



Ethics in IT

Class 10

Lab 1

Lab Objectives:

- Email Hijacking

Ethical Hacking - Email Hijacking

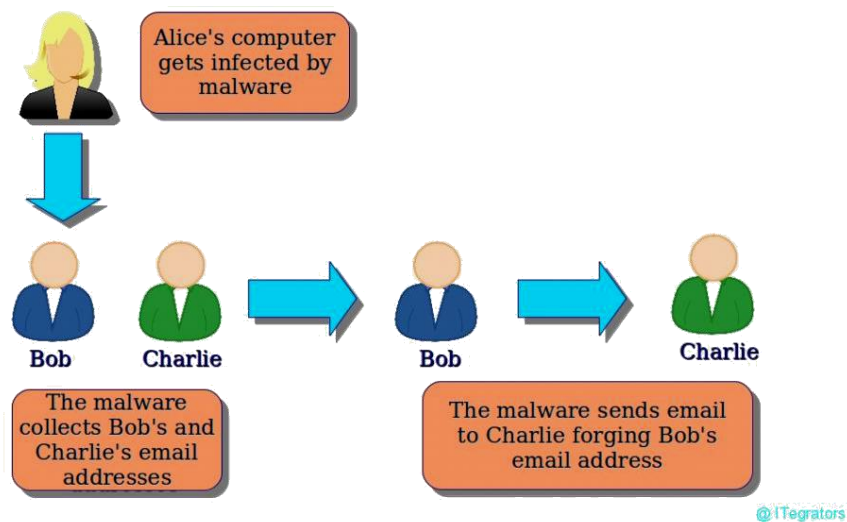
Email Hijacking, or email hacking, is a widespread menace nowadays. It works by using the following three techniques which are email spoofing, social engineering tools, or inserting viruses in a user computer.





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 Linux that can drive you to hijack an email.



Email hacking can also be done by phishing techniques.

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 cybercriminals, 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 –

1. Change the passwords immediately.



2. Notify your friends not to open links that they receive from your email account.
3. Contact the authorities and report that your account has been hacked.
4. Install a good antivirus on your computer and update it.



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