Password Security Assessment with John-the-Ripper

The primary goal of this project is to assess password security by employing the john-the-ripper function in Ubuntu to crack passwords. We have meticulously designed five designated user accounts, each with varying types of passwords, to gauge their vulnerability to potential attacks. Through this project, we aim to shed light on the importance of robust password practices and reinforce the significance of data protection for user accounts.

User Names & Passwords:
To comprehensively analyze password security, we created five new user accounts: Jim, Reed, Ouse, House, Karim, and Sameer. Each user's password represents a different complexity level:

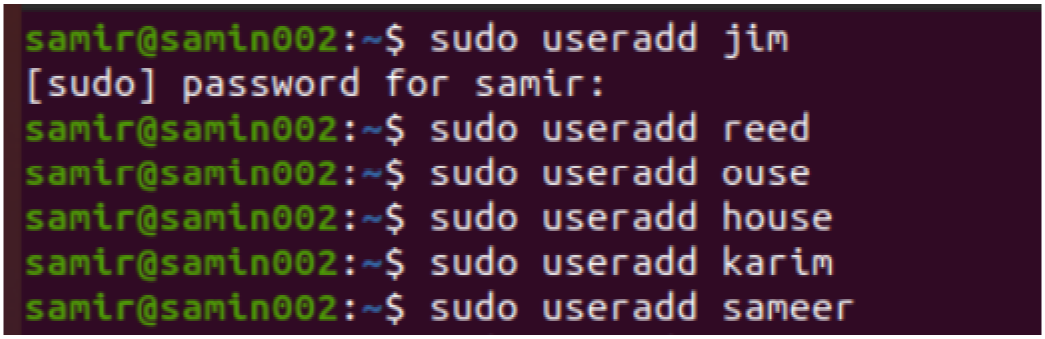
1. Jim: Utilizing a simple dictionary word as the password (e.g., "same").
2. Reed: Employing four simple digits as the password (e.g., "1234").
3. Ouse: Combining a simple dictionary word with digits (e.g., "house123").
4. House: Integrating a simple dictionary word with digits and a symbol (e.g., "phone123&").
5. Karim: Incorporating a simple dictionary word with digits (e.g., "car123").
6. Sameer: Creating a complex password with dictionary words, upper and lower cases, digits, and symbols (e.g., "ComPutEr123$").

Methodology:
After setting up the user accounts and their respective passwords, we compiled the passwords into a single hash file, "Samiraminzay2002.hash," using the tail and hash functions. We allowed a ten-minute waiting period before initiating the john-the-ripper program to attempt password cracking. Through this process, we were able to identify which passwords were successfully cracked and which remained unbroken, revealing potential security vulnerabilities.

Significance:
This project serves as an eye-opening exploration into password security assessment, emphasizing the critical role strong and complex passwords play in safeguarding user accounts and sensitive information. By demonstrating the effectiveness of john-the-ripper and highlighting password weaknesses, we aim to empower users to adopt secure password practices and enhance overall data protection.

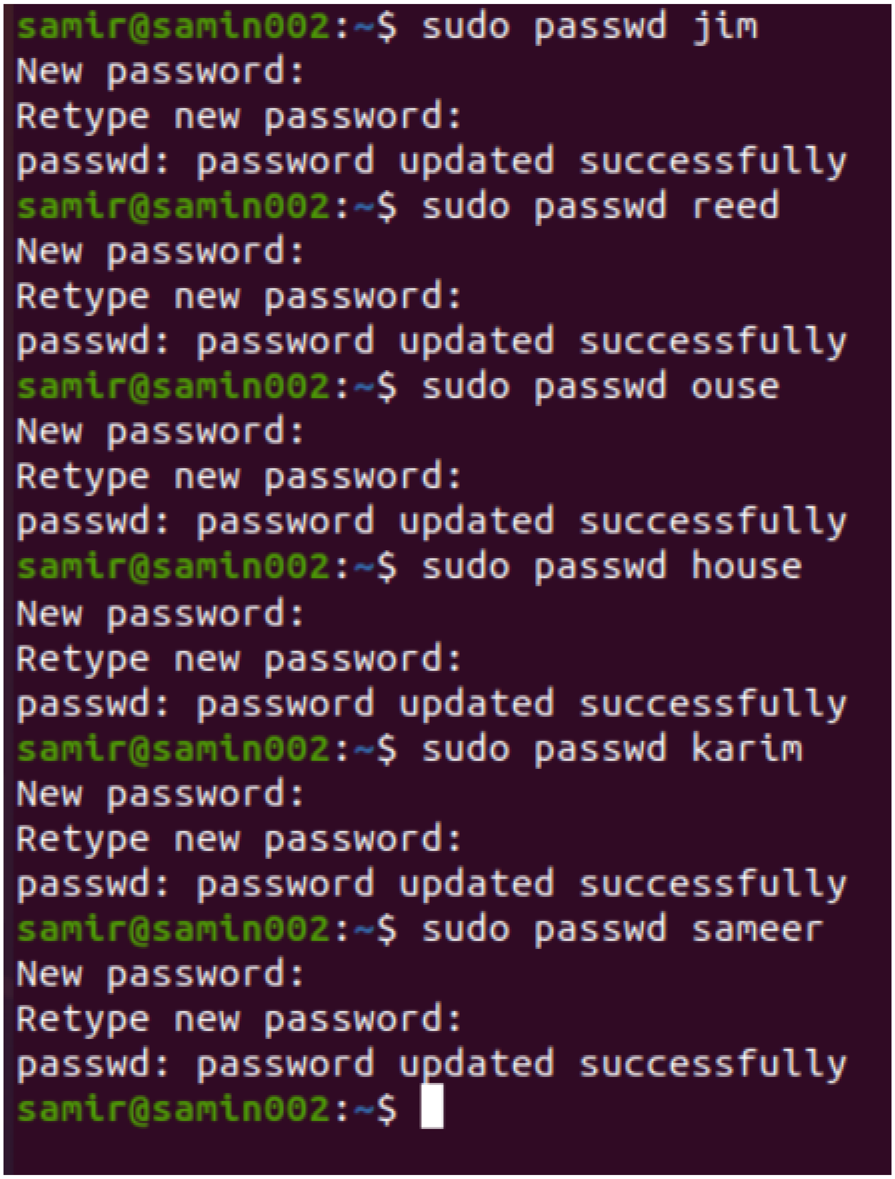
Password Security Assessment with John-the-Ripper

Step One (Create Users):



```
samir@samin002:~$ sudo useradd jim
[sudo] password for samir:
samir@samin002:~$ sudo useradd reed
samir@samin002:~$ sudo useradd ouse
samir@samin002:~$ sudo useradd house
samir@samin002:~$ sudo useradd karim
samir@samin002:~$ sudo useradd sameer
```

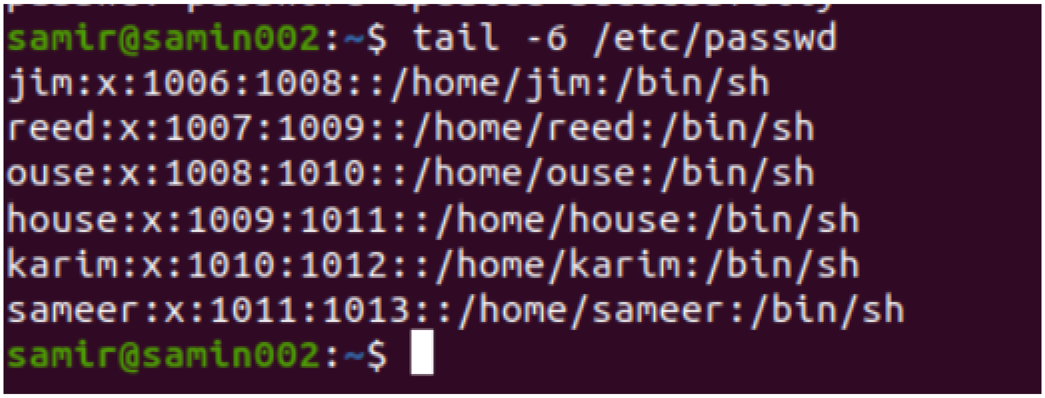
Step Two (Create Passwords):



```
samir@samin002:~$ sudo passwd jim
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ sudo passwd reed
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ sudo passwd ouse
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ sudo passwd house
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ sudo passwd karim
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ sudo passwd sameer
New password:
Retype new password:
passwd: password updated successfully
samir@samin002:~$ 
```

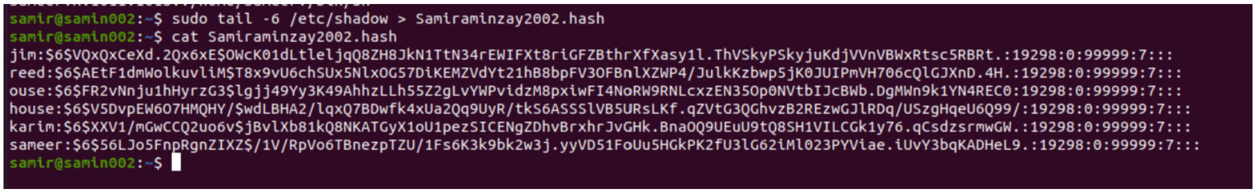
Step Three (Hash Function):

Password Security Assessment with John-the-Ripper



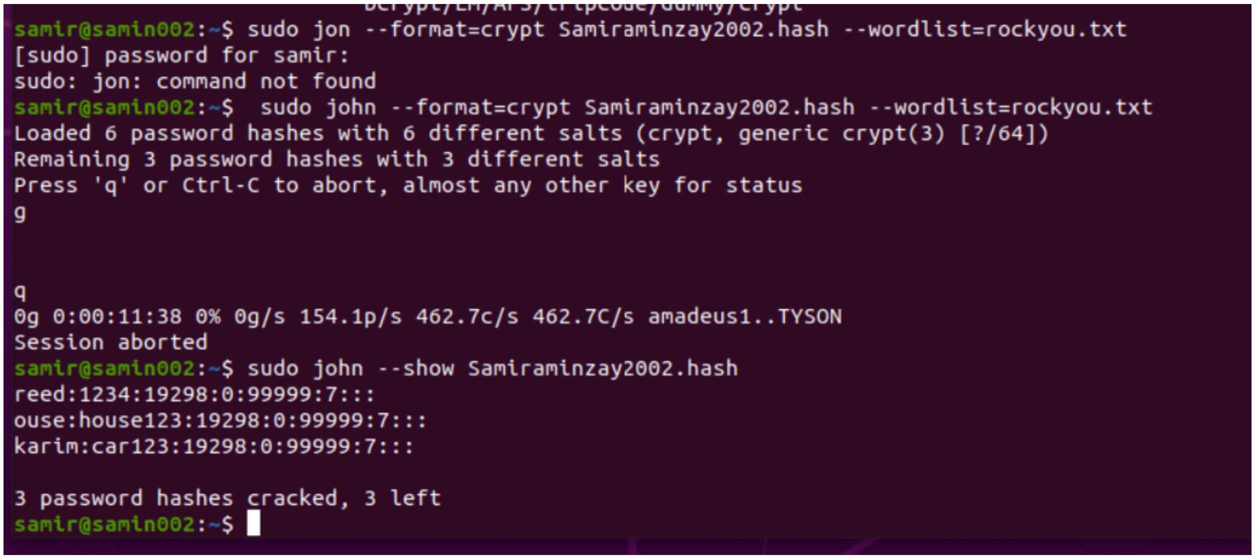
```
samir@samin002:~$ tail -6 /etc/passwd
jim:x:1006:1008::/home/jim:/bin/sh
reed:x:1007:1009::/home/reed:/bin/sh
ouse:x:1008:1010::/home/ouse:/bin/sh
house:x:1009:1011::/home/house:/bin/sh
karim:x:1010:1012::/home/karim:/bin/sh
sameer:x:1011:1013::/home/sameer:/bin/sh
samir@samin002:~$ 
```

Step Four (Hash Function):



```
samir@samin002:~$ sudo tail -6 /etc/shadow > Samiraminzay2002.hash
samir@samin002:~$ cat Samiraminzay2002.hash
jim:$6$VQxQxCeXd.2Qx6xE$OWcK01dLtleljqQ8ZH8JkN1TtN34rEWIFXt8riGFZBthrXfXasy1l.ThVSkyPSkyjuKdjVVnVBWxRtsc5RBRt.:19298:0:99999:7:::
reed:$6$AEtF1dmWolkuvliM$T8x9vU6chSUx5NlxOG57DiKEMZVdYt21hB8bpFV3OFBnlXZWP4/JulkKzbwp5jK0JUIPmVH706cQlGJXnD.4H.:19298:0:99999:7:::
ouse:$6$FR2vNnju1hHyrzG3$lgjj49Yy3K49AhhzLLh55Z2gLvYWPvidzM8pxiwFI4NoRW9RNLcxzEN35Op0NVtbIJcBWb.DgMWn9k1YN4REC0:19298:0:99999:7:::
house:$6$V5DvpEW6O7HMQHY/$wdLBHA2/lqxQ7BDwfk4xUa2Qq9UyR/tkS6ASSSlVB5URsLKf.qZVtG3QGhvzB2REzwGJlRDq/USzgHqeU6Q99/:19298:0:99999:7:::
karim:$6$XXV1/mGwCCQ2uo6v$jBvlXb81kQ8NKATGyX1oU1pezSICENgZDhvBrxhrJvGHk.BnaOQ9UEuU9tQ8SH1VILCGk1y76.qCsdzsrmwGW.:19298:0:99999:7:::
sameer:$6$56LJo5FnpRgnZIXZ$/1V/RpVo6TBnezpTZU/1Fs6K3k9bk2w3j.yyVD51FoUu5HGkPK2fU3lG62iMl023PYViae.iUvY3bqKADHeL9.:19298:0:99999:7:::
samir@samin002:~$ 
```

Step Five (Passwords Hacked):



```
samir@samin002:~$ sudo jon --format=crypt Samiraminzay2002.hash --wordlist=rockyou.txt
[sudo] password for samir:
sudo: jon: command not found
samir@samin002:~$  sudo john --format=crypt Samiraminzay2002.hash --wordlist=rockyou.txt
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Remaining 3 password hashes with 3 different salts
Press 'q' or Ctrl-C to abort, almost any other key for status
g


q
0g 0:00:11:38 0% 0g/s 154.1p/s 462.7c/s 462.7C/s amadeus1..TYSON
Session aborted
samir@samin002:~$ sudo john --show Samiraminzay2002.hash
reed:1234:19298:0:99999:7:::
ouse:house123:19298:0:99999:7:::
karim:car123:19298:0:99999:7:::

3 password hashes cracked, 3 left
samir@samin002:~$ 
```