# Password Hacking

# Welcome UML Hackers

Hello everybody,

The UMass Lowell Cybersecurity Club thanks you for attending the first meeting of the year!

We will be covering a fun topic today that surely will want you to come back for more…

If you have any suggestions or you wanna see other tools or hacking techniques… don’t be afraid to post suggestions in the Discord.

# Passwords

- All applications have passwords
  - Social Media, Banks, Login pages, Phones/Computers
- Not all passwords are good
  - So make them good or face the consequences…
- Data Breaches contain the most passwords
  - Companies are hacked every day and contain sensitive information
- Multiple ways to get passwords
  - Phishing, Smishing, Quishing, or social engineering
- Passwords aren't always enough
  - You might need 2FA or MFA

# Password Cracking

- Passwords are cracked or decoded in various ways
  - Dictionary attacks, hash cracking, rainbow table, brute forcing
- How to crack one
  - On the Kali VM's login to Kali Linux U:Kali P:Kali
- Use the example Matt made
  - This contains the passwords that you need to crack
- Use various tools to crack the password
  - Hashcat, JohnTheRipper, RainbowCrack
- Use different techniques
  - You might not be able to crack a password one way but there are other ways!
- Try a brute force!
  - Hydra, Patator, or Medusa will be your friends!

# Techniques and Tools

- Go Phishing!
  - Try sending a funny link to one of your friends or one of us to get some creds!
- Use wordlists
  - Wordlists like Rockyou or Fasttrack are used for dictionary attacks and majority of password attacks. Simply type “wordlists”
- Profile someone
  - Try gathering more info on a target and make a wordlists tailored for them. Get a hash from them and try cracking their password!

AGE GROUP
INDUSTRY
AGE
JOB TITLE
REVENUE
$
COMPANY SIZE
LOCATION
Salespanel

# Important Commands

- hashcat -m 0 -a 0 -o cracked.txt <hash.txt> /usr/share/wordlists/<wordlist>
- john -- /usr/share/wordlists/<wordlist> <hash.txt>
  - john --show hashes.txt (after hash is cracked)
- hydra <ip> -u <uname> or -U <uname file> -p <password> or -P <password file> protocol <ssh, ftp, telnet>
- medusa -h <target-ip> -u <username> -P <wordlist.txt> -M <module>
  - Module = service you want to attack
- hashidentifer
  - This will check the type of hash that you will be cracking. This is useful for hashcat as it needs proper guidance to crack. This is where -m comes into play, this will signify the hash.
- Zphisher
  - A phishing tool from GitHub that will allow you to grab credentials from targets you send a link too. This is important for social engineering and quickly grabbing login info. Follow instructions on the page
- PLEASE RUN BEFORE EVERYTHING
  - docker run -it --rm --network host linuxserver/kali-linux bash
- ATTACK THIS
  - user@ec2-54-221-52-61.compute-1.amazonaws.com

# Got Stuck?

- We all need help
  - If you need help don't hesitate to ask for it!!!
- No Holding Back
  - We don't hold back on what you want to learn. You wanna learn something else talk to one of us!
- Two hackers are better than one
  - Grab a friend or another aspiring hacker and work with them to use the tools or hack!
- Hack Squad
  - Make a little group of hackers and try to get access to the machine in the cloud