

LAB 5 Password Cracking Linux

1. User 1 password (dog)

```
(student@kali.example.com)-[~]
└─$ sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
```

2. User 2 password (8571)

```
(student@kali.example.com)-[~]
└─$ sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
```

3. User3 password (food09)

```
(student@kali.example.com)-[~]
└─$ sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
```

4. User4 password (candy24\$\$)

```
passwd: password unchanged
(student@kali.example.com)-[~]
└─$ sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
(student@kali.example.com)-[~]
```

5. User5 password (love302)

```
passwd: password updated successfully
(student@kali.example.com)-[~]
└─$ sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
(student@kali.example.com)-[~]
```

6. User6 password (Money20\$\$)

```
passwd: password updated successfully
(student@kali.example.com)-[~]
└─$ sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
(student@kali.example.com)-[~]
```

```
passwd: password updated successfully
(student@kali.example.com)-[~]
└─$ sudo cat /etc/shadow | grep -E 'user1|user2|user3|user4|user5|user6'
user1:$y$j9T$jZj9kaxw/CHKuDUI7BzuG.$x0qXRSEzDtL0yEfDIq58yIJeQRchDgLoBo.oGiZJML7:
20153:0:99999:7:::
user2:$y$j9T$PTse5N7h3w/07nbnScn5k1$6vLp0bMwCvmmw08MzqIcZi/zN2ggy/zLT89uTmIGKQC:
20153:0:99999:7:::
user3:$y$j9T$3c1wvJG2l.LWDWXGIllis60$PORDkLCDAn2Ijq2mDxSNjGCIU7IV4iTpX7A.S3Cru3:
20153:0:99999:7:::
user4:$y$j9T$7AwXhgULHhRqS20qSj6t/$0Ho3oZNzaEkf0QX11Rf2bICX3ykA4pvmMAVFFgVmA:
20153:0:99999:7:::
user5:$y$j9T$g6BuaTv5gJVjCHUcoDARK.$.$zZnhql.t66Hhvy080cZNIqOx.BhEhXR9mmsbjo72i3:
20153:0:99999:7:::
user6:$y$j9T$Uvbo/ZiTnnNlchpZkFQe40$wgAL8mskJFkkuYVCRzSY1IwMFxXZQ46WZEQBsFvm800:
20153:0:99999:7:::
```

7.

```
(student@kali.example.com)-[~]
└─$ sudo john --format=crypt zjord001.hash --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:decrypt 2:md5crypt 3:summd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
fopen: rockyou.txt: No such file or directory
(student@kali.example.com)-[~]
```

LAB 5 Password Cracking Linux

```
→ sudo john --show --format=ntlm --list=/usr/share/john/ntlm.lst  
student:student:1000:1001:1001:Cyber Range Student:/home/student:/bin/bash  
xxxxx:abcde:1001:1002:1002:1002:/home/xxxxx:/bin/sh
```

8. 2 password hashes cracked, 0 left