Cybersecurity 701

Passwords Lab

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Passwords Materials

- Description of the lab
- Materials needed
  - Kali Linux Machine
- Software Tools used
  - Leafpad

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
    - Password attacks

Password Lab Overview

1. Set up Environment
2. Navigate to Shadow
3. Exploring the Kali Password
4. Creating a User
5. Creating a Password
6. Moving the Password
7. Testing the Password
8. On Your Own Activity

Set up Environment

- Log into the cyber range
- Open the Kali Linux Environment
  - You should be on your Kali Linux Desktop
  - Open the Terminal

Navigate to Shadow

- Make yourself the root user:

  `sudo su -`

- Change directory to the etc folder:

  `cd /etc/`

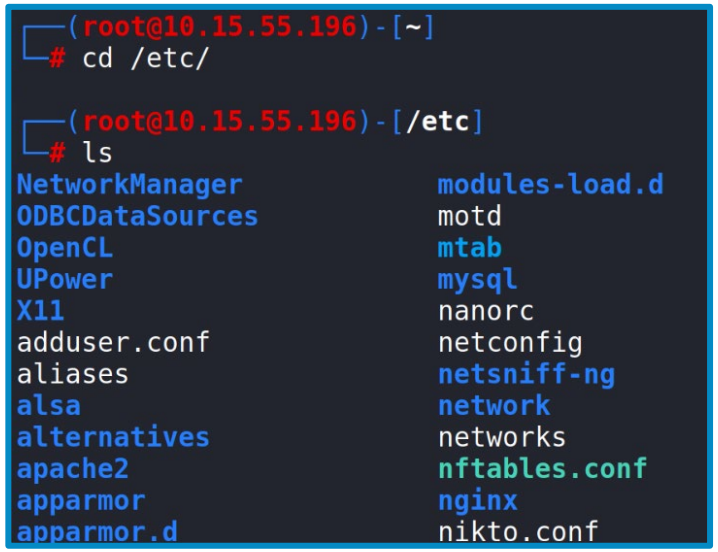
- Display all the directories within /etc:

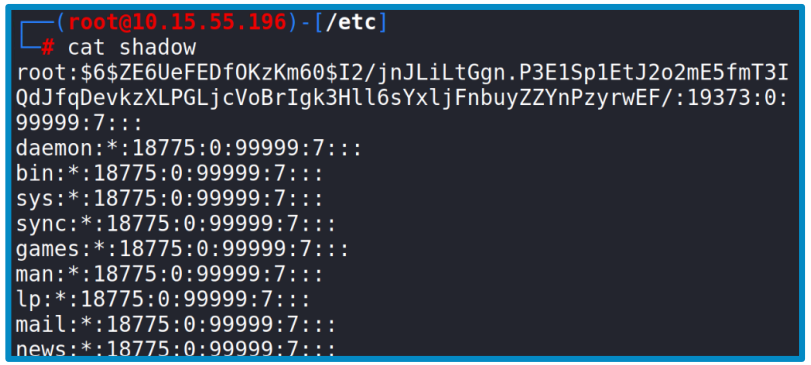
  `ls`

  - You should be able to see the shadow file

- Read the Shadow file where the passwords are stored:

  `cat shadow`





Notice that the users root and kali have passwords stored

Exploring the Kali Password

- Take a look at the kali password*
  - Remember, “password” is the password*

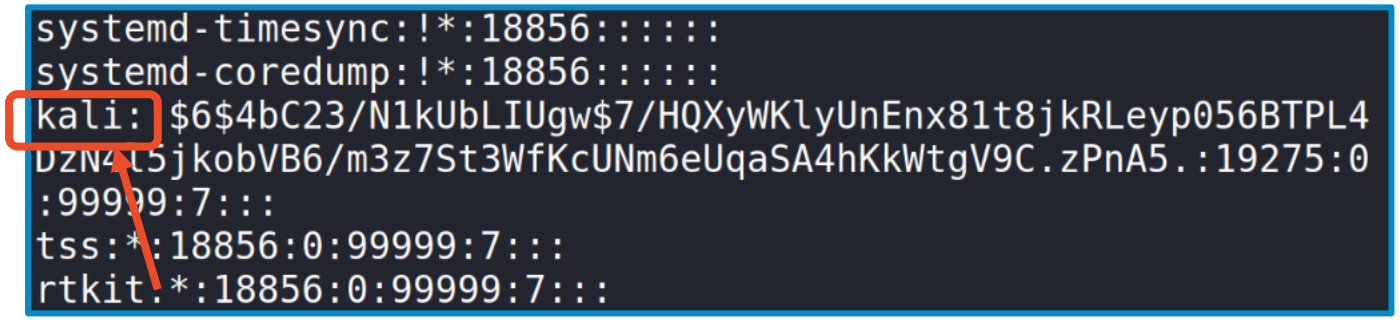
```
systemd-timesync:!*:18856::::::
systemd-coredump:!*:18856::::::
kali:!$6$4bC23/N1kUbLIUgw$7/HQXyWKlyUnEnx81t8jkRLeyp056BTPL4
DzN4l5jkobVB6/m3z7St3WfKcUNm6eUqaSA4hKkWtqV9C.zPnA5.:19275:0
:99999:7:::
tss:*:18856:0:99999:7:::
rtkit:*:18856:0:99999:7:::
```

What does all this mean?

*Please Note: The username/password combination can differ depending on the range/environment you are using

Exploring the Kali Password

- Take a look at the kali password
  - Remember, “password” is the password



The user’s name

Exploring the Kali Password

- Take a look at the kali password
  - Remember, “password” is the password

```
systemd-timesync:!*:18856::::::
systemd-coredump:!*:18856::::::
kali: $6$4bC23/N1kUbLIUgw$7/HQXyWKlyUnEnx81t8jkRLeyp056BTPL4
DzN4l5jkobVB6/m3z7St3WfKcUNm6eUqaSA4hKkWtgV9C.zPnA5.:19275:0
:99999:7:::
tss:*:18856:0:99999:7:::
rtkit:*:18856:0:99999:7:::
```

The Hash Algorithm
(Here it is 6, thus using SHA-512 Algorithm)

1 → MD5

2 → Blowfish

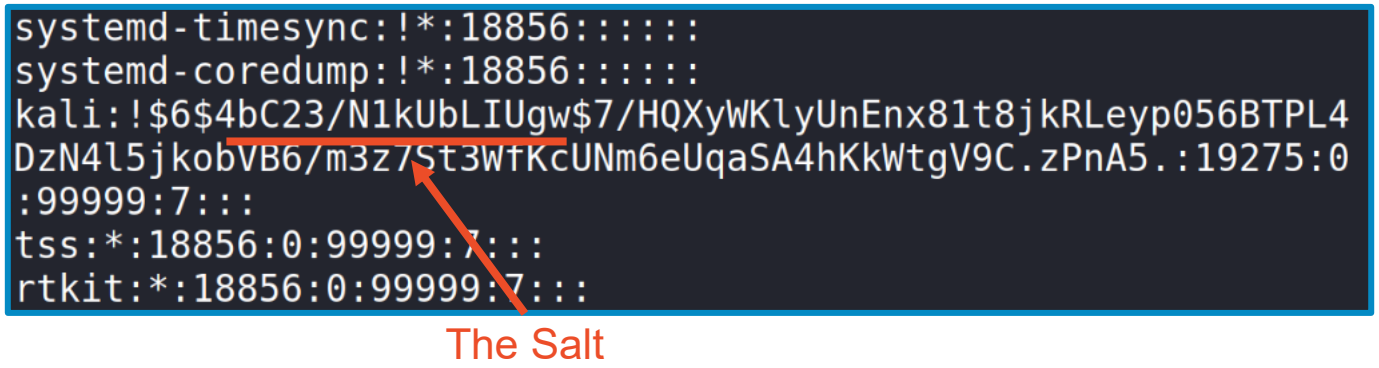
$2a$ → ekaBlowfish

5 → SHA-256

6 → SHA-512

Exploring the Kali Password

- Take a look at the kali password
  - Remember, “password” is the password



What is the purpose of a salt? Why is this important for security?

Exploring the Kali Password

- Take a look at the kali password
  - Remember, “password” is the password

```
systemd-timesync:!*:18856::::::
systemd-coredump:!*:18856::::::
kali:!$6$4bC23/N1kUbLIUgw$7/HQXyWKlyUnEnx81t8jkRLeyp056BTPL4
DzN4l5jkobVB6/m3z7St3WfKcUNm6eUqaSA4hKkWtgV9C.zPnA5.:19275:0
:99999:7:::
tss:*:18856:0:99999:7:::
rtkit:*:18856:0:99999:7:::
```

The Hashed Password

What is a hashed password and why are passwords stored like this?

Exploring the Kali Password

```
systemd-timesync:!*:18856::::::
systemd-coredump:!*:18856::::::
kali:!$6$4bC23/N1kUbLIUgw$7/HQXyWKlyUnEnx81t8jkRLeyp056BTPL4
DzN4l5jkobVB6/m3z7St3WfKcUNm6eUqaSA4hKkWtgV9C.zPnA5.:19275:0
:99999:7:::
tss:*:18856:0:99999:7:::
rtkit:*:18856:0:99999:7:::
```

- Thus, passwords are stored in the following format:

  username: $hash number$salt$hashed password:

- Kali has the following data:
  - username = kali
  - Hash Algorithm = 6 or SHA-512
  - Salt is ‘4bC23/N1kUbLIUgw’
  - Hash is ‘7/HQXyWKlyUnEnx81t8jkRLeyp056BTPL4DzN4l5jkobVB6/m3z7St3WfKcUNm6eUqaSA4hKkWtgV9C.zPnA5.’
  - Plaintext password is ‘password’

Creating a User

- Create a new user with the same hash and password as ‘kali’
- Create a new user:
  - **useradd johnsmith**
- Now, check out johnsmith’s data:
  - **cat shadow**
- Notice, that johnsmith has a “!” where the password should be stored

```
┌──(root@10.15.55.196)-[/etc]
└─# useradd johnsmith

┌──(root@10.15.55.196)-[/etc]
└─# cat shadow
root:$6$ZE6UeFEDfOKzKm60$I2/jnJLiLtGgn.P3E1Sp1EtJ
LPGLjcVoBrIgk3Hll6sYxljFnbuyZZYnPzyrwEF/:19373:0:
daemon:*:18775:0:99999:7:::
bin:*:18775:0:99999:7:::
```

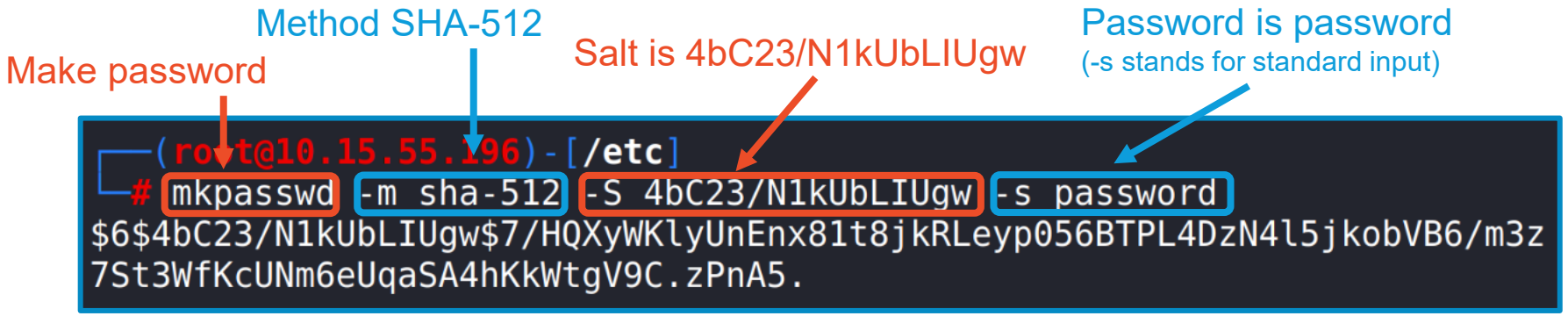
No stored password

```
colord:*:18856:0:99999:7:::
nm-openconnect:*:18856:0:99999:7:::
johnsmith:!:19543:0:99999:7:::
```

Creating a Password

- Use the following command to make the same password as the kali account:

mkpasswd -m sha-512 -S *<YOUR SALT>* -s password



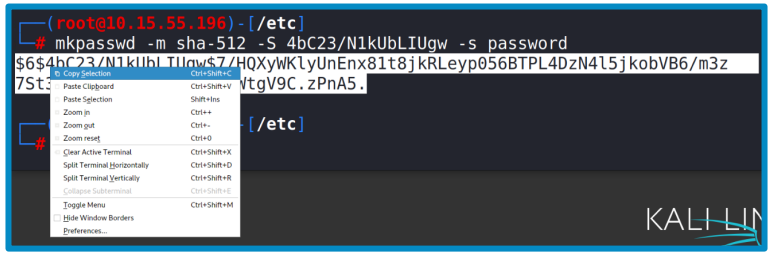
Notice, the password created is the same as the original user

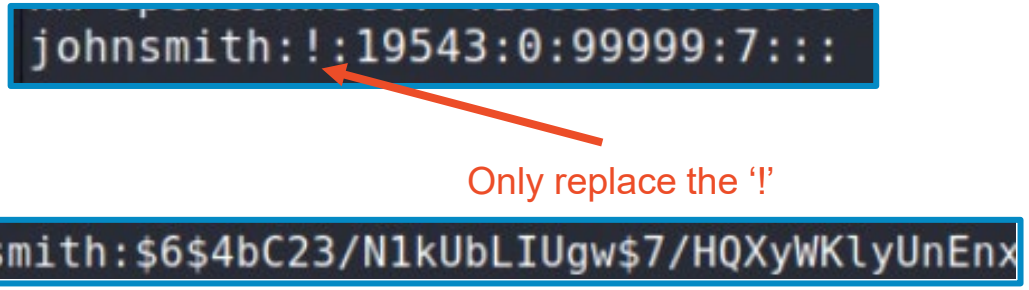
Moving the Password

- Highlight the entire password
- Right-click, and select “copy selection”
- Open shadow in Leafpad:

  `leafpad shadow`

- Navigate to user johnsmith
- Delete the exclamation mark
- Paste in the password
- Save and exit Leafpad!



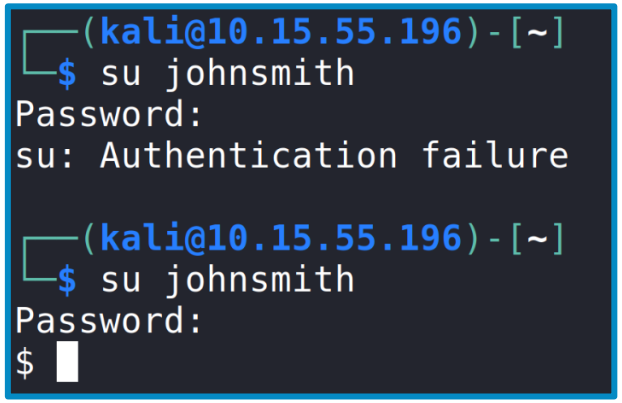


Please Note: If Leafpad is not able to open the display while logged in as the root user, use the following command to open the text in the nano editor:

`nano shadow`

Test the password

- Open a new Terminal (should not be root access)
- Switch user to johnsmith:
  - **`su johnsmith`**
- When prompted, enter the wrong password
  - Do not type in ‘password’
- You should see “Authentication failure”
- Switch user to johnsmith:
  - **`su johnsmith`**
- Now type in ‘password’ as the password
  - You should notice that it gave you access to johnsmith account!



On Your Own Activity

- Try and make passwords for the following:
  1. Create your own SHA-512 password with a different salt
  2. A different password using MD5 Algorithm (-m md5)
  3. Another password using SHA-256 Algorithm (-m SHA-256)
- Here was the command we used to create the kali password:

```
mkpasswd -m sha-512 -S 4bC23/N1kUbLIUgw -s password
```

- Remember to check to make sure the password works!