> *靶机地址:* https://www.vulnhub.com/entry/view2akill-1,387/

信息收集

```
nmap -sP 192.168.56.0/24
```

```
root@kali:~# nmap -sP 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 19:30 EST
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
MAC Address: 0A:00:27:00:00:3F (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00028s latency).
MAC Address: 08:00:27:47:7C:A0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up (0.00038s latency).
MAC Address: 08:00:27:E1:70:CE (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.11 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.104
```

```
root@kali:~# nmap -sS -sV -T5 -A -p- 192.168.56.104
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-19 19:32 EST
Nmap scan report for 192.168.56.104
Host is up (0.00071s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 54:8e:3a:14:b2:be:03:5c:d4:08:3a:ed:bb:e1:55:53 (RSA)
|   256 aa:be:cb:e1:b6:7f:47:75:29:f7:63:e5:f9:39:78:2e (ECDSA)
|_  256 de:1c:31:e0:15:4d:f5:dc:8e:bc:3c:e4:7d:64:75:54 (ED25519)
25/tcp   open  smtp    Postfix smtpd
|_smtp-commands: rain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
| ssl-cert: Subject: commonName=rain
| Subject Alternative Name: DNS:rain
| Not valid before: 2019-07-22T22:11:20
|_Not valid after:  2029-07-19T22:11:20
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-robots.txt: 4 disallowed entries
|_/joomla /zorin /dev /defense
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: A View To A Kill
8191/tcp open  http    PHP cli server 5.5 or later
|_http-title: electronic controller app
```

目录爆破

```
gobuster dir -u http://192.168.56.104 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/01/19 19:34:11 Starting gobuster
===============================================================
/dev (Status: 301)
/index.html (Status: 200)
/pics (Status: 301)
/joomla (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
/defense (Status: 301)
[ERROR] 2020/01/19 19:34:33 [!] parse http://192.168.56.104/error_log: net/url: invalid control
haracter in URL
/index.html (Status: 200)
```

访问robots.txt

```
User-agent: *
Disallow: /joomla
Disallow: /zorin
Disallow: /dev
Disallow: /defense
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/102926919