Basic Hash Cracking Techniques Using Hashcat

Hashcat is a powerful password cracking tool that can be used to crack a wide range of password hashes. In this guide, we will cover some of the basic hash cracking techniques using Hashcat.

Prerequisites

Before you start using Hashcat, make sure you have the following:

- A computer with a modern GPU (Nvidia or AMD) or CPU.
- Hashcat installed on your system. You can download Hashcat from the official website.
- Your raspberry pis should have the software pre-installed.

Types of Hashes - Example

Hashcat supports a wide range of password hashes, including:

- MD5 - mode 0
- LM - mode 3000
- NTLM - mode 1000
- bcrypt - mode 3200
- and many others.

Basic Hash Cracking Techniques

Dictionary Attack

A dictionary attack is one of the most basic and popular hash cracking techniques. In this attack, Hashcat uses a pre-defined list of words (called a dictionary) to try to crack the password.

To perform a dictionary attack with Hashcat, use the following command:

```
hashcat -m [hash mode] [hash file] [dictionary file]
```

For example, to crack an MD5 hash using a dictionary file called "passwords.txt", use the following command:

```
hashcat -m 0 hash.txt passwords.txt
```

Brute-Force Attack

A brute-force attack is a method of trying every possible combination of characters until the correct password is found. This technique is more time-consuming and resource-intensive than a dictionary attack but can crack stronger passwords that are not in the dictionary.

To perform a brute-force attack with Hashcat, use the following command:

```
hashcat -m [hash mode] [hash file] -a 3 ?l?l?l?l?l?l?l?l
```

This command will try all possible combinations of eight lowercase letters.

'?l' represents 1 lower case character.
'?c' represents 1 upper case character.
'?d' represents 1 digit character.
'?a' represents 1 upper, lower, number or symbol character.

Example:

```
hashcat -m [hash mode] [hash file] -a 3 ?c?l?l?l?l?l?d
```

This would crack the password Summer1

Hybrid Attack

A hybrid attack is a combination of a dictionary attack and a brute-force attack. In this attack, Hashcat uses a dictionary file and applies various rules to each word in the dictionary to generate new password combinations.

To perform a hybrid attack with Hashcat, use the following command:

```
hashcat -m [hash mode] [hash file] -a 6 [dictionary file] [mask]
```

For example, to perform a hybrid attack on an NTLM hash using a dictionary file called "passwords.txt" and a rules file called "rules.txt", use the following command:

```
hashcat -m 1000 hash.txt -a 6 passwords.txt ?d?s
```

Rule Based Attack

A rule based attack is a combination of a dictionary attack and a mask attack. In this attack, Hashcat uses a dictionary file and applies various rules from a rule file to each word in the dictionary to generate new password combinations.

To perform a rule based attack with Hashcat, use the following command:

```
hashcat -m [hash mode] [hash file] -a 0 [dictionary file] [rule file]
```

For example, to perform a rule based attack on an NTLM hash using a dictionary file called "passwords.txt" and a rules file called "best64.rule", use the following command:

```
hashcat -m 1000 hash.txt -a 0 passwords.txt /usr/share/hashcat/rules/best64.rule
```

Conclusion

Remember cracked hashes can be submitted on the banking website to earn points!

https://megatroncyberbank.root66tulsa.club/

Cracking passwords without permission is illegal and unethical. Use this knowledge responsibly and only for authorized purposes.