Lab - Recover Passwords

Objectives

- Use a tool to recover user passwords.
- Change a user password to a stronger password.

Background / Scenario

There are four user accounts, Alice, Bob, Eve, and Eric, on a Linux system. There is also the superuser account cisco. The user accounts in the VM are not meant to be secure as the VM is sandbox environment and is not meant for real world applications. In this lab, you will use John the Ripper, an open source password recovery tool, to recover the passwords for all five accounts.

Required Resources

PC with the **CSE-LABVM** installed in VirtualBox

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

b. Double-click the **Terminal** icon to open a terminal.

Step 2: Combine passwords and usernames into one text file.

a. Enter the following command to change to the directory where John the Ripper is located:

```
cisco@labvm:~$ cd Downloads/john/run
cisco@labvm:~/Downloads/john/run$
```

b. Use the **unshadow** command to 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**. Enter **password** as the superuser password, if requested. The syntax for the **unshadow** command is as follows:

```
cisco@labvm:~/Downloads/john/run$ sudo ./unshadow /etc/passwd /etc/shadow > mypasswd
[sudo] password for cisco: password
cisco@labvm:~/Downloads/john/run$
```

Step 3: Run John the Ripper to recover the passwords.

a. To see that the passwords are not yet recovered (cracked), enter the command **./john --show mypasswd**.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
Created directory: /home/cisco/.john
0 password hashes cracked, 5 left
cisco@labvm:~/Downloads/john/run$
```

b. 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. At

the command prompt, enter the following command to recover the passwords stored in the **mypasswd** file.

```
cisco@labvm:~/Downloads/john/run$ ./john --wordlist=password.lst --rules
mypasswd --format=crypt
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (Eric)
password         (cisco)
password         (Eve)
12345            (Bob)
123456           (Alice)
5g 0:00:00:00 100% 6.097g/s 117.0p/s 585.3c/s 585.3C/s #CSE course accounts from Lab -
Authentication Authorization Accounting..natasha
Use the "--show" option to display all of the cracked passwords reliably
Session completed
cisco@labvm:~/Downloads/john/run$
```

c. Enter the **./john --show mypasswd** command again to see that the passwords are now cracked.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
cisco:password:900:900:Cybersecurity Analyst,,,:/home/cisco:/bin/bash
Alice:123456:1000:1000::/home/Alice:/bin/bash
Bob:12345:1001:1001::/home/Bob:/bin/bash
Eve:password:1002:1002::/home/Eve:/bin/bash
Eric:password1:1003:1003::/home/Eric:/bin/bash

5 password hashes cracked, 0 left
cisco@labvm:~/Downloads/john/run$
```

Step 4: Change a user password to a stronger version and try to recover it.

a. Create your own strong password or use an online password generator to create one.

b. Find an online "password strength checker" to test the strength of your password. Your password should take at least thousands of years to crack.

c. Use your superuser privileges to change Eric's password from **password1** to the value for your new strong password. Make sure you get the "password updated successfully" message.

```
cisco@labvm:~/Downloads/john/run$ sudo passwd Eric
[sudo] password for cisco: password
New password: <your_new_strong_password>
Retype new password: <your_new_strong_password>
passwd: password updated successfully
cisco@labvm:~/Downloads/john/run$
```

d. Run **unshadow**, and then **john** again to see if you can crack Eric's password. If you changed Eric's password to one that is strong enough to take thousands of years to crack, you will be waiting a long time. When you are done waiting, enter **q** or **Ctrl+C** to stop John the Ripper.

```
cisco@labvm:~/Downloads/john/run$ ./john --wordlist=password.lst --rules
mypasswd --format=crypt
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Remaining 1 password hash
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
0g 0:00:00:17 7% 0g/s 599.6p/s 599.6c/s 599.6C/s reddog1..mark1
Session aborted
```

e. Enter the **./john --show mypasswd** command to see that only four passwords are cracked and one is left.

```
cisco@labvm:~/Downloads/john/run$ ./john --show mypasswd
cisco:password:900:900:Cybersecurity Analyst,,,:/home/cisco:/bin/bash
Alice:123456:1000:1000::/home/Alice:/bin/bash
Bob:12345:1001:1001::/home/Bob:/bin/bash
Eve:password:1002:1002::/home/Eve:/bin/bash

4 password hashes cracked, 1 left
cisco@labvm:~/Downloads/john/run$
```