Carleton
Cyber
Security
Club

Week 1.2 - Password Cracking

Password Cracking:

Tools: unshadow, hydra, john the ripper, hashcat, …

Focus: Correct Usage

Unshadow:

Usage: combine /etc/passwd and /etc/shadow into one file that can be cracked by hashcat or john

Syntax:

```
unshadow passwd shadow > outfile
```

John the Ripper:

Usage: crack file with username and password hashes

Syntax:

```
sudo john -wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou-75.txt
-rules crackme
```

Install seclists: sudo apt-get install seclists

- wordlist - the hashes to compare to
- rules - allows changing of cases, ints to be added, etc
- crackme is file with hashes

Hashcat:

Usage: crack file with username and password hashes

Syntax: You must know the type of hash. Find at https://hashcat.net/wiki/doku.php?id=example_hashes

```
Hashcat -m [HASH TYPE] -a 0 --force [FILE WITH HASHES] [DICTIONARY LOCATION]
```

-m - hash type, look up on wiki

- a - number of accelerators

-o [FILENAME] - save results to outfile

//Note force is graphics card specific

Hydra:

Usage: For services like ssh, ftp, ... when you know username but not password

Syntax:

```
hydra -l [USERNAME or LIST OF USERS] -p /path/to/dict [SERVICE]://[IP ADDRESS]
```

ie.

```
hydra -l root -p /usr/seclists/Leaked-Databases/Passwords/rockyou-10.txt
ssh://192.168.0.10
```

```
-l - user or list of users
- p - password list
[SERVICE] - target service
[IP ADDRESS] - target ip address
```