**Network**

**Security**

**Class 10**

**Lab 29**

|  |
| --- |
| Lab Objectives:  * Email Hijacking * Password Hijacking |

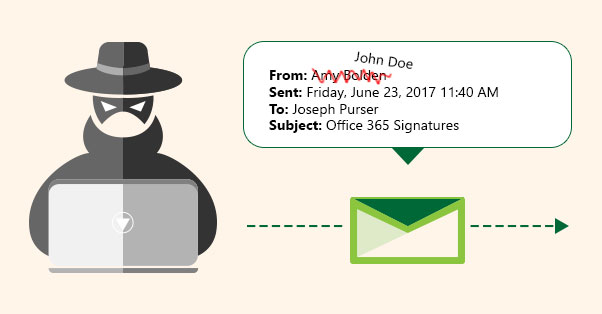
# Email Hijacking

## Email Hijacking is a widespread threat nowadays. An hacker can take the full control of a target email using Email Hijacking technique. It works by using the following three techniques which are email spoofing, social engineering tools, or inserting viruses in a user computer.



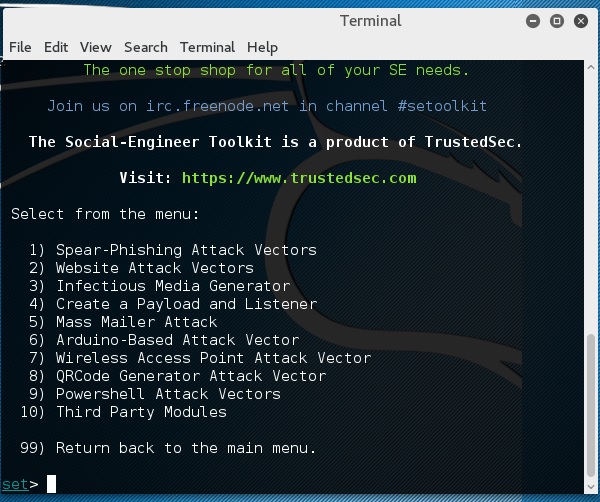
# Email Spoofing

## In email spoofing, the spammer sends emails from a known domain, so the receiver thinks that he knows this person and opens the mail. Such mails normally contain suspicious links, doubtful content, requests to transfer money, etc.

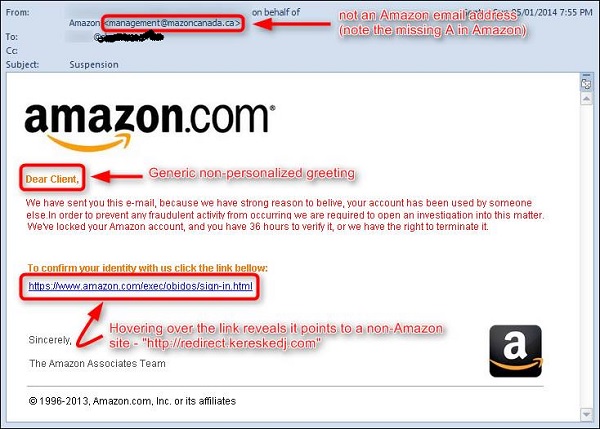


# Social Engineering

## Spammers send promotional mails to different users, offering huge discount and tricking them to fill their personal data. You have tools available in Kali that can drive you to hijack an email.



## Email hacking can also be done by phishing techniques. See the following screenshot.



## The links in the email may install malware on the user’s system or redirect the user to a malicious website and trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

## Phishing attacks are widely used by cyber criminals, as it is far easier to trick someone into clicking a malicious links in the email than trying to break through a computer’s defenses.

# Inserting Viruses in a User System

## The third technique by which a hacker can hijack your email account is by infecting your system with a virus or any other kind of malware. With the help of a virus, a hacker can take all your passwords.



# How to detect if your email has been hijacked?

## The recipients of spam emails include a bunch of people you know.

## You try to access your account and the password no longer works.

## You try to access the “Forgot Password” link and it does not go to the expected email.

## Your Sent Items folder contains a bunch of spams you are not aware of sending.

# Quick tips

## In case you think that your email got hijacked, then you need to take the following actions −

## Change the passwords immediately.

## Notify your friends not to open links that they receive from your email account.

## Contact the authorities and report that your account has been hacked.

## Install a good antivirus on your computer and update it.

## Set up double authentication password if it is supported.

# Password Hacking

## We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account.



## In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

## One should always take care to have a strong password to defend their accounts from potential hackers. A strong password has the following attributes −

## Contains at least 8 characters.

## A mix of letters, numbers, and special characters.

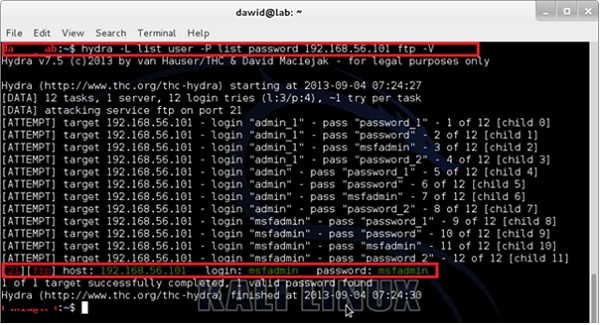
## A combination of small and capital letters.



# Dictionary Attack

## In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.

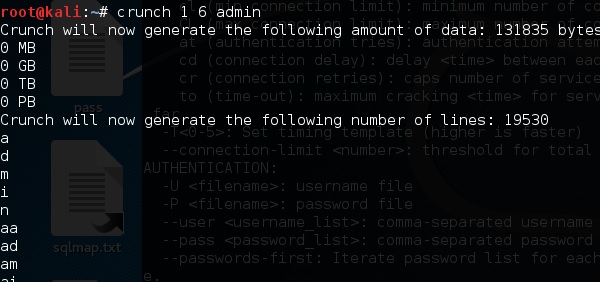
## Hydra is a popular tool that is widely used for dictionary attacks. Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service.



# Hybrid Dictionary Attack

## Hybrid dictionary attack uses a set of dictionary words combined with extensions. For example, we have the word “admin” and combine it with number extensions such as “admin123”, “admin147”, etc.

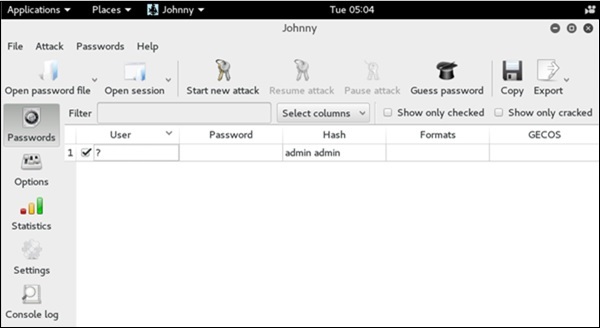
## Crunch is a word list generator where you can specify a standard character set or a character set. Crunch can generate all possible combinations and permutations. This tool comes bundled with the Kali distribution of Linux.



# Brute-Force Attack

## In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.

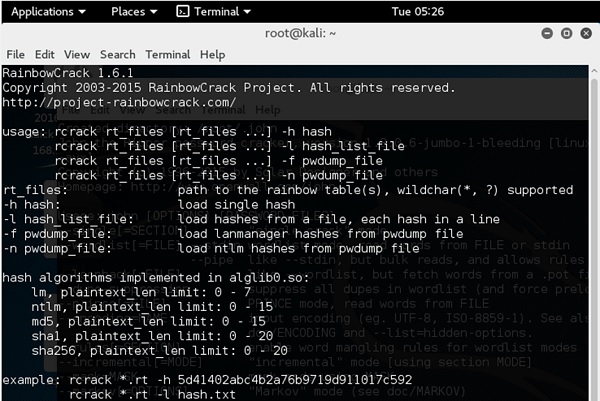
## John the Ripper or Johnny is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



# Rainbow Tables

## A rainbow table contains a set of predefined passwords that are hashed. It is a lookup table used especially in recovering plain passwords from a cipher text. During the process of password recovery, it just looks at the pre-calculated hash table to crack the password. The tables can be downloaded from [http://project-rainbowcrack.com/table.htm](http://project-rainbowcrack.com/table.htm" \t "/home/deepto/Documents\\x/_blank)

## RainbowCrack 1.6.1 is the tool to use the rainbow tables. It is available again in Kali distribution.



# Quick Tips

## Don’t note down the passwords anywhere, just memorize them.

## Set strong passwords that are difficult to crack.

## Use a combination of alphabets, digits, symbols, and capital and small letters.

## Don’t set passwords that are similar to their usernames.