**Brute-Force Attack**

**Brute-Force Attack with Hashcat**

A brute-force attack systematically attempts every possible combination of characters to find the correct password. Here’s a step-by-step guide on how to perform a brute-force attack using Hashcat:

**Step 1: Identify the Hash Type**

You need to know the hash type you are trying to crack. Hashcat supports a wide range of hash types, and each has a specific mode identifier. For example, MD5 is 0, SHA-1 is 100, etc.

**Step 2: Prepare Your Hash File**

Create a file containing the hash you want to crack. Let’s assume the file is named hashes.txt and contains a single hash.

**Step 3: Choose a Charset and Mask**

Brute-force attacks require a charset and a mask to define the range of characters and the length of the password.

* A mask defines the pattern of the password:
  + ?l – Lowercase letters
  + ?u – Uppercase letters
  + ?d – Digits
  + ?s – Special characters
  + ?a – All printable ASCII characters

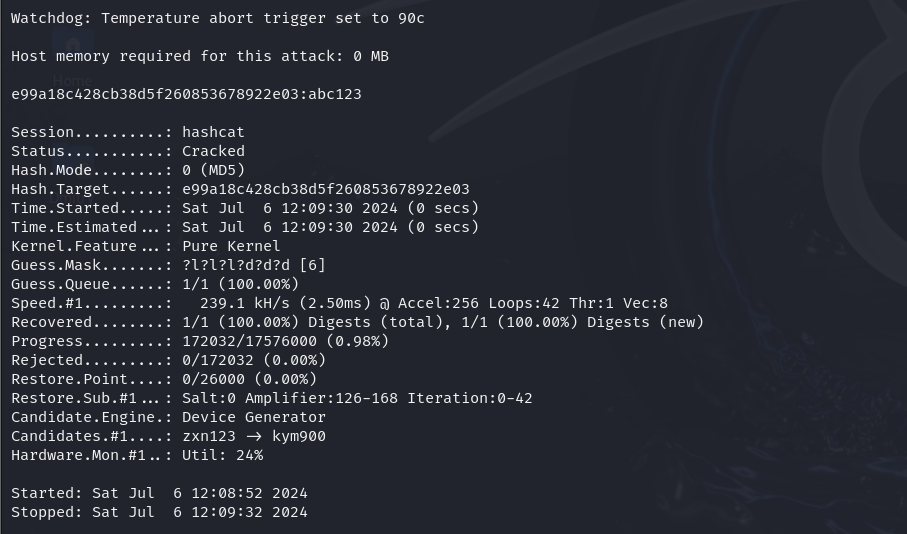
For example, to attempt all combinations of lowercase letters with a length of 4:

* Mask: ?l?l?l?l

**Step 4: Run Hashcat**

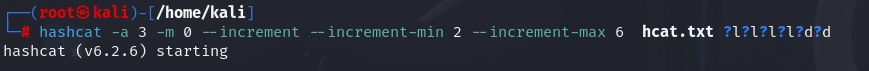
Run Hashcat with the appropriate options. Here’s a basic example:

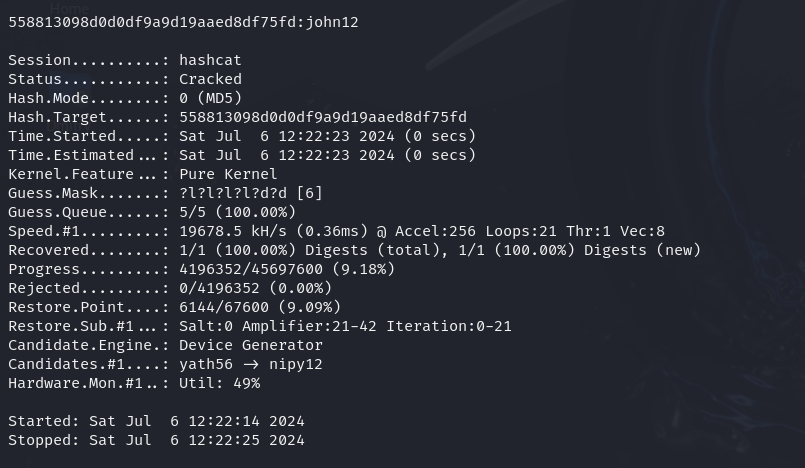
****

****

If you do not know the length of password, we will use increment and set minimum range and maximum range and perform brute-force

**Incremental Mode**: Start with shorter lengths and gradually increase.

****

****

**Using Medusa for Brute-Force Attacks:**

Step 1: Identify the Target

Determine the target service and IP address or hostname you want to brute-force. You will also need a list of usernames and passwords.

Step 2: Prepare Username and Password Lists

Create or obtain files containing possible usernames and passwords. For example:

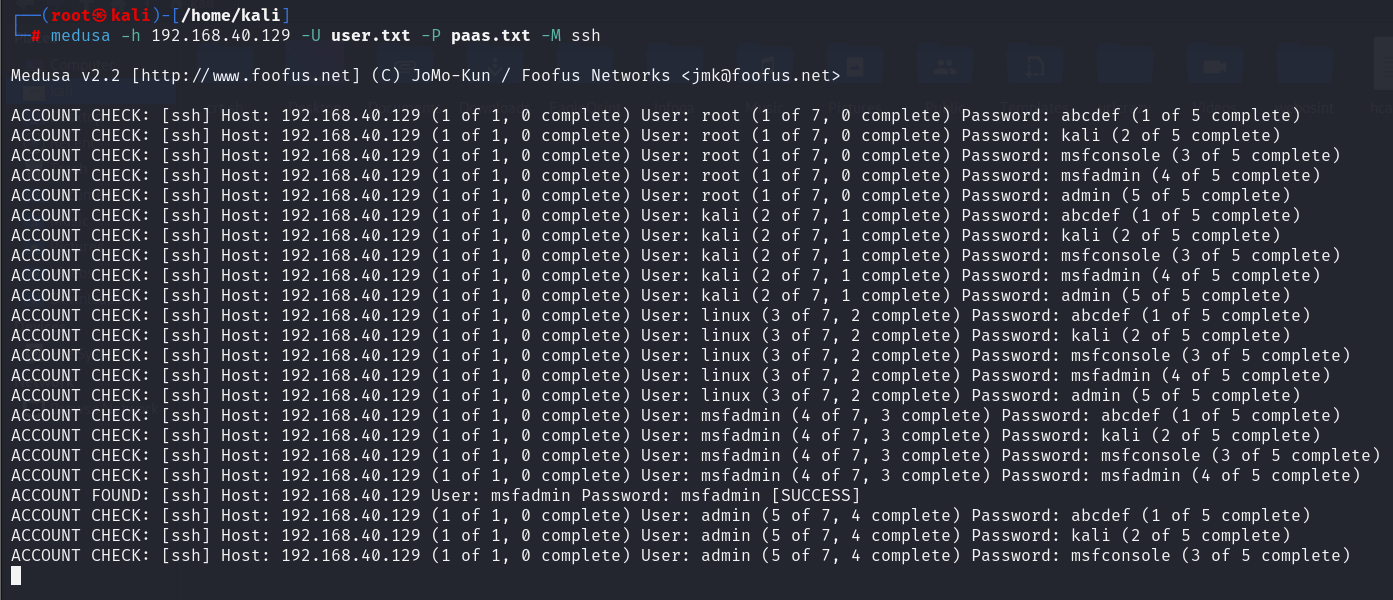
* user.txt
* paas.txt

Step 3: Run Medusa

Run Medusa with the appropriate options to perform the brute-force attack. Here are some examples for different services:

**Example 1: Brute-Forcing SSH**

To brute-force an SSH service on a target IP 192.16840.129:



**FTP Brute Force Attack on a Specific Port**:

**Example 2: Brute-Forcing FTP**

To brute-force an FTP service on a target IP 192.168.40.129:

