SECURITY DESIGN PRINCIPLES

MINIMIZE SECRETS

CRACKIN' PASSWORDS

Students will utilize John the Ripper on a Kali VM to demonstrate what cracking passwords actually looks like. The default username and password for the Kali VM should be "root" and "toor," respectively.

There's so many programs out there to get into your system. Once they're in, there's even more programs to get your data. That's why it's important to keep your amount of secrets to a minimum for when you get compromised. It's no fun changing 20 different secrets when a few would've done the trick.

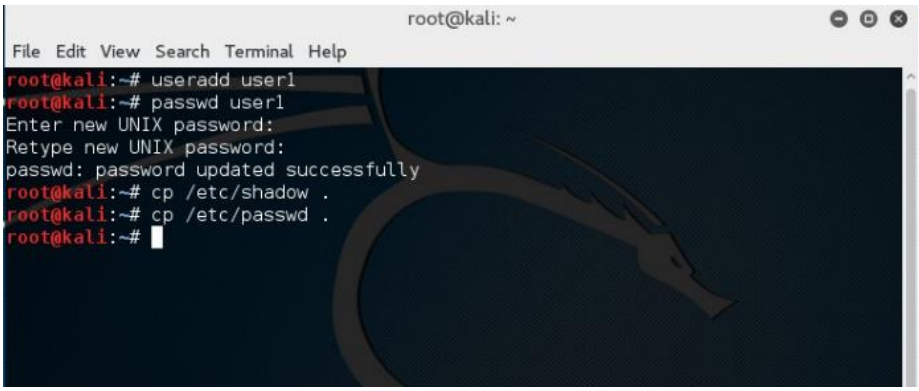
STEP 1

Open the Kali VM and log in.

STEP 2

Open a terminal. Type these commands to unzip the wordlist we will be using.

- cp /usr/share/wordlists/rockyou.txt.gz .
- gunzip rockyou.txt



STEP 3

Now add some users by typing these commands. (Note, the passwords will not show up when you are typing them)

- useradd user1
- passwd user1
    - flower
    - flower
- useradd user2
- passwd user2
    - 12345
    - 12345
- useradd rmolt
- passwd rmolt
    - duke
    - duke
- useradd guest
- passwd guest
    - password123
    - password123

STEP 4

Let's copy the files we need into our home directory:

- cp /etc/shadow .
- cp /etc/passwd .

STEP 5

Now for the fun part: John the Ripper! Enter this command:

- john shadow
    - hit enter whenever you want to see the status of john
    - watch and enjoy

STEP 6

To quit, hit q then type:

- john shadow --show

- this will show you the usernames and passwords john has cracked so far

QUESTIONS

- What operating system is this?
- What is held in the file /etc/passwd?
- What is held in the file /etc/shadow?
- What does john the ripper do?

WHAT TO SUBMIT

Submit your answers in a word document.