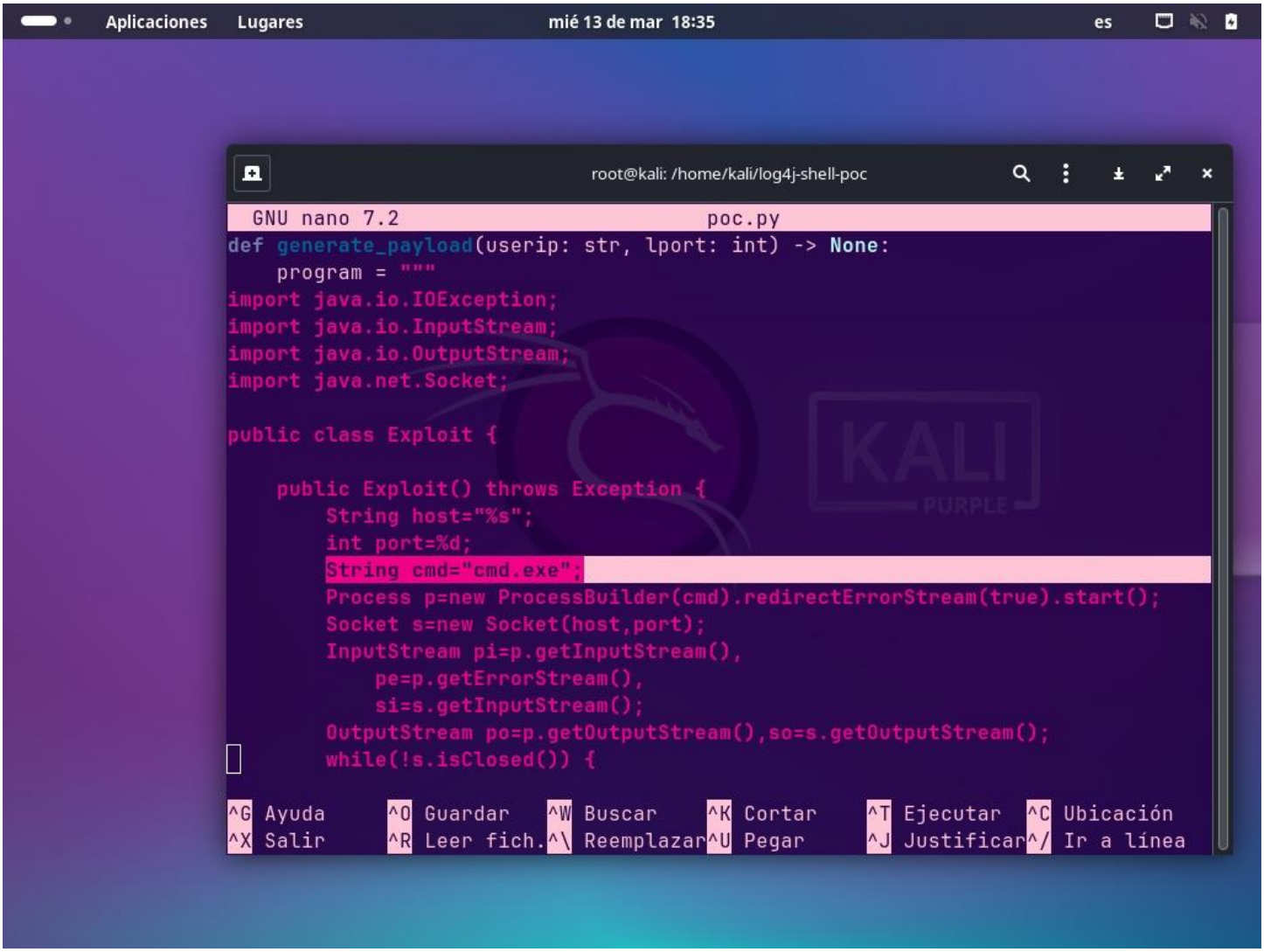
Se utilizó el exploit PoC de https://github.com/kozmer/log4j-shell-poc

Pasos clave:

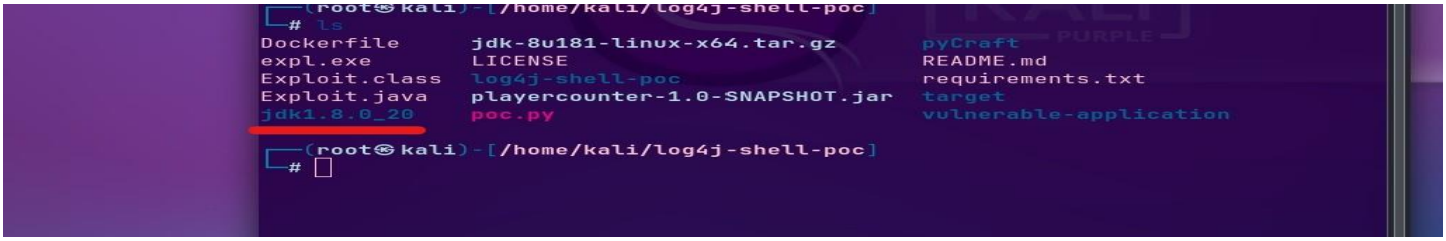
1. Clonar el repositorio del exploit



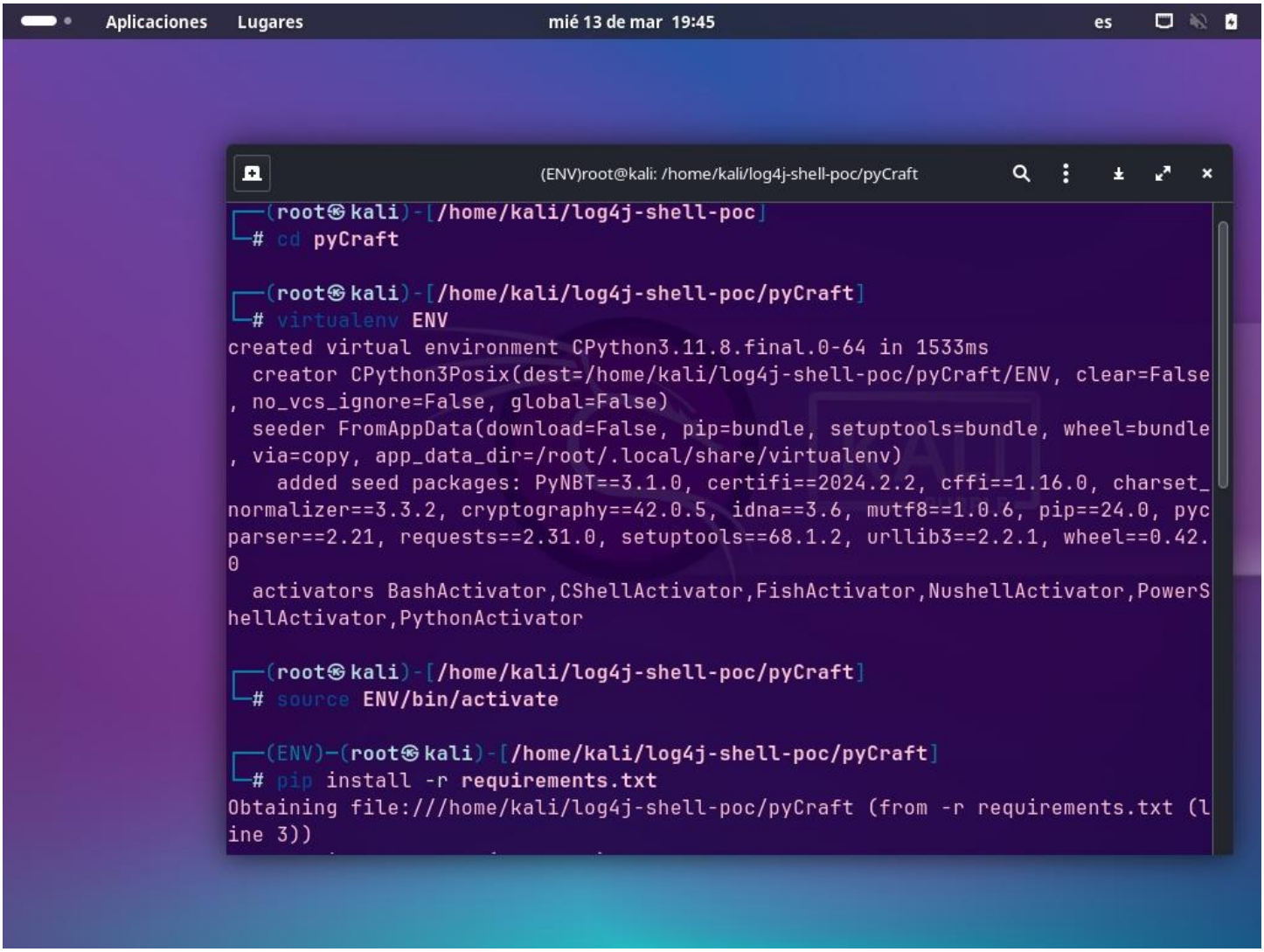
2. Modificar la salida del exploit para generar cmd.exe (Windows)



3. Descargar y configurar temporalmente JDK 8u181 (requerido por el exploit)

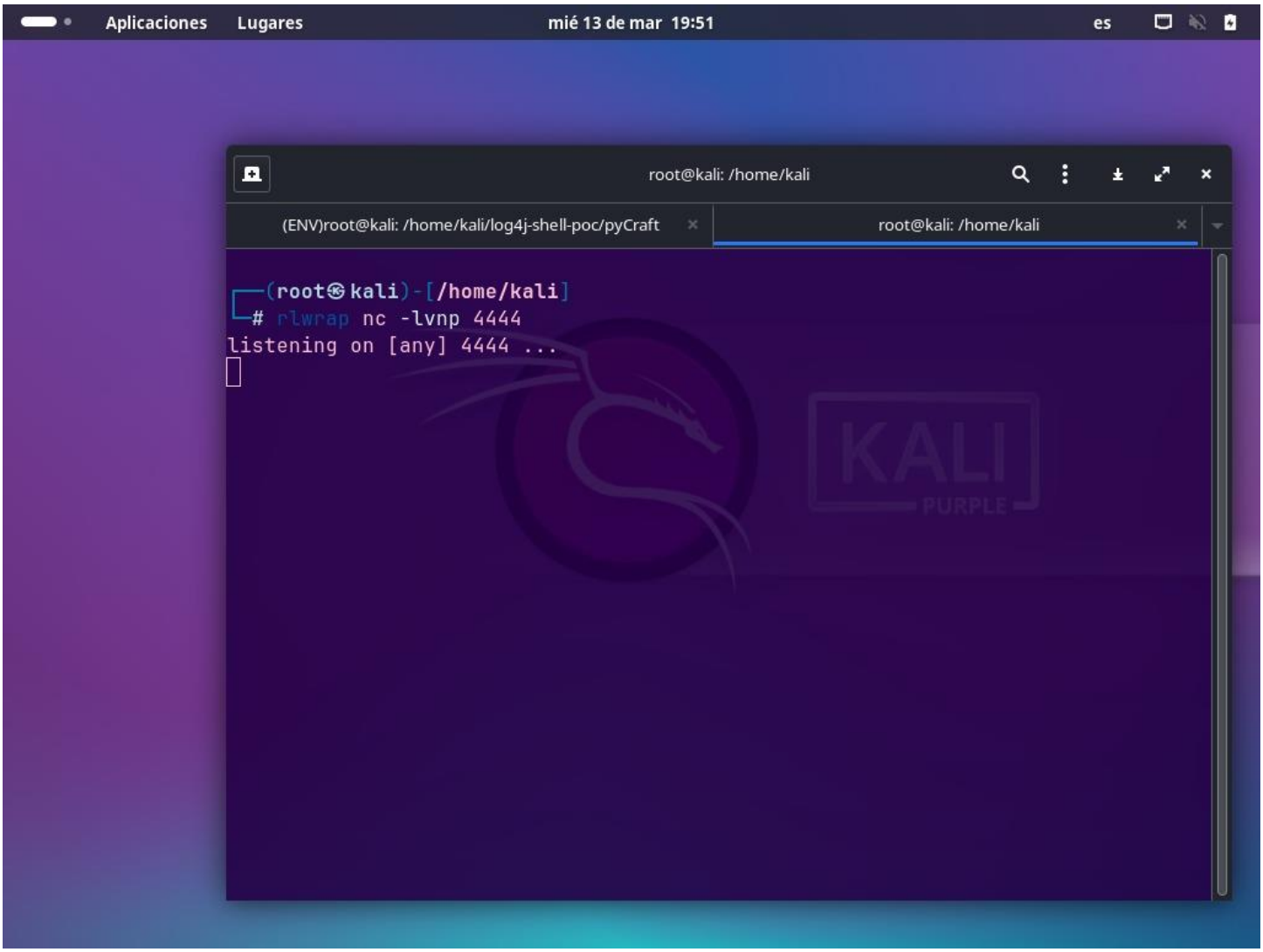


4. Descargar e instalar pyCraft, necesaria para enviar mensajes al servidor Minecraft

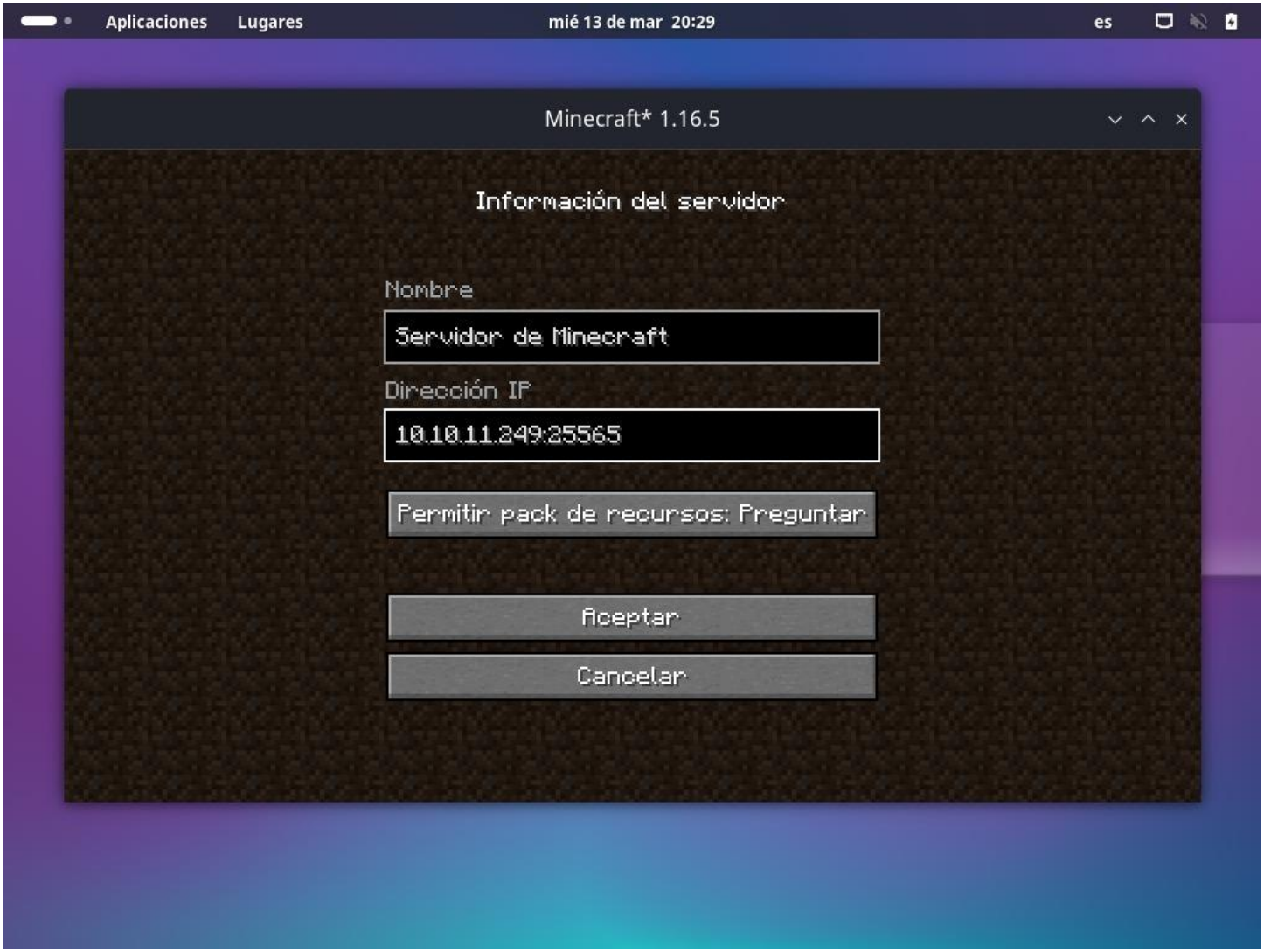


5. Configurar:

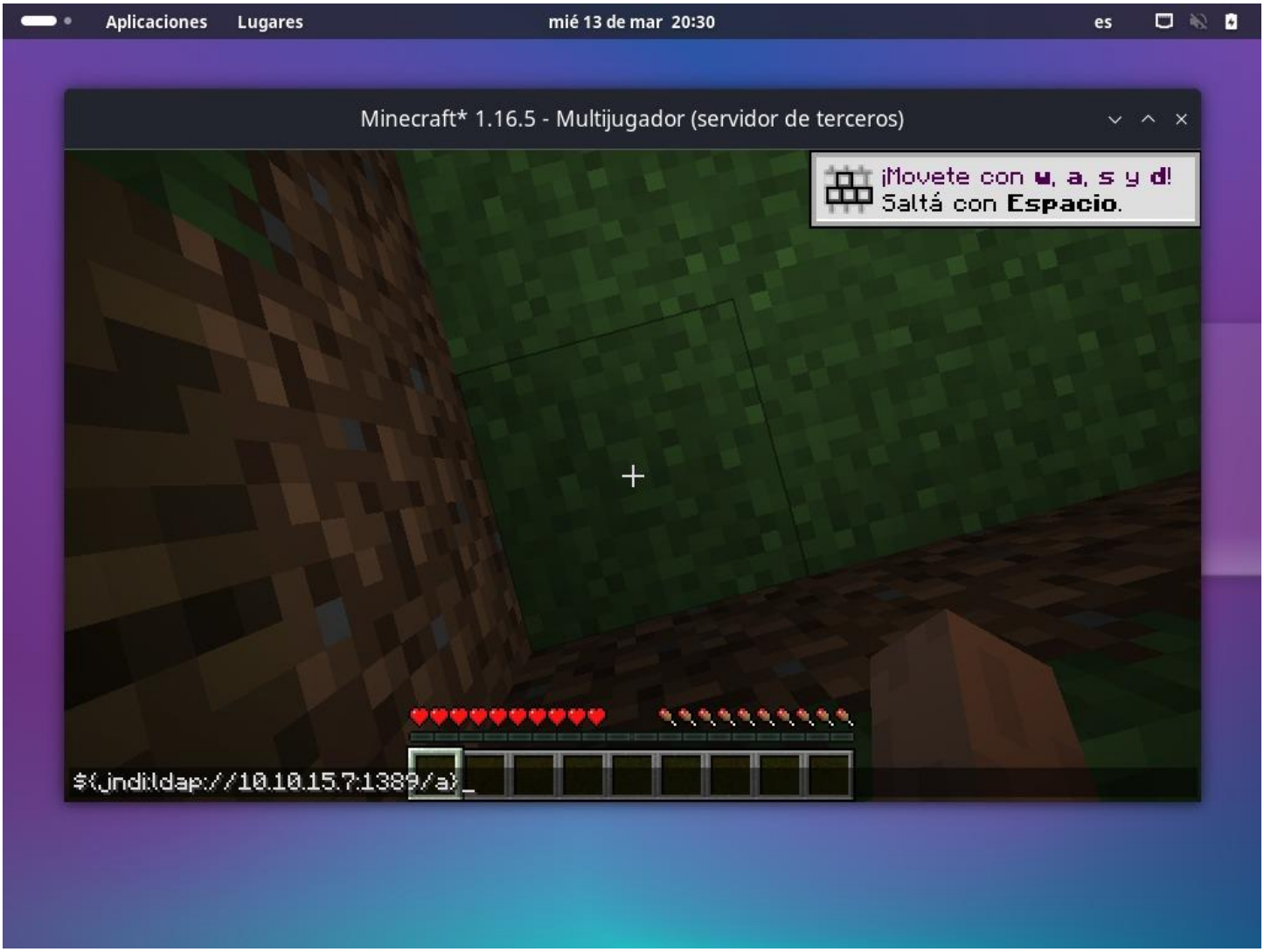
- Servidor LDAP
- Listener (nc -lvnp 4444)



6. Ingresar al servidor Minecraft usando TLauncher, versión 1.16.5 (vulnerable)

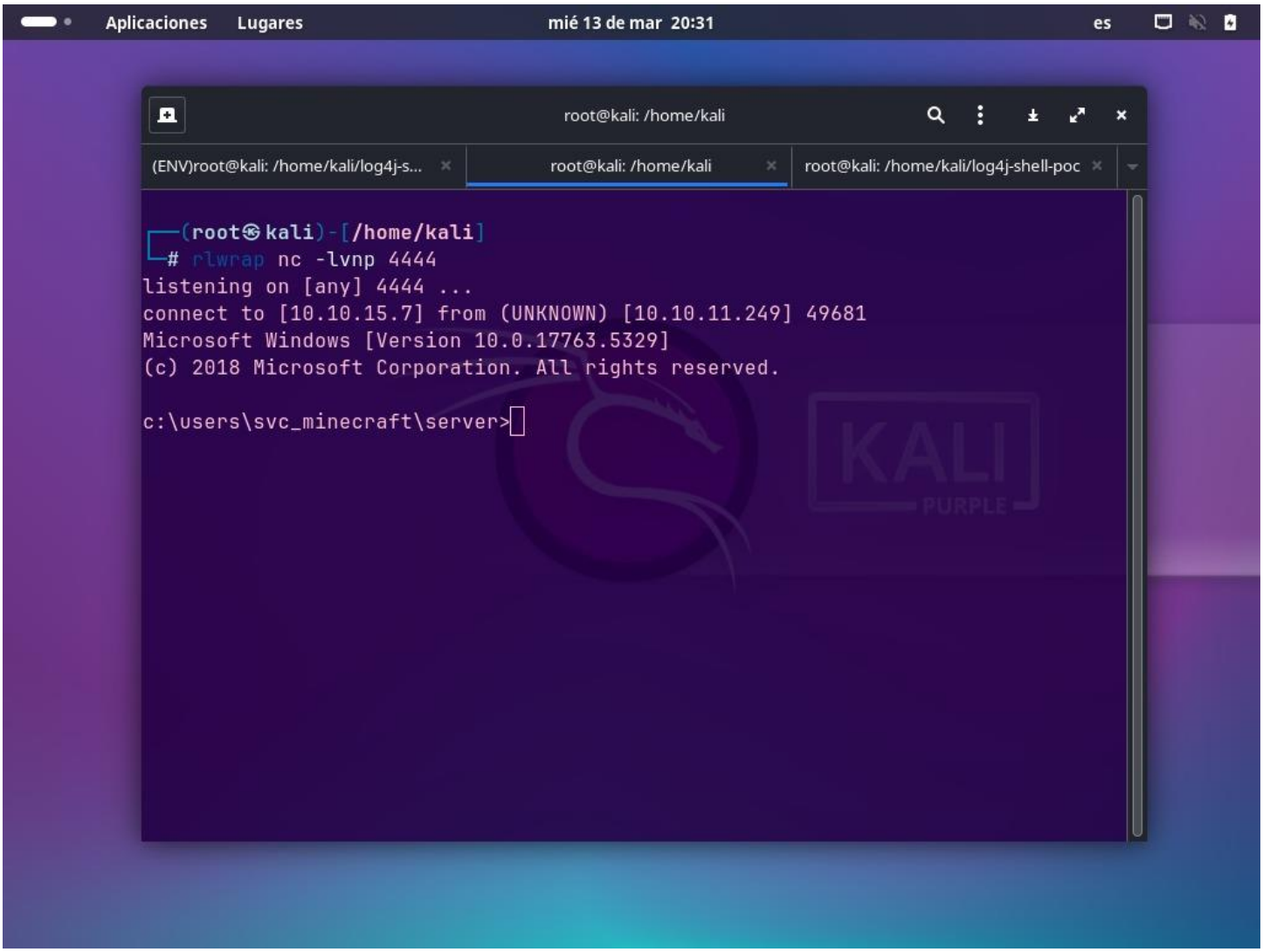


7. Enviar la cadena maliciosa vía chat (inyecta la carga JNDI)

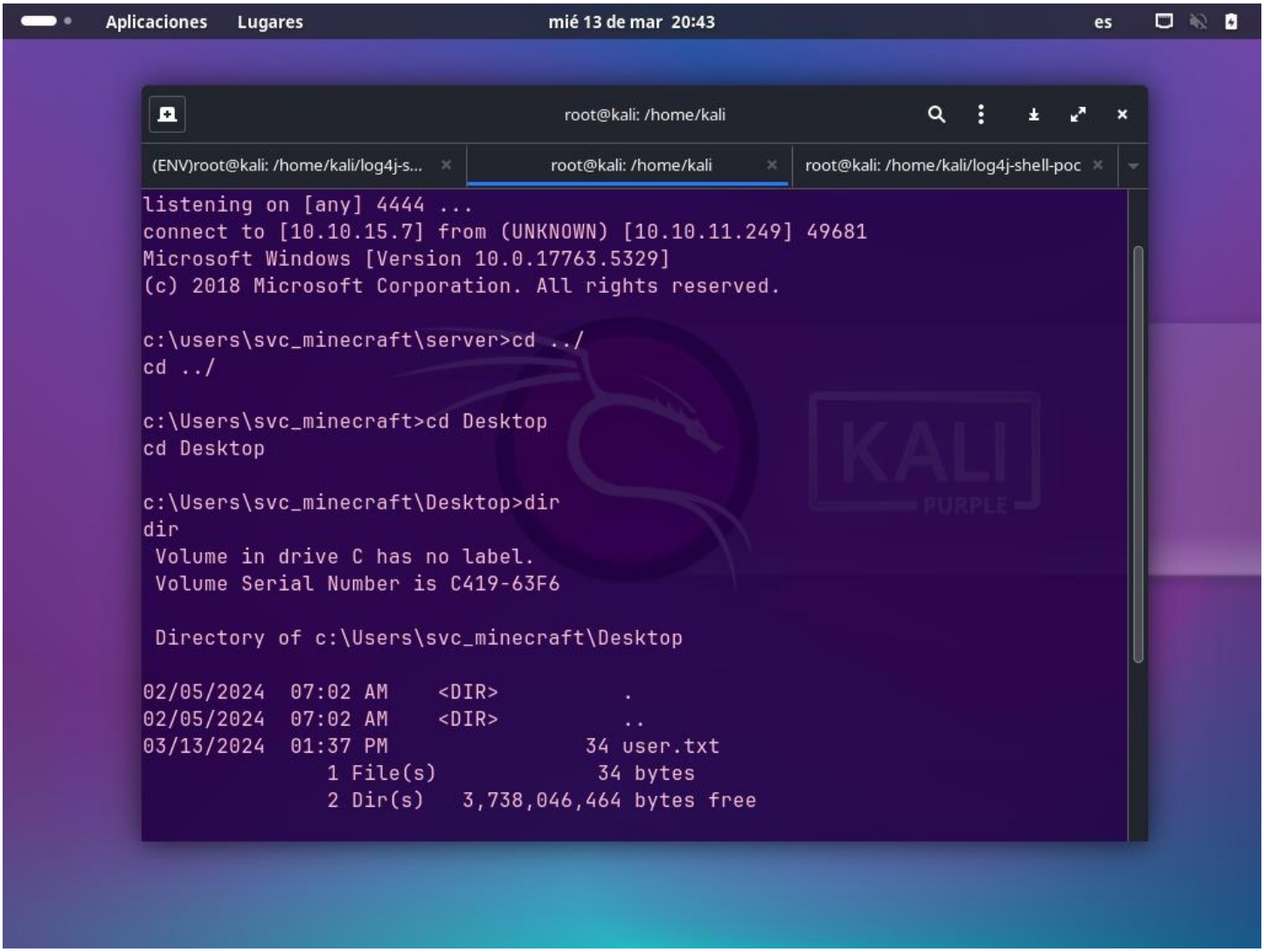


Resultado:

Se obtuvo reverse shell con permisos de usuario



Se capturó la flag de usuario



4. Escalada de privilegios

Dentro del servidor Minecraft, en el directorio de plugins, había un archivo .jar sospechoso

Para descargarlo:

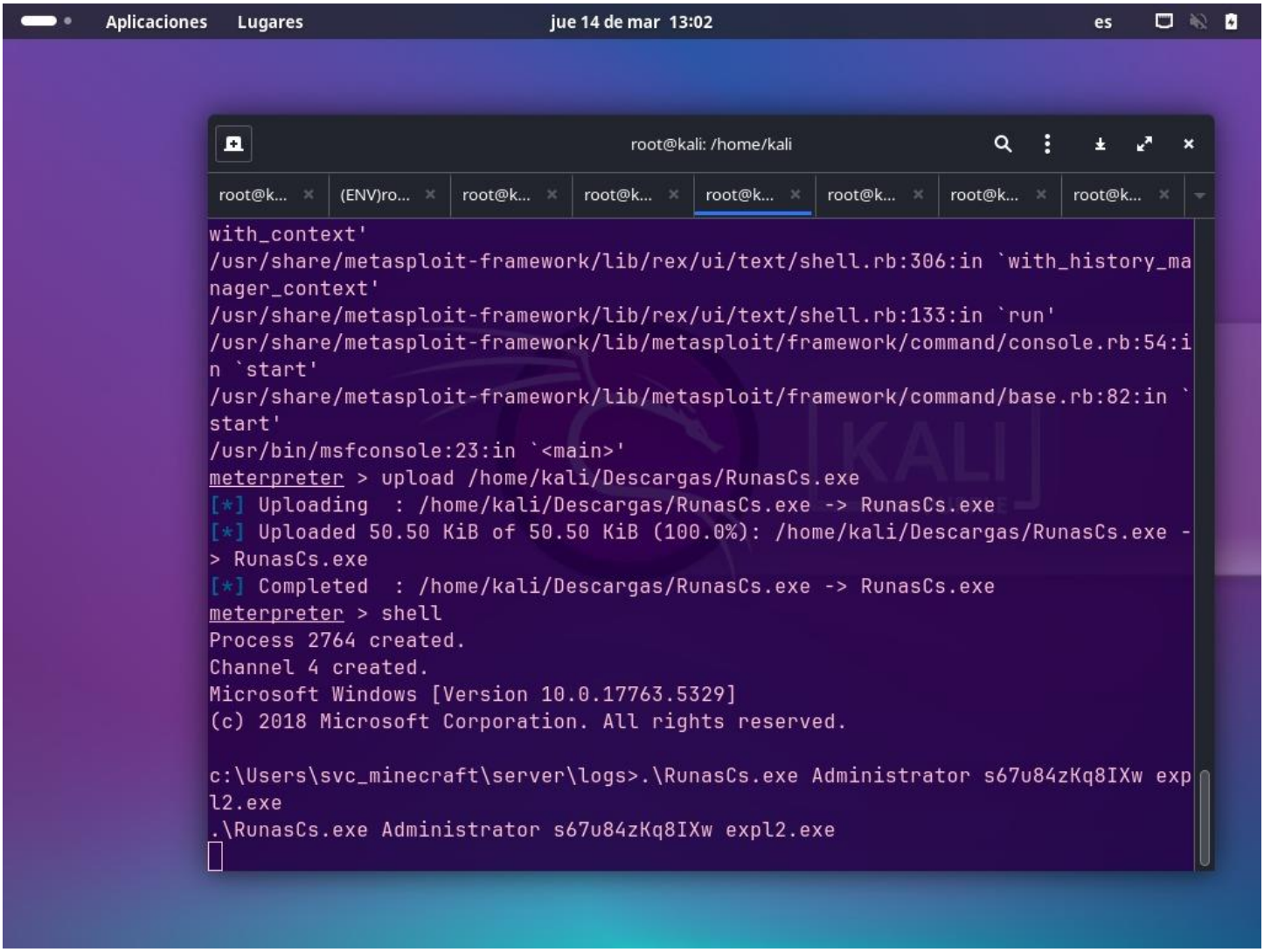
1. Se generó un payload con msfvenom windows/x64/meterpreter/reverse_tcp
2. Se subió el archivo al objetivo mediante certutil
3. Se ejecutó el payload y se obtuvo sessions en Meterpreter
4. Con Meterpreter se descargó el archivo .jar

Análisis del plugin:

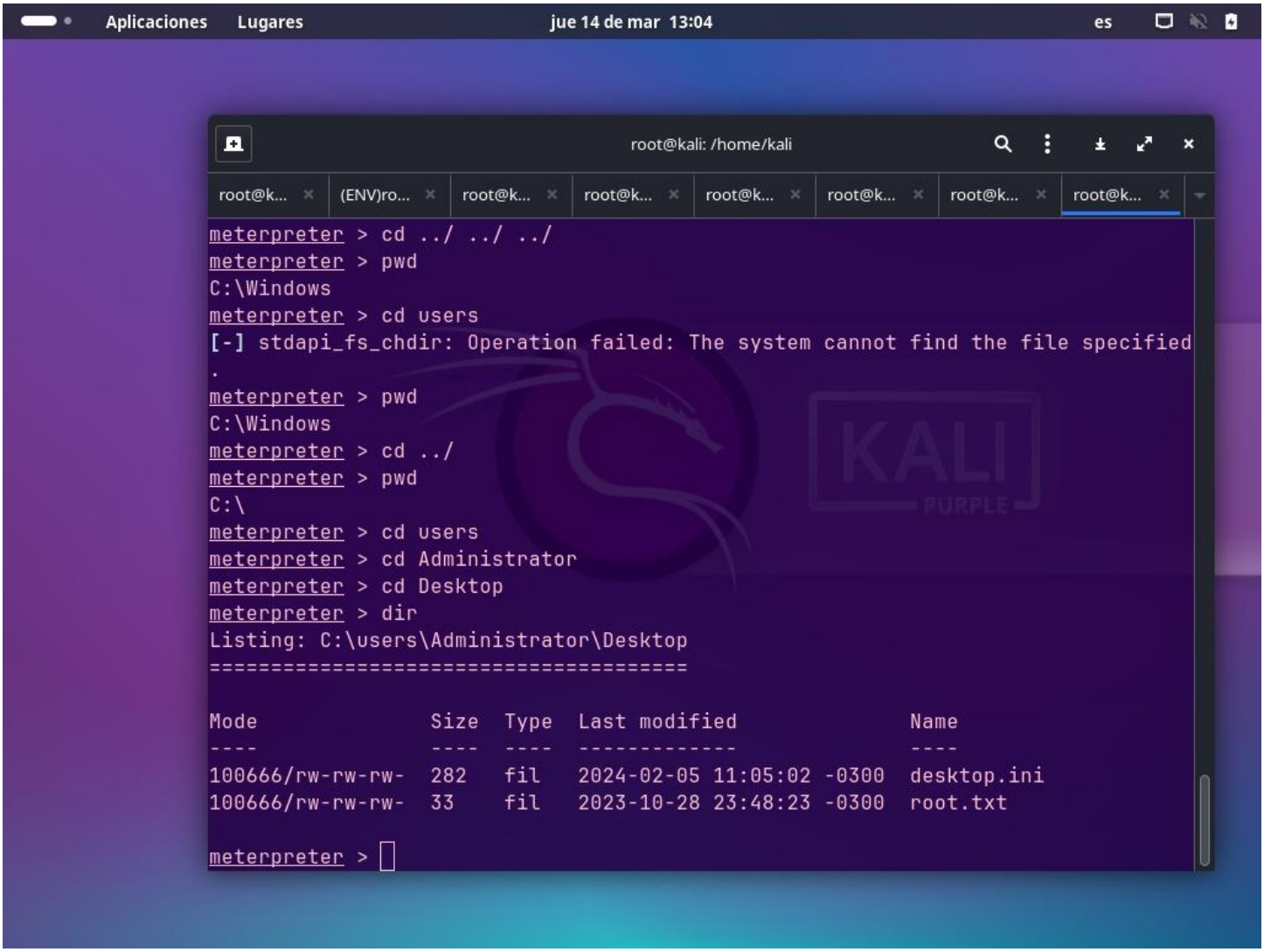
Usando JD-GUI, se identificó una contraseña en texto plano dentro del código del plugin

5. Obtención de Shell de Administrador

Para ejecutar procesos con credenciales elevadas, se descargó RunasCs.exe



Luego se generó un segundo payload con msfvenom (“expl2.exe”), se subió al objetivo y se ejecutó con RunasCs.exe Administrator <contraseña> expl2.exe



6. Resumen Final

- Se identificó un servidor vulnerable a Log4Shell (CVE-2021-44228) en puerto 25565 (Minecraft)
- Se creó un entorno completo para explotar la vulnerabilidad (LDAP, JDK, pyCraft)
- Se obtuvo acceso inicial mediante un mensaje malicioso enviado desde el juego
- Se escaló a Meterpreter, se descargó un plugin .jar y se extrajo una contraseña
- Usando RunasCs se obtenieron privilegios de administrador
- Se capturaron ambas flags: user y root