UTSA
The University of Texas at San Antonio™

Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques

Lab 3 – Password Cracking

Lab Description and Instructions:
We learn how to use John the Ripper to check the password security of different users on the local system (Kali VM). To do so, we will first create three users and setup their passwords using the following interactive command in the Terminal:

`sudo adduser username` (replace username with unique names)

Next, we will combine the *passwd* file and *shadow* file in to a single *mypassword* file using the following command in the Terminal:

```
sudo unshadow /etc/passwd /etc/shadow > mypassword
```

You can view the usernames and hashed passwords in the *mypassword* file using this command:

```
cat mypassword
```

Next, we will use John the Ripper (or *john*) to try and crack the hashed password, only for the newly created users, using this command:

```
john mypasswords --users=username1,username2,username3
```
(replace usernames with the ones created earlier)

John the Ripper starts the password cracking attack and displays recovered passwords in the Terminal. It starts off using a dictionary (wordlist) based attack and follows up by a brute-force attempt in case one or more passwords in the *mypassword* file were not found in the dictionary. While we can create our own dictionary, John the Ripper provides a wordlist of commonly used passwords that we will be using. This wordlist is located in /usr/share/john/password.lst and can be viewed in the Terminal as follows:

```
cat /usr/share/john/password.lst
```

Troubleshooting:
John the Ripper remembers certain metadata on prior password cracking attempts. If you are trying multiple times to crack your *mypassword* file, it may be helpful to delete this metadata using the following command:

```
rm ~/.john/ -R
```

Homework:
Try all the above steps in your VM with varying passwords, and try to compile and use your own wordlist. Here is a tutorial on how to create custom wordlists: https://netsec.ws/?p=457