Lab – Password Cracking

Objectives

Use a password cracking tool to recover a user's password.

Background / Scenario

There are four user accounts, Alice, Bob, Eve, and Eric, on a Linux system. You will recover these passwords using John the Ripper, an open source password cracking tool.

Required Resources

- PC with Ubuntu 16.04 Desktop LTS installed in a VirtualBox or VMware virtual machine.

Step 1: Open a terminal window in Ubuntu.

a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

b. Click on the terminal icon to open terminal.

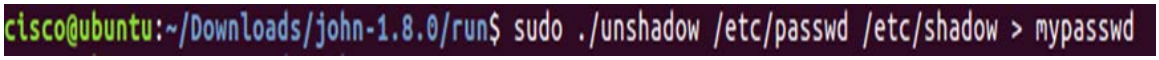
Step 2: Run John the Ripper.

a. At the command prompt, enter the following command to change to the directory where John the Ripper is located:

```
cisco@ubuntu:~$ cd ~/Downloads/john-1.8.0/run
```

b. At the command prompt, enter the following command :

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ sudo ./unshadow /etc/passwd
/etc/shadow > mypasswd
```

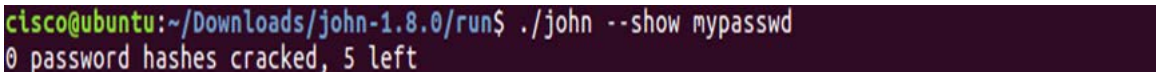


This command will combine the /etc/passwd file where user accounts are stored, with the /etc/shadow file where user passwords are stored, into a new file called “mypasswd”.

Step 3: Recover Passwords.

a. Type the following command in terminal:

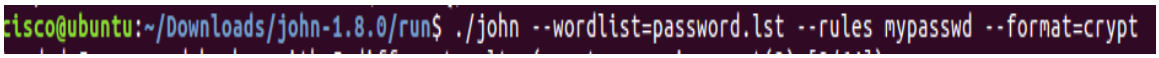
```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```



As shown above, there are no cracked passwords at this point.

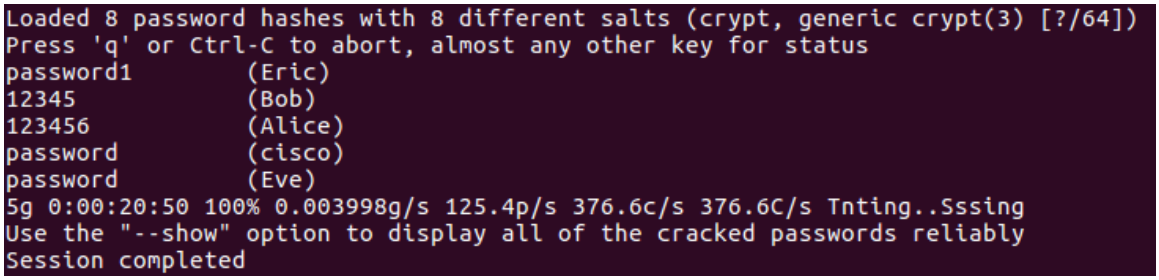
b. At the command prompt, enter the following command:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst --
rules mypasswd --format=crypt
```



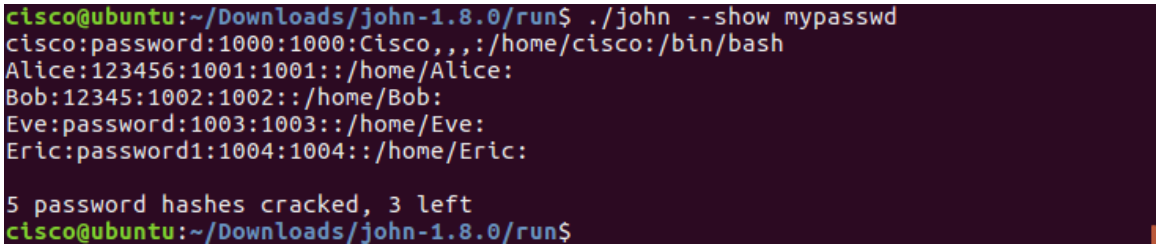
The program, John the Ripper, uses a predefined dictionary called **password.lst** with a standard set of predefined “rules” for handling the dictionary and retrieves all password hashes of both md5crypt and crypt type.

The results below display the passwords for each account.



c. At the command prompt, enter the following command:

```
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --show mypasswd
```



How many passwords were cracked?

References

John the Ripper: http://www.openwall.com/john/