**Dictionary Attack**

**Hashcat:**

**Performing a Password Crack with Hashcat**

**Step 1: Identify the Hash Type**

Before you start cracking, we need to identify the type of hash we are dealing with. Common types include MD5, SHA1, SHA256, etc. Tools like hash-identifier or online services can help identify the hash type based on the hash string.

**Step 2: Prepare Your Environment**

1. **Open Terminal or Command Prompt**: Depending on your operating system, open the terminal (Linux/macOS) or command prompt (Windows).
2. **Navigate to Hashcat Directory**: Change to the directory where you extracted Hashcat.

**Step 3: Create a Hash File**

Save the hash we want to crack in a text file. For example, md5.txt. Ensure each hash is on a new line.

**Step 4: Choose Dictionary Attack**: Uses a wordlist to guess the password.

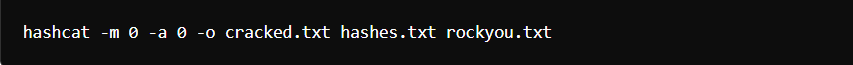
**Step 5: Download or Create a Wordlist**

You can use existing wordlists or create your own. Popular wordlists include:

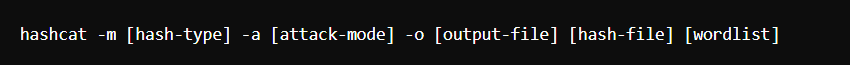
* [Rockyou.txt](https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt)
* [SecLists](https://github.com/danielmiessler/SecLists)

**Step 6: Run Hashcat**

Execute the Hashcat command with the appropriate options. The basic syntax is:



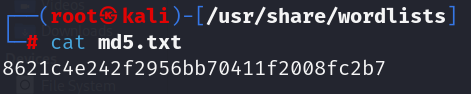
For example, to crack an MD5 hash using a dictionary attack:



* **-m 0**: Specifies the hash type (0 for MD5).
* **-a 0**: Specifies the attack mode (0 for dictionary attack).
* **-o cracked.txt:** Output file for cracked passwords.
* **hashes.txt:** Input file containing hashes.
* **rockyou.txt:** Wordlist to use.

**Dictionary Attack:**

First, we create a hash txt file.

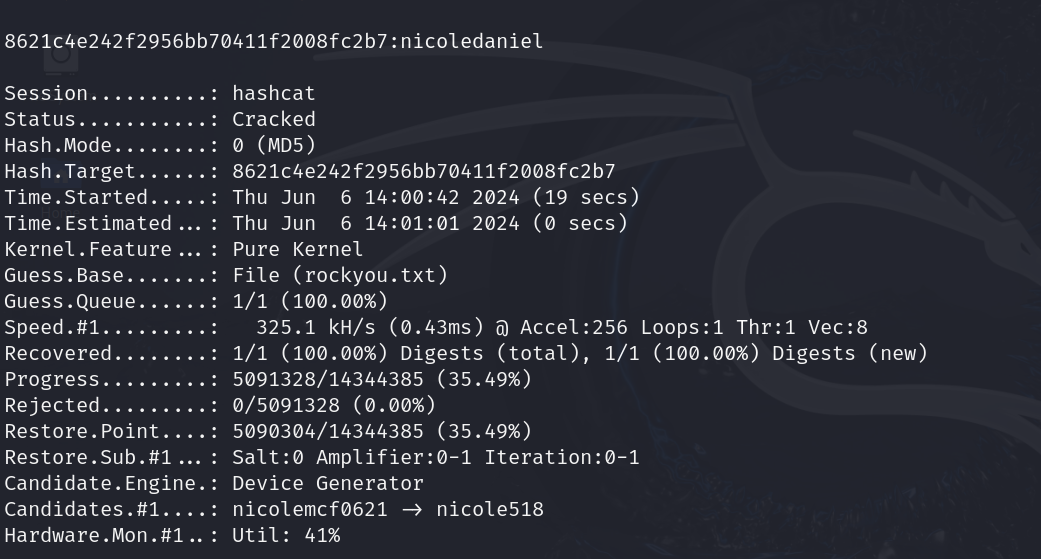


Now we perform hashcat dictionary attack to crack hash:





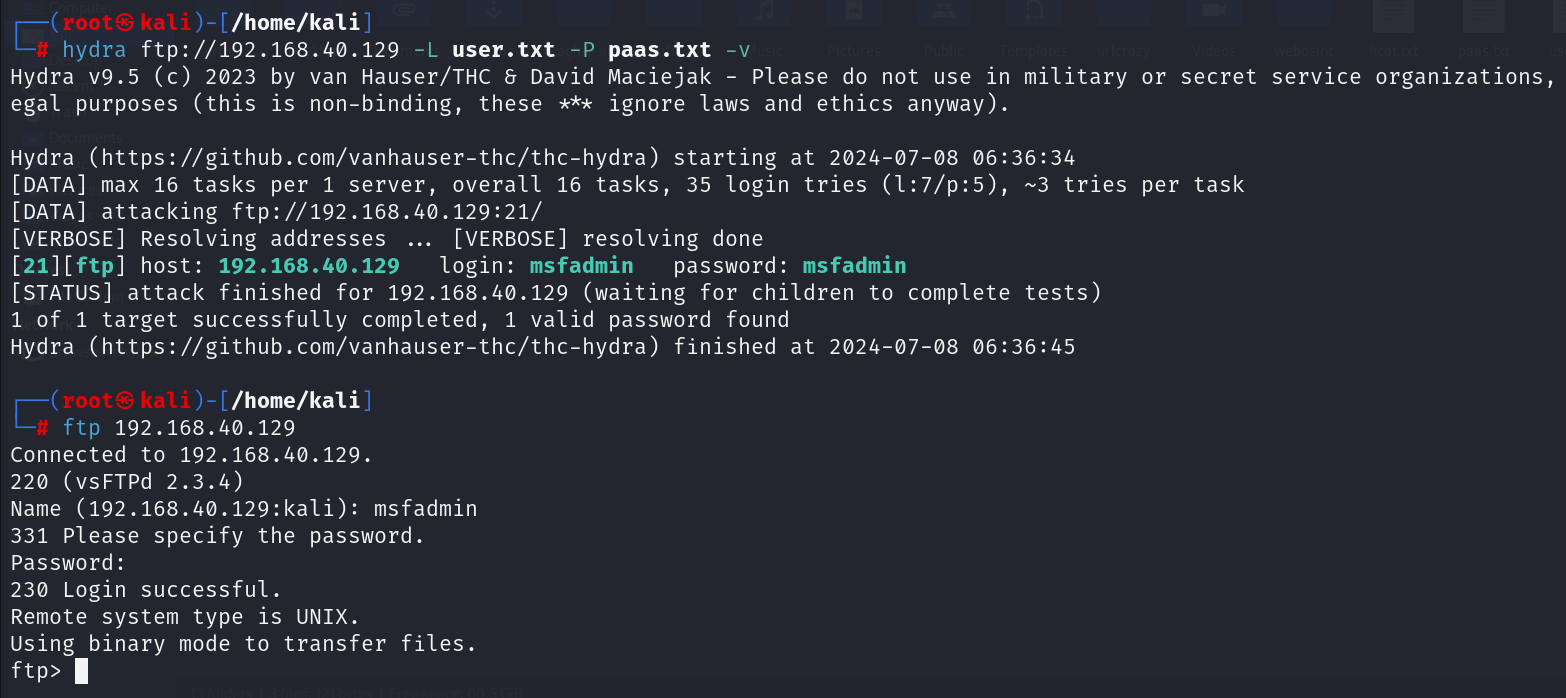




**Hydra:**

Hydra is a very popular tool for performing dictionary attacks on various protocols, including FTP, SSH, HTTP, and many more.

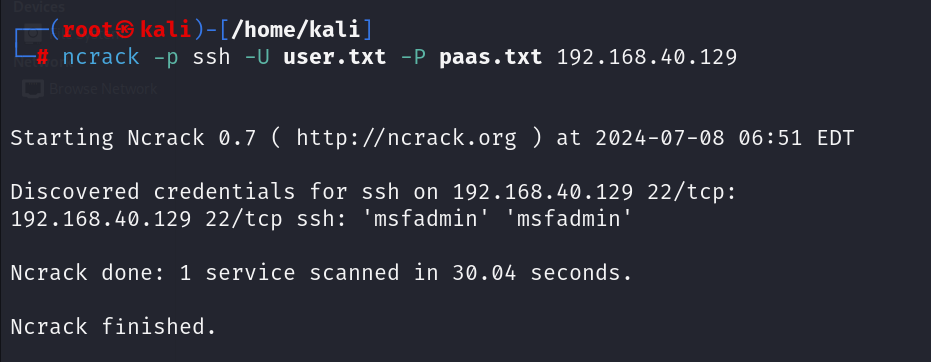
Usage Example for FTP:



**Ncrack:**

Ncrack is a fast and efficient tool designed to test and break network authentication protocols.

Example:

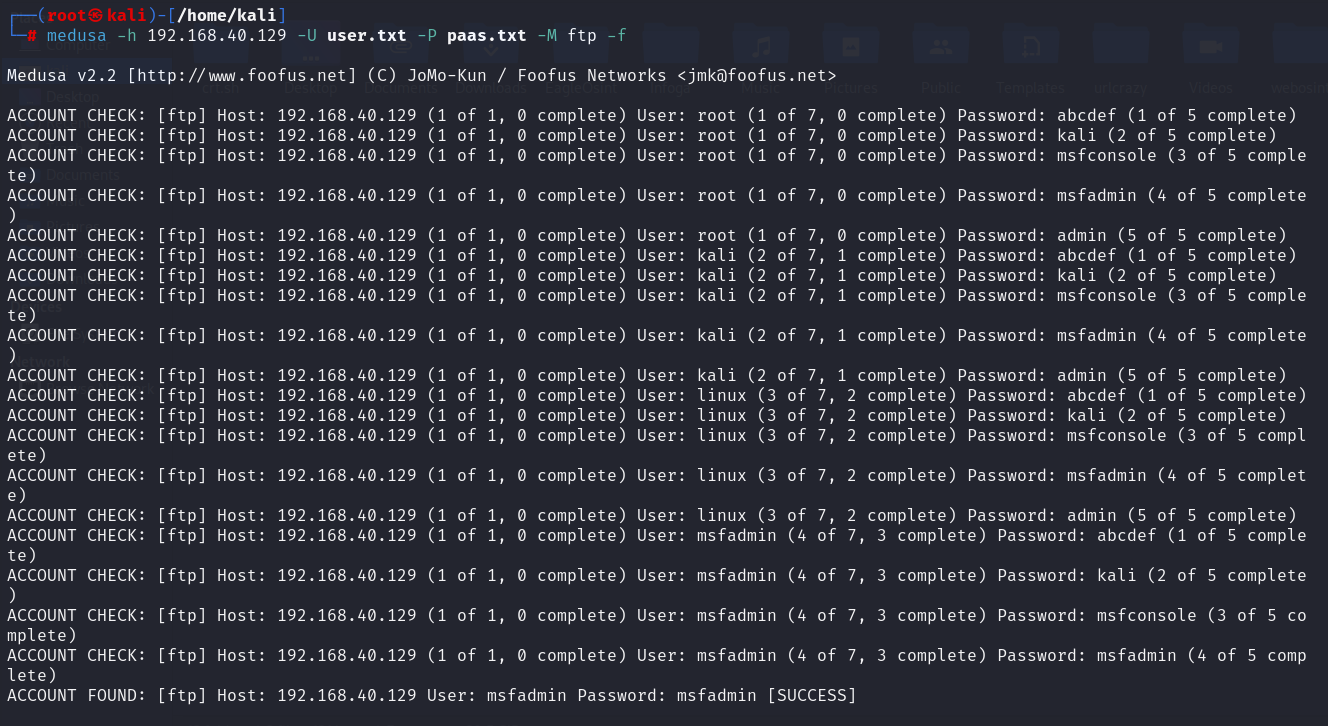


* -p ssh: Specify the service (ssh in this case).
* -U: File containing a list of usernames.
* -P: File containing a list of passwords.

**Medusa:**

Medusa is a parallel, modular, login brute-force that supports many protocols.

Example for FTP:



* -h: Target host.
* -U: File containing a list of usernames.
* -P: File containing a list of passwords.
* -M: Service module to use (ftp in this case).