CYBERDRAGONS UBUNTU 16 PRACTICE IMAGE II WRITE UP

Forensics Question I

Which users are members of the group villains?

```
getent group villains
```

Forensics Question II

What is the absolute path including the file name?

```
find / -type f -size 168490c -user kzorel
2>/dev/null
```

Forensics Question III

Decipher the graphic and determine the plaintext of the cipher.

```
  1.  Open the file that is referenced in the
    previous forensics question
  2.  Copy the ciphertext and key
  3.  Find a bifid cipher decoder on the Internet
  4.  Retrieve the plaintext and answer the
    question!
```

Auto updates have been enabled

1. Go to Software & Updates
2. Under “Ubuntu Software,” check the first three boxes
3. Under “Other Software,” check both “Canonical Partners” boxes
4. Under “Updates,” check the first three boxes, automatically check for updates daily, and never notify for new Ubuntu versions

Bash has been updated, FireFox has been updated, Linux kernel has been updated

```
sudo apt-get upgrade -y
reboot when complete
```

User mel is not an administrator

```
gpasswd -d mel sudo
```

User jjons is now an administrator

```
gpasswd -a jjons sudo
```

Removed unauthorized user lexluthor

```
userdel lexluthor
```

Removed unauthorized user sarias

```
userdel sarias
```

Firewall protection has been enabled

```
ufw enable
ufw allow ssh
```

Changed insecure password for user adanvers

1. Go to “Users and groups”
2. Change adanvers’ password

In a competition scenario, you would change the passwords of all authorized users to something secure, not just adanvers’s.

Catco and deo groups added

```
groupadd catco
groupadd deo
```

Groups catco and DEO have members added

```
gpasswd -a kzorel deo
gpasswd -a adanvers deo
gpasswd -a jjons deo
gpasswd -a wschott deo
gpasswd -a kzorel catco
gpasswd -a jolsen catco
gpasswd -a cgrant catco
```

Guest account has been disabled

```
cd /etc/lightdm
gedit lightdm.conf
add “[Seat:*]
allow-guest=false”
```

Default Password MAX Days set to 90/MIN Days set to 10

```
gedit /etc/login.degs
set PASS_MAX_DAYS to 90
set PASS_MIN_DAYS to 10
```

Prohibited software Doomsday removed

1. Use the command dpkg -l
2. Look for any prohibited software
3. If you have found something suspicious, search for it in the package list with dpkg -l | egrep “name”

```
dpkg -l | egrep “doom”
apt-get purge doomsday doomsday-common doomsday-data freedoom -y
```

Prohibited mp3 files are removed

```
find /home -type f -iname *.mp3
find /home -type f -iname *.mp3 -exec rm {} +
```

Unauthorized app kismet has been uninstalled

1. Use the command dpkg -l
2. Look for any prohibited software
3. If you have found something suspicious, search for it in the package list with dpkg -l | egrep “name”

```
dpkg -l | egrep “kis”
apt-get purge kismet -y
```

Prohibited software aircrack-ng removed

1. Use the command dpkg -l
2. Look for any prohibited software
3. If you have found something suspicious, search for it in the package list with dpkg -l | egrep “name”

```
dpkg -l | egrep “crack”
apt-get purge aircrack-ng -y
```

PureFTPd service has been disabled or removed

1. Use the command netstat -tulpn
2. Notice that PureFTPd is running when it does not need to be running
3. dpkg -l | egrep “ftp”
4. apt-get purge pure-ftpd pure-ftpd-c