Cyberpaths

- CTF Password Lab -

Lab Goals

1. Apply different decryption techniques.

2. Understand encryption concepts such as symmetric key encryption.

3. Use pivot machines and learn what these are.

Quick introduction to CTFs and Passwords

Capture The Flag (CTF) is a common cyber security competition format where participants have to find a secret or vulnerability or error (flag) that is hidden in a file, website, log, etc. CTFs questions are asking for short answers, often single word. This exercise simulates a CTF experience. Although you are only competing with yourself, this will be a “detective” style exercise to reveal the secrets of four users, Alice, Bob, Carol, and David. Alice is not security conscious at all! She saves passwords unsafely. Bob is a little more security aware; he still saves passwords unsafely, but not plainly as Alice. Carol is pretty aware of security, her passwords are saved in a safe manner, however they can be cracked because Carol puts convenience to memorize a password above all! Finally, David is very security aware. He saves his passwords securely and they are hard to guess!

Prerequisites

1. Basic cryptography: Khan academy has a great class on cryptography and these ciphers that can be found here

2. Passwords and how these should be stored: You can find a lot of examples about building strong passwords. We also recommend that you try to measure some of your password strength by using this tool.

3. Hashing: Here is an interesting video from khan academy on hash functions.

4. How not to store a password

5. Password cracking

6. Some tools that will be useful in this lab:

   - Rumkin Cipher Tools
   - CrackStation Hash Cracker

Part 1: Setting up the topology

1. Use the provided RSpec

2. (ON ALL MACHINES)Run the following commands:

   - Wait some time to allow background installations to finish once nodes are set up.

  - The terminal window should halt after running the script. Just close it and open another terminal for each node.

```
sudo python /local/setup.py
```

Part 2: The Mission: Snoop around

Your mission is to find Alice’s, Bob’s, Carol’s, and David’s password.

1. First you will use a pivot machine with the password

```
su pivot
Password: …
```

We assume that the pivot machine has already been compromised either with social engineering or with a password cracking tool, such as hydra.

2. What is a pivot machine? It is usually a machine in a target network that may not be an important asset but it is used to “pivot” to other machines that may store important data or are assets for different reasons, i.e., run an important service etc.

3. Look around in the files on the pivot machine. Alice's file is somewhere and it has her password! You can also try weak passwords, one of these may belong to Alice.

4. After you find Alice's password, login to Alice's machine using the command:

```
ssh alice@alice
```

5. Look around in Alice's machine. She has saved Bob's password

somewhere. After you find it, try to crack it. Think about what kind of encryption scheme Bob may be using for his password. You can use one of the recommended sites in the sources to break Bob's password.

6. After you crack Bob's password, login to Bob's machine using the command:

```
ssh bob@bob
```

7. Look around bob's directories. You may need to dig a bit more into Bob's directories to find Carol's password file. After you find it, try to crack it. Keep in mind that Carol is a secure user, so she may have saved her file securely using a one-way hash function. You can use one of the recommended sites in the sources to break Carol's password.

8. After you crack Carol's password, login to Carol's machine using the command:

```
ssh carol@carol
```

9. Look around Carol's directories. You may need to dig deeply to find David's password file. After you find it, try to break it. Keep in mind that David is a secure user, so he may have sent his file securely and saved using a one-way hash function.You can use one of the recommended sites in the sources to break David’s password.

10. You may not be able to break David’s password, unless you use a tool such as hydra or john the ripper. You can find out more about these tools in the attached sources.