



[Oh My Grub] WriteUp

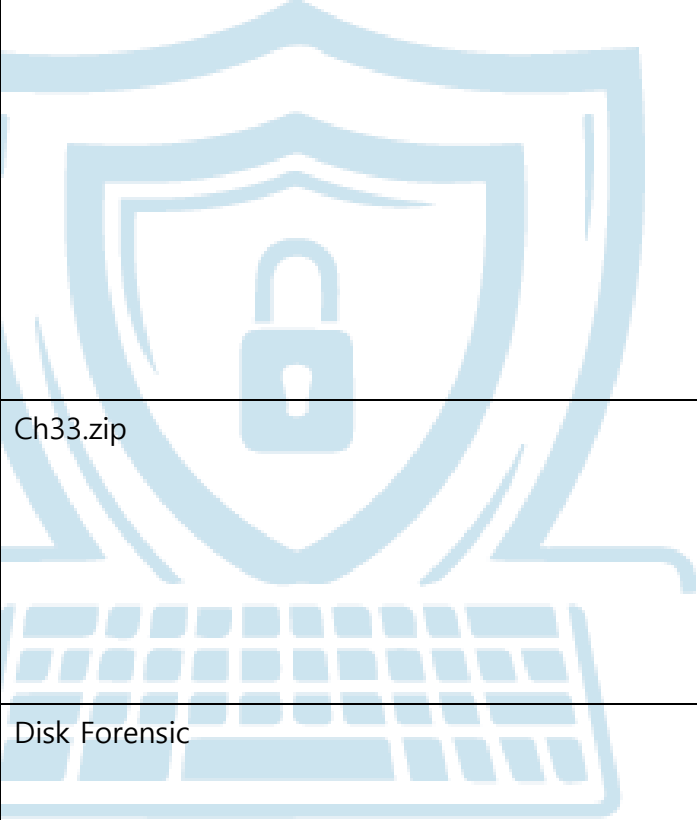
| | |
|---------|-----------------------|
| 작성자 | 윤건우 |
| 분석 일자 | 2025.04.20 |
| 분석 대상 | root.ova |
| 작성자 이메일 | liiiiiqueur@gmail.com |

목차

1. 문제
2. 분석 도구
3. 환경
4. WriteUp
5. Reference



1.문제

| | |
|-------|---|
| URL | https://www.root-me.org/en/Challenges/Forensic/Oh-My-Grub |
| 문제 설명 | <p>귀하의 회사가 오래된 서버에 접근할 수 없게 되었습니다. 안타깝게도 서버에는 중요한 파일이 담겨 있습니다. 이를 찾는 것은 귀하의 몫입니다.</p>  |
| 문제 파일 | Ch33.zip |
| 문제 유형 | Disk Forensic |
| 난이도 | 2 / 5 |

2.분석 도구

| 도구명 | 다운로드 링크 | 버전 |
|------------------------------|---|-----------------------|
| VMware Workstation 17 Player | https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion | 17.5.2 build-23775571 |
| | | |
| | | |
| | | |
| | | |
| | | |

3.환경

| 운영체제 |
|---|
| Microsoft Windows 11 Home 64-bit 10.0.26100 |
| |
| |

*확인 명령어(cmd): wmic os get Caption,CSDVersion,OSArchitecture,Version

4. WriteUp

| | |
|--------|-------------------------------------|
| 파일명 | root.ova |
| 용량 | 292305408 bytes |
| MD5 | X |
| SHA256 | X |
| 타임스탬프 | 2019-08-12 22:17:30.000000000 +0900 |

다운로드 받은 root.ova 파일의 용량은 292305408 bytes이고, 타임스탬프는 2019-08-12 22:17:30.000000000 +0900임을 확인할 수 있다.

```
C:\Users\Yungeonwoo\Desktop>stat root.ova
File: root.ova
Size: 292305408      Blocks: 285456      IO Block: 65536  regular file
Device: 64656f7bh/1684369275d  Inode: 6192449487974254  Links: 1
Access: (0644/-rw-r--r--)  Uid: (197609/Yungeonwoo)  Gid: (197609/Yungeonwoo)
Access: 2025-04-20 13:09:23.037464400 +0900
Modify: 2019-08-12 22:17:30.000000000 +0900
Change: 2025-04-20 13:09:23.045069400 +0900
Birth: 2025-04-20 13:09:01.315032800 +0900
```

사진 1 - 파일 용량 및 타임스탬프 확인

ova 파일은 기본적으로 가상 머신을 공유하기 위해 사용되는 것이다. 파일을 VMware에서 로드한다.

"Open a Virtual Machine" → root.ova 열기 → Import → Retry → Play virtual machine

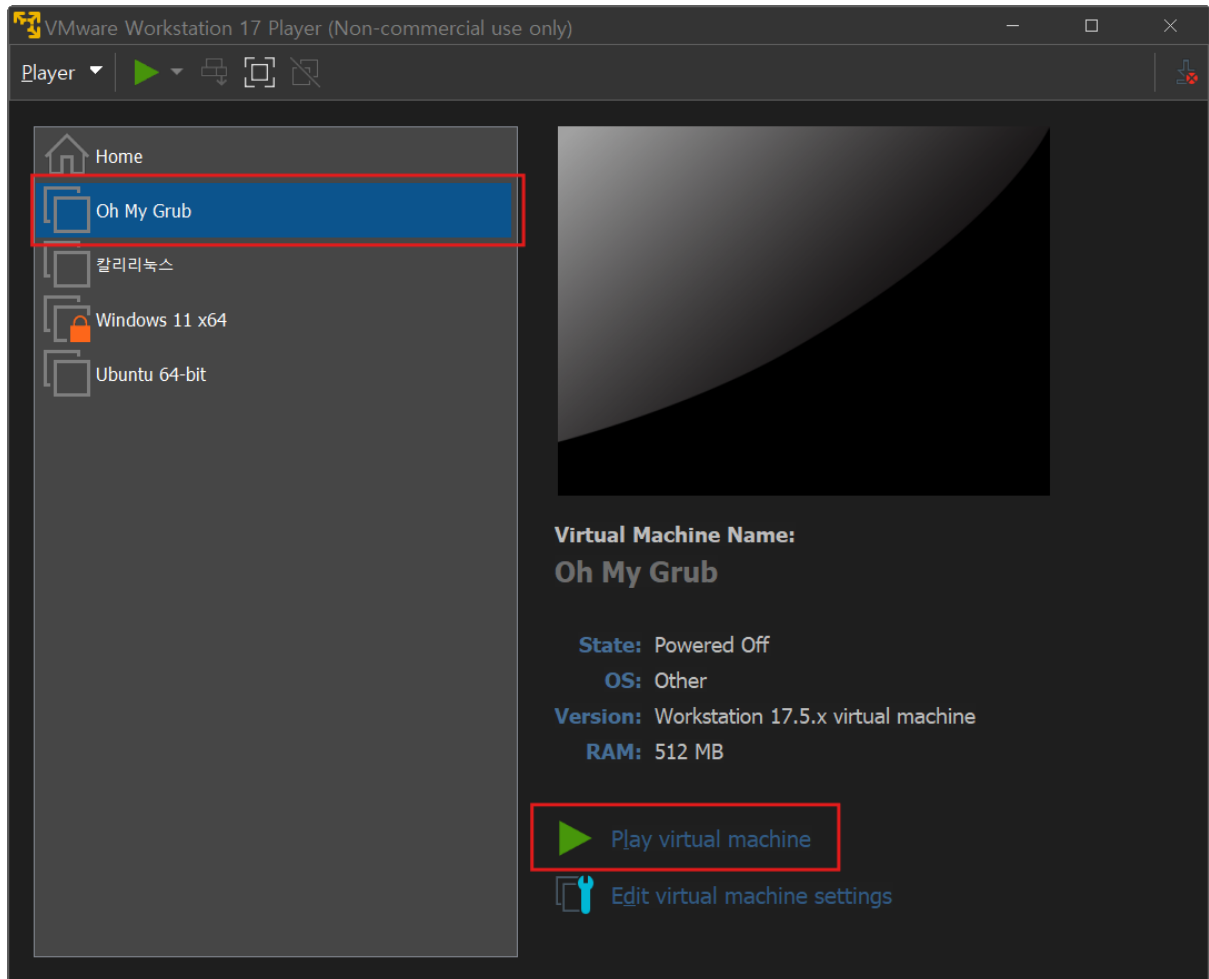


사진 2 - root.ova 로드

root.ova 파일이 로드되면 Debian GNU가 나타나 사용자 이름과 비밀번호를 묻는데 알 수 없다. 문제 이름에서 알 수 있듯이 GRUB를 사용하는 문제로 GRUB는 GNU에서 만든 부트로더다. 부트로더는 부팅을 도와주는 역할 프로그램이다. GRUB를 사용하면 패스워드 없이 부팅이 가능하다. GRUB의 내용은 레퍼런스에서 확인 가능하다.



사진 3 - 로그인

Restart Guest 후 두 번째 항목인 안전 모드에 진입 후 recovery mode 를 선택하고 e 키를 눌러 부팅 매개 변수를 수정할 수 있는 파일로 진입한다.

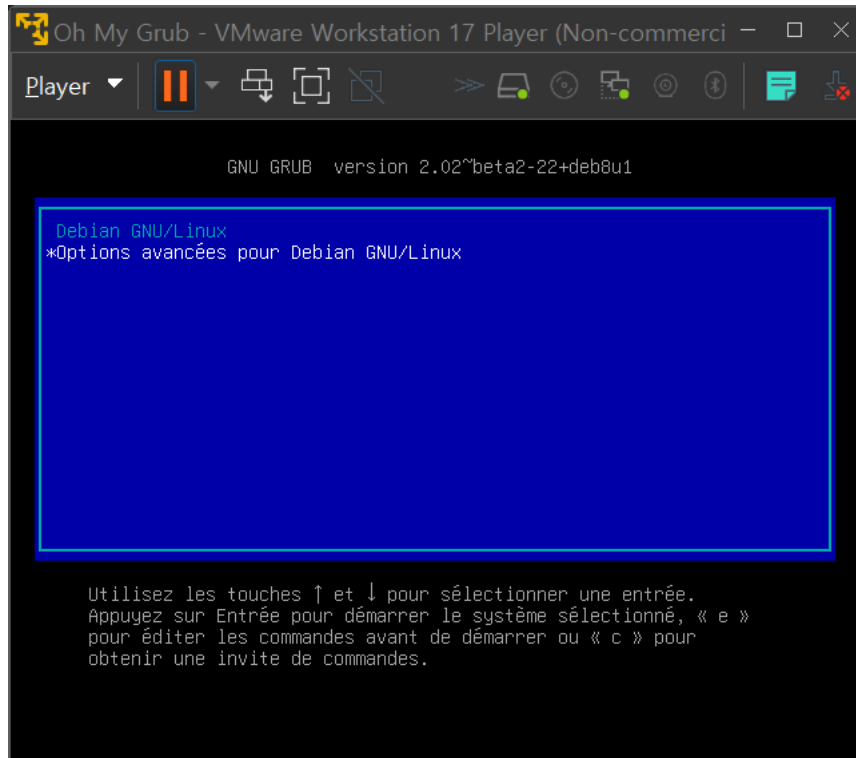


사진 4 - 안전 모드 진입

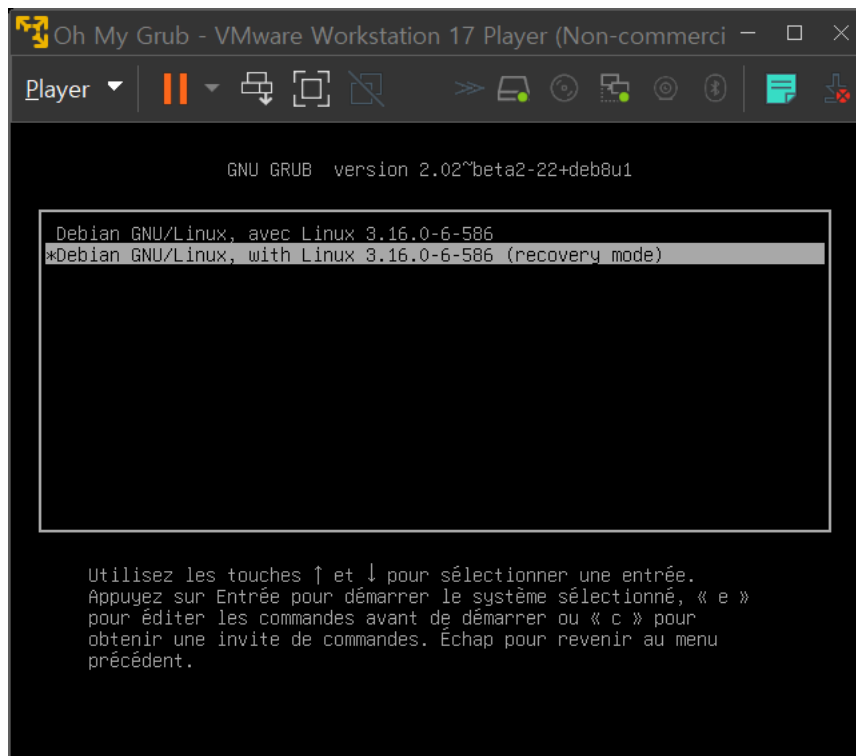
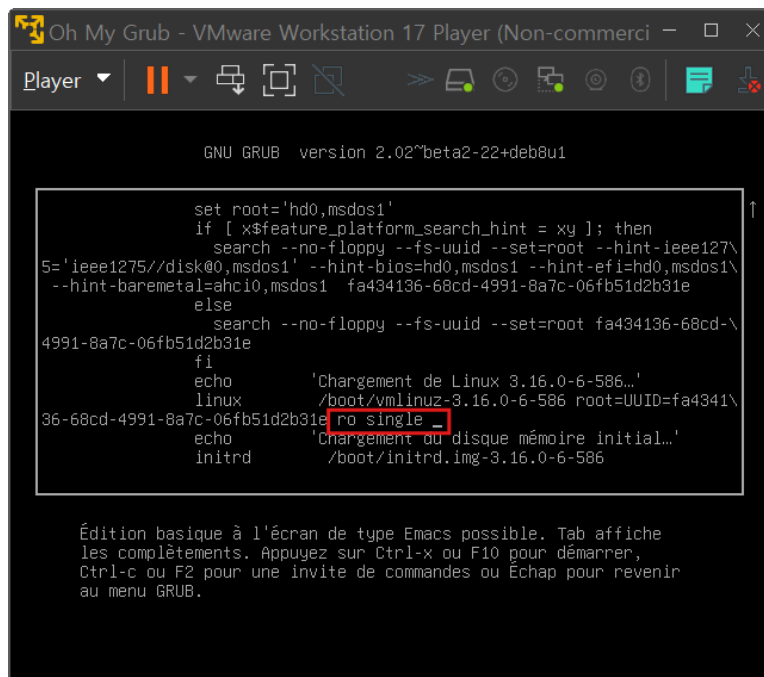


사진 5 – recovery mode 진입

진입한 파일은 grub.cfg 파일로 이 파일의 항목을 수정하고 재부팅하면 패스워드 입력

없이 로그인 가능하다. ro single 을 rw init=/bin/bash 로 변경 후, Ctrl + x 로 재부팅한다.

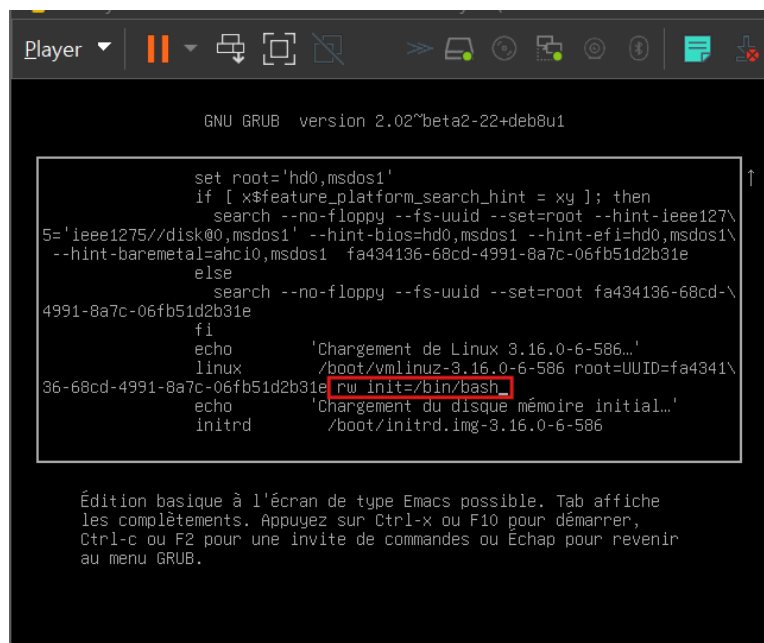


```
GNU GRUB version 2.02~beta2-22+deb8u1

set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-ieee127\
5='ieee1275//disk@0,msdos1' --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1\
--hint-baremetal=ahci0,msdos1 fa434136-68cd-4991-8a7c-06fb51d2b31e
else
  search --no-floppy --fs-uuid --set=root fa434136-68cd-\
4991-8a7c-06fb51d2b31e
fi
echo          'Chargement de Linux 3.16.0-6-586...'
linux        /boot/vmlinuz-3.16.0-6-586 root=UUID=fa4341\
36-68cd-4991-8a7c-06fb51d2b31e ro single
echo          'Chargement du disque mémoire initial...'
initrd       /boot/initrd.img-3.16.0-6-586

Édition basique à l'écran de type Emacs possible. Tab affiche
les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer,
Ctrl-c ou F2 pour une invite de commandes ou Echap pour revenir
au menu GRUB.
```

사진 6 – grub.cfg 파일 변경 전



```
GNU GRUB version 2.02~beta2-22+deb8u1

set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
  search --no-floppy --fs-uuid --set=root --hint-ieee127\
5='ieee1275//disk@0,msdos1' --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1\
--hint-baremetal=ahci0,msdos1 fa434136-68cd-4991-8a7c-06fb51d2b31e
else
  search --no-floppy --fs-uuid --set=root fa434136-68cd-\
4991-8a7c-06fb51d2b31e
fi
echo          'Chargement de Linux 3.16.0-6-586...'
linux        /boot/vmlinuz-3.16.0-6-586 root=UUID=fa4341\
36-68cd-4991-8a7c-06fb51d2b31e rw init=/bin/bash
echo          'Chargement du disque mémoire initial...'
initrd       /boot/initrd.img-3.16.0-6-586

Édition basique à l'écran de type Emacs possible. Tab affiche
les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer,
Ctrl-c ou F2 pour une invite de commandes ou Echap pour revenir
au menu GRUB.
```

사진 7 – grub.cfg 파일 변경 후


```
Oh My Grub - VMware Workstation 17 Player (Non-commercial use only)
Player
[ 3.057168] usb 1-2: Manufacturer: VMware, Inc.
[ 3.058697] hub 1-2:1.0: USB hub found
[ 3.059085] hub 1-2:1.0: 7 ports detected
[ 3.619450] random: nonblocking pool is initialized
[ 4.875553] floppy0: no floppy controllers found
[ 4.876869] work still pending
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [ 4.889252] PM: Starting manual resume from disk
done.
Begin: Will now check root file system ... fsck from util-linux 2.25.2
[/sbin/fsck.ext4 (1) -- /dev/sda1] fsck.ext4 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 12163/499712 files, 149903/1998336 blocks
done.
[ 4.986478] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/#
```

사진 8 - Ctrl + x로 재부팅한 결과

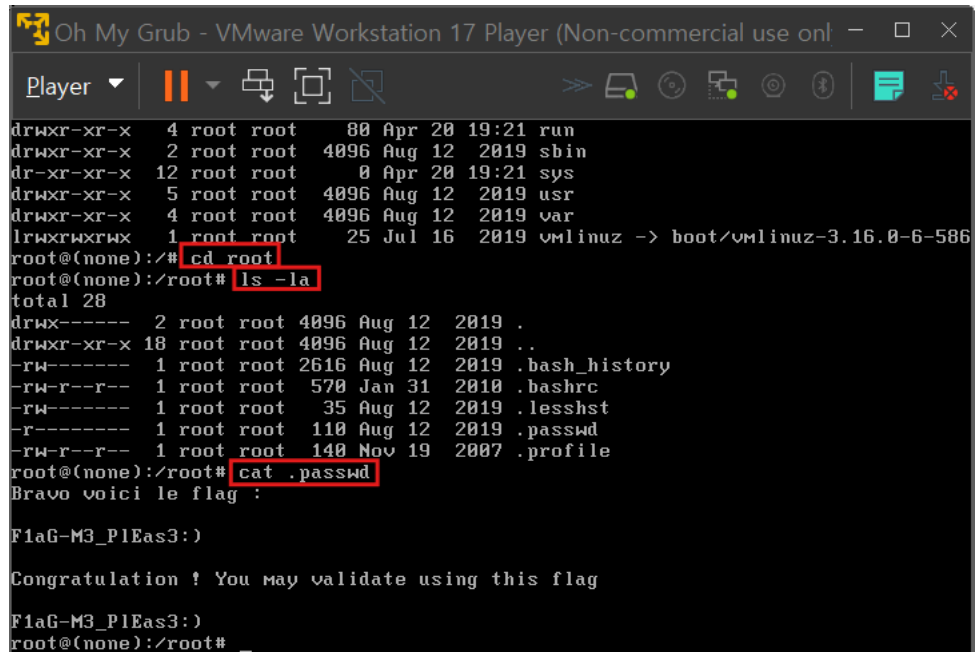
ls -la 명령어로 파일 및 디렉토리 목록을 확인하면 사용자가 직접 추가한 디렉토리인 root를 발견할 수 있다.

```
Oh My Grub - VMware Workstation 17 Player (Non-commercial use only)
Player
bash: no job control in this shell
root@(none):/# ls -la
total 68
drwxr-xr-x 18 root root 4096 Aug 12 2019 .
drwxr-xr-x 18 root root 4096 Aug 12 2019 ..
drwxr-xr-x 2 root root 4096 Jul 16 2019 bin
drwxr-xr-x 3 root root 4096 Jul 16 2019 boot
drwxr-xr-x 9 root root 2320 Apr 20 19:21 dev
drwxr-xr-x 55 root root 4096 Aug 12 2019 etc
drwxr-xr-x 3 root root 4096 Jul 16 2019 home
lrwxrwxrwx 1 root root 29 Jul 16 2019 initrd.img -> /boot/initrd.img-3.16.0-6-586
drwxr-xr-x 14 root root 4096 Jul 16 2019 lib
drwx----- 2 root root 16384 Jul 16 2019 lost+found
drwxr-xr-x 3 root root 4096 Jul 16 2019 media
drwxr-xr-x 2 root root 4096 Jul 16 2019 opt
dr-xr-xr-x 106 root root 0 Apr 20 19:21 proc
drwx----- 2 root root 4096 Aug 12 2019 root
drwxr-xr-x 4 root root 80 Apr 20 19:21 run
drwxr-xr-x 2 root root 4096 Aug 12 2019/sbin
dr-xr-xr-x 12 root root 0 Apr 20 19:21 sys
drwxr-xr-x 5 root root 4096 Aug 12 2019/usr
drwxr-xr-x 4 root root 4096 Aug 12 2019/var
lrwxrwxrwx 1 root root 25 Jul 16 2019 vmlinuz -> boot/vmlinuz-3.16.0-6-586
root@(none):/#
```

사진 9 - root 디렉토리

이후 root 디렉토리에 접근 후, 다시 한 번 파일 및 디렉토리 항목을 확인하면 .passwd

파일을 확인할 수 있고, 이 파일을 읽어보면 flag 값을 발견할 수 있다.



```
Oh My Grub - VMware Workstation 17 Player (Non-commercial use only)
Player
drwxr-xr-x 4 root root 80 Apr 20 19:21 run
drwxr-xr-x 2 root root 4096 Aug 12 2019 sbin
dr-xr-xr-x 12 root root 0 Apr 20 19:21 sys
drwxr-xr-x 5 root root 4096 Aug 12 2019 usr
drwxr-xr-x 4 root root 4096 Aug 12 2019 var
lrwxrwxrwx 1 root root 25 Jul 16 2019 vmlinuz -> boot/vmlinuz-3.16.0-6-586
root@(none):/# cd root
root@(none):/root# ls -la
total 28
drwx----- 2 root root 4096 Aug 12 2019 .
drwxr-xr-x 18 root root 4096 Aug 12 2019 ..
-rw----- 1 root root 2616 Aug 12 2019 .bash_history
-rw-r--r-- 1 root root 570 Jan 31 2010 .bashrc
-rw----- 1 root root 35 Aug 12 2019 .lesshst
-r----- 1 root root 110 Aug 12 2019 .passwd
-rw-r--r-- 1 root root 140 Nov 19 2007 .profile
root@(none):/root# cat .passwd
Bravo voici le flag :

F1aG-M3_PlEas3:)

Congratulation ! You may validate using this flag

F1aG-M3_PlEas3:)
root@(none):/root# _
```

사진 10 - .passwd 파일 내용 보기

5.Reference

<https://www.gnu.org/software/grub/manual/grub/grub.html>