1.red star (10 Point) wath distribution of Linux is being used on this machine?

First of all, I am going to take a look in all the evidence with fdisk just to see the partitions

```
drjekyll@drjekyll:~/Documentos/defcon$ sudo fdisk -l adamdisk.001
Disco adamdisk.001: 50 GiB, 53687091200 bytes, 104857600 sectores
Unidades: sectores de 1 * 512 = 512 bytes
Tamaño de sector (lógico/físico): 512 bytes / 512 bytes
Tamaño de E/S (mínimo/óptimo): 512 bytes / 512 bytes
Tipo de etiqueta de disco: dos
Identificador del disco: 0xc2714295

Dispositivo    Inicio Comienzo     Final Sectores Tamaño Id Tipo
adamdisk.001p1 *          2048   1126399  1124352   549M  7 HPFS/NTFS/exFAT
adamdisk.001p2         1126400  67104767 65978368  31,5G  7 HPFS/NTFS/exFAT
adamdisk.001p3        67106816  73500671  6393856   3,1G  7 HPFS/NTFS/exFAT
adamdisk.001p4        75560958 104855551 29294594    14G  5 Extendida
adamdisk.001p5        75560960 104855551 29294592    14G 83 Linux
```

As we can see, the important one is the last one, from 75560960 to 104855551, then I will extract the partition

```
drjekyll@drjekyll:~/Documentos/defcon$ dd if=adamdisk.001 of=linux.dd
skip=75560960 count=104855551
29296640+0 registros leídos
29296640+0 registros escritos
14999879680 bytes (15 GB, 14 GiB) copied, 185,615 s, 80,8 MB/s
```

A good and fast option is to mount the partition and just go inside an look

```
drjekyll@drjekyll:~/Documentos/defcon$ sudo mount -o loop linux.dd /mnt/
drjekyll@drjekyll:$ cd mnt
drjekyll@drjekyll:/mnt$ ls
0     dev   initrd.img      lib64       mnt    root  srv  usr      vmlinuz.old
bin   etc   initrd.img.old  lost+found  opt    run   sys  var
boot  home  lib             media       proc   sbin  tmp  vmlinuz
```

We are in!! to solve the firs qestion we have to search in boot:

```
drjekyll@drjekyll:/mnt/boot$ ls
config-4.13.0-kali1-amd64      System.map-4.13.0-kali1-amd64
grub                           vmlinuz-4.13.0-kali1-amd64
initrd.img-4.13.0-kali1-amd64
```

The answer is Kali linux

2.abc123 (10 Point) What is the MD5 has of the apache access.log?

This is a eassy one Linux save the logs files in */var* logs

```
drjekyll@drjekyll:$ cd /mnt/var/log/apache2
drjekyll@drjekyll:/mnt/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
drjekyll@drjekyll:/mnt/var/log/apache2$ md5sum access.log
d41d8cd98f00b204e9800998ecf8427e  access.log
```

The answer is d41d8cd98f00b204e9800998ecf8427e

3.Radiohead — No Surprises (10 Point) It is believed that a credential dumping tool was downloaded, what is the name of the download?

Going to the download directory just to see…

```
drjekyll@drjekyll:$ cd /mnt/root/Downloads
drjekyll@drjekyll:/mnt/root/Downloads$ ls
mimikatz_trunk.zip
```

A research in github tell us that it is the software that we are looking for https://github.com/gentilkiwi/mimikatz, then the answer is mimikatz

4.super duper secret (15 Point) There was a super secret file created, what is the absolute path

We can focus on bash history that is allocated in root directory but not currently visible, I use *ls -a*

```
drjekyll@drjekyll:/mnt/root$ ls -a
.               .cache     .gconf         .mozilla  Public     .viminfo
..              .config    .gnupg         .msf4     .rnd
.bash_history   Desktop    .ICEauthority  Music     snky
.bashrc         Documents  irZLAohL.jpeg  Pictures  Templates
.binwalk        Downloads  .local         .profile  Videos
```

We are going to take a look in shell history, usually linux people use vim, nano, cat or visudo to menage files:

```
drjekyll@drjekyll:/mnt/root$ sudo cat /mnt/root/.bash_history | egrep "vim|nano|
visudo|cat"
cat snky snky > /root/Desktop/SuperSecretFile.txt
vim hellworld.sh
vim firstscript
vim firstscript
vim firstscript
vim firstscript_fixed
sudo visudo
```

The answer is *SuperSecretFile.txt*

5.this is a hard one (15 Point) what program used didyouthinkwedmakeiteasy.jpg durin execution?

We are going to do the same than in last question

```
drjekyll@drjekyll:/mnt/root$ sudo cat /mnt/root/.bash_history | egrep
"didyouthink"
binwalk didyouthinkwedmakeiteasy.jpg
```

Binwalk

overachiever (15 Point) What is the third goal from the checkist Karen created.

I made a research with fin, as a result I had a lot of lines but reading I found the interesting one:

```
drjekyll@drjekyll:/mnt/root$ find /mnt -user root -iname checklist*
……..
find: ‘/mnt/var/spool/exim4’: Permiso denegado
find: ‘/mnt/var/spool/rsyslog’: Permiso denegado
find: ‘/mnt/tmp/tracker-extract-files.0’: Permiso denegado
find: ‘/mnt/lib/firmware/b43’: Permiso denegado
find: ‘/mnt/lib/firmware/b43legacy’: Permiso denegado
find: ‘/mnt/root/.local’: Permiso denegado
/mnt/root/Desktop/Checklist
find: ‘/mnt/root/.gconf’: Permiso denegado
find: ‘/mnt/root/.mozilla’: Permiso denegado
find: ‘/mnt/root/.gnupg’: Permiso denegado
find: ‘/mnt/root/.config/leafpad’: Permiso denegado
……….
```

Going to the rooute and reading the list:

```
drjekyll@drjekyll:/mnt/root/Desktop$ cat Checklist
Check List:

- Gain Bob's Trust
- Learn how to hack
- Profit
```

Profit was the answer

7.attack helicopter (20 Point) How many times was apache run?

Logs are stored in */var/log*

```
drjekyll@drjekyll:/mnt/var/log/apache2$ cat access.log
```

It not seem to have nothing inside...

```
drjekyll@drjekyll:/mnt/var/log/apache2$ du -s access.log
0      access.log
```

It is empty, so he has never acceded, the answer is 0. Also it has an other reason, doing ls in the directory we only see:

```
drjekyll@drjekyll:/mnt/var/log/apache2$ ls
access.log  error.log  other_vhosts_access.log
```

There is a file called logrotate of any program, it has the configuration to save the logs, is designed to ease administration of systems that generate large numbers of log files. It allows automatic rotation, compression, removal, and mailing of log files. For this reason we usually see things like this when we search a log:

```
auth.log    auth.log.1
```

There are the different rotations, and also apache haves his one:

```
drjekyll@drjekyll:/mnt/etc/logrotate.d$ ls
alternatives  exim4-base        nginx              speech-dispatcher
apache2       exim4-paniclog    postgresql-common  stunnel4
apt           glusterfs-common  ppp                unattended-upgrades
couchdb       macchanger        rsyslog
dpkg          mysql-server      samba
drjekyll@drjekyll:/mnt/etc/logrotate.d$ cat apache2
/var/log/apache2/*.log {
      daily
      missingok
      rotate 14
      compress
      delaycompress
      notifempty
      create 640 root adm
      sharedscripts
      postrotate
                if invoke-rc.d apache2 status > /dev/null 2>&1; then \
                    invoke-rc.d apache2 reload > /dev/null 2>&1; \
                fi;
      endscript
      prerotate
            if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
                  run-parts /etc/logrotate.d/httpd-prerotate; \
            fi; \
      endscript
}
```

And also in the estatus file:

```
drjekyll@drjekyll:/mnt/var/lib/logrotate$ cat status | egrep "apache2"
"/var/log/apache2/access.log" 2019-3-13-17:0:0
"/var/log/apache2/other_vhosts_access.log" 2019-3-13-17:0:0
"/var/log/apache2/error.log" 2019-3-13-17:0:0
```

Probably the creation of the files

I check it only to be sure, everything is correct, it is not other log file because apache was never used.

8.oh no some1 call ic3 (25 Point) It is believed this machine was used to attack another, what file prove it?

In the bash history we can see that he was using metasploit:

```
drjekyll@drjekyll:/mnt/root$ sudo cat /mnt/root/.bash_history
[sudo] contraseña para drjekyll:
msfconsole
systemctl status postgresql
systemctl enable postgresql
systemctl start postgresql
msfconsole
msfdb init
msfconsole
```

In the history and logs of msf I didn't see nothing of interest

```
drjekyll@drjekyll:/mnt/root/.msf4$ cat history
```

```
db_nmap -sV -O -T5 -Pn 10.0.0.101
db_nmap -sV -O -T5 -Pn 10.0.0.101 -oX ~/nmap_out.xml
db_nmap -sV -O -T5 -Pn 10.0.0.101 -oX /root/nmap_out.xml
search eternal
use exploit/windows/smb/ms17_010_eternalblue
options
set RHOST 10.0.0.101
run
```

The target host was 10.0.0.101…

Well,at the end the solution was in the root directory, just the jpg image named irZLAohL.jpeg. Sincerely I did not understand this part…

10.the who (30 Point) a user su’d to root at 11:26 multiple times. Who was it’

Searchin in auth.log

```
drjekyll@drjekyll:/mnt/var/log$ cat auth.log | egrep "su"
Mar 20 11:26:22 KarenHacker su[4060]: Successful su for postgres by root
Mar 20 11:26:22 KarenHacker su[4060]: + ??? root:postgres
Mar 20 11:26:22 KarenHacker su[4060]: pam_unix(su:session): session opened for
user postgres by (uid=0)
```

11./ (30 Point) Based on the bahs history, what is the current working directory?

As we can see in bash history the last one was myfirsthack:

```
drjekyll@drjekyll:/mnt/var/log$ sudo cat /mnt/root/.bash_history
...
cd ..
ls
cd home/
ls
cd /root
ls
cd ../root
cd ../root/Documents/myfirsthack/../../Desktop/
sl
ls
cd ../Documents/myfirsthack/
netstat
echo bob.txt
…
```