Cybersecurity

Dictionary Lab

CYBER.ORG

Dictionary Lab

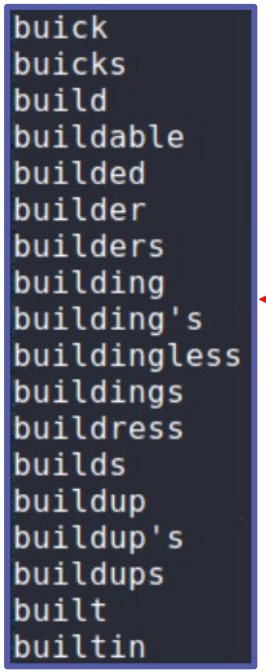
- Materials needed
  - Kali Linux Virtual Machine
- Software Tool used
  - JTR (John the Ripper)
    - Password cracking tool (pre-installed on Kali OS)

Objectives Covered

- Security+ Objectives (SY0-601)
  - Objective 1.2 - Given a scenario, analyze potential indicators to determine the type of attack.
    - Password Attacks
      - Dictionary
  - Objective 4.1 - Given a scenario, use the appropriate tool to assess organizational security.
    - Password crackers

What is a Dictionary Attack?

- A dictionary attack is a form of password attack where the attacker uses a pre-determined list of passwords, or dictionary, to attempt to crack a password.



This is part of the contents of a dictionary list pre-installed on most Kali systems. It can be found at the following directory:

/usr/share/ike-scan/

The Dictionary Lab

- Setup Environment
- Create dictionary
- Create example users
- Set example passwords
- Locate password file
- Launch the Attack
- Observe results

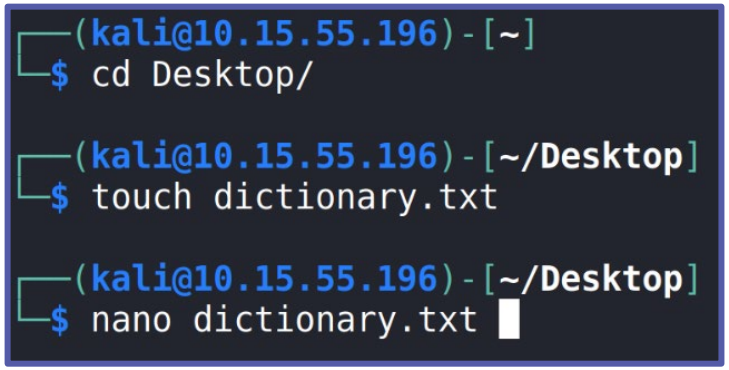
Note: In this lab, you are going to create a dictionary of passwords that contains a list of names of people that you know.

From that list, you will create users with passwords that are contained within the dictionary.

Setup Environment

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

Create the Dictionary



- Open Terminal in Kali
- Navigate to the Desktop:

  `cd Desktop`
- Create a **.txt** file that will serve as the dictionary:

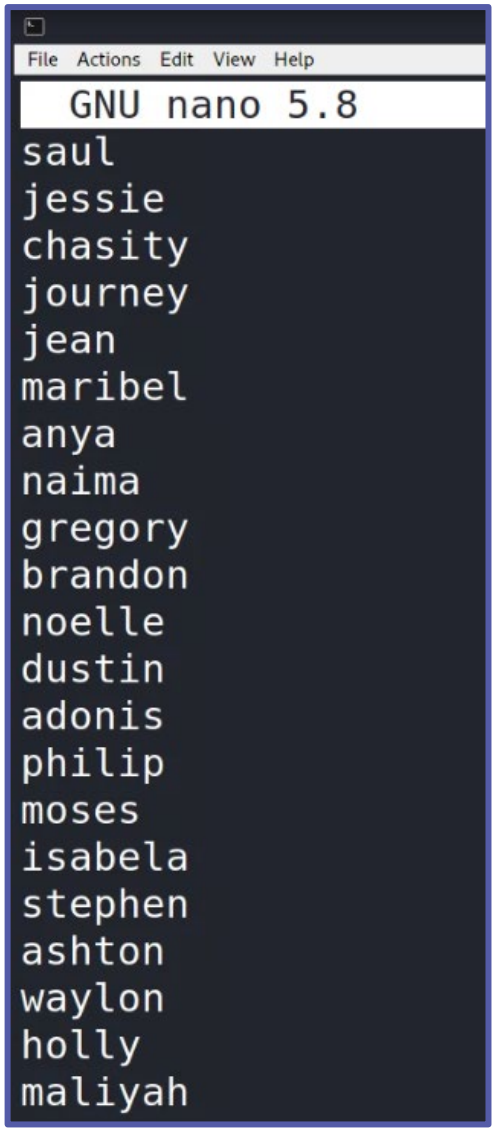
  `touch dictionary.txt`
- Open the dictionary file with a text editor

  `nano dictionary.txt`

Creating the Dictionary

- In the text editor, add a list of 20 names of people you know, just like the example on the right
- Once finished, press **CTRL+X** to exit
- Press **Y** to save
- Press **ENTER** to save as the same name (**dictionary.txt**)

You can ensure the names are saved in the file by double clicking to open the file on the Desktop.



Create Users

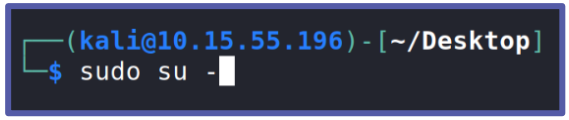
- Login as the root user with the following command:

  `sudo su -`

- Notice the command prompt is now **root@kali**
- Create additional users by using the following command:
  - This command creates a user named “ginny”

    `useradd ginny`

- Create at least 3 users
- Remember the users' names - you will need these to set passwords for them



Set passwords

- Use the following command to set a password for each account:
  - The following command starts the prompt to set a password for the user ginny

    `passwd ginny`
- Enter the password at the prompt "New password:"
  - Set the password to be one from the list of the names you added to the dictionary file earlier!
- Repeat this step for all user accounts you created.

```
┌──(root@10.15.55.196)-[~]
└─# passwd ginny
New password:
Retype new password:
passwd: password updated successfully
```

Locate Hashed Passwords

- Navigate to the **`etc`** directory:
  `cd /etc`
- View the files
  `ls`
- The file **`passwd`** contains all the usernames on the system (See the accounts you created?)
- In older systems, the password for each user was stored in the **`passwd`** file (That's why it's named that)
  - NOT a secure way of storing passwords!

```
passwd
passwd-
```

Locate Hashed Passwords

- Linux switched over to hashing passwords and storing them in a file named **shadow**
- Use the following command to see the hashed passwords in the **shadow** file:

  cat shadow

- Copy the **shadow** file to your Desktop using the following command:

  cp shadow /home/kali/Desktop

You should have both the **dictionary.txt** file and **shadow** file on your Desktop

Launch the Attack

- Navigate to the Desktop directory:

  `cd /home/kali/Desktop`

- To launch the attack with the dictionary you created, use the following command:

  `john shadow --wordlist=dictionary.txt`

- You should notice John The Ripper cracked the passwords very quickly using the dictionary that you created.

```
┌──(root@10.15.55.196)-[/home/kali/Desktop]
└─# john shadow --wordlist=dictionary.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha
512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hash
es
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key f
or status
holly            (harry)
saul             (ginny)
jessie           (ron)
3g 0:00:00:00 DONE (2023-07-05 16:25) 10.00g/s 70.00
p/s 350.0c/s 350.0C/s saul..maliyah
Use the "--show" option to display all of the cracke
d passwords reliably
Session completed
```

Please Note: If you see the following message, try the command (all one line). (The brute force offline lab would have had a similar issue)

`john shadow --wordlist=dictionary.txt --format=crypt`

How to Defend Against a Dictionary Attack

- Do not use generic passwords or old passwords
  - Dictionary attacks use commonly-used passwords
  - Dictionary attacks often contain old passwords that make have been compromised in the past
- Strong Passwords
- Increasingly longer delay between failed attempts
- Lockout after __ failed attempts
- Two-Factor Authentication
  - Why would these help secure your password?
- What are some other ways of defending against a dictionary attack?

Real Dictionaries

- Real dictionary attacks use *millions* and *billions* of passwords.
- The dictionary file sizes are enormous because of all the possible combinations they contain.
- Where do these passwords come from?
  - When a cyberattack occurs, the culprits will sometimes leak usernames and passwords online. These are added into a continuously growing list of known passwords and circulated online.
  - A simple Google search will provide plenty of examples that can be used.