# Network Security

Class 10

Lab 28

UNITED TRUST

bdeducation™
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

## Lab Objectives:

- Trojans
- TCP/IP Hijacking

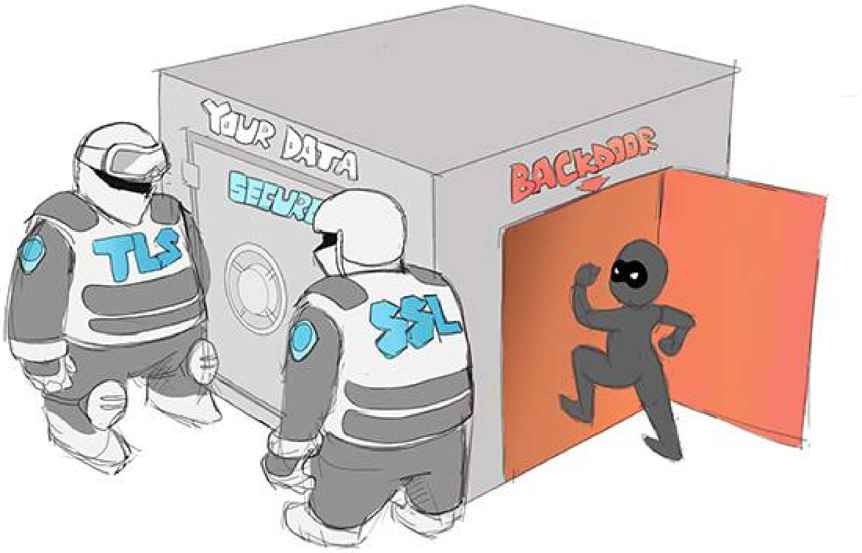
## Trojans

Trojans are non-replication programs; they don’t reproduce their own codes by attaching themselves to other executable codes. They operate without the permissions or knowledge of the computer users.

Trojans hide themselves in healthy processes. However we should underline that Trojans infect outside machines only with the assistance of a computer user, like clicking a file that comes attached with email from an unknown person, plugging USB without scanning, opening unsafe URLs.

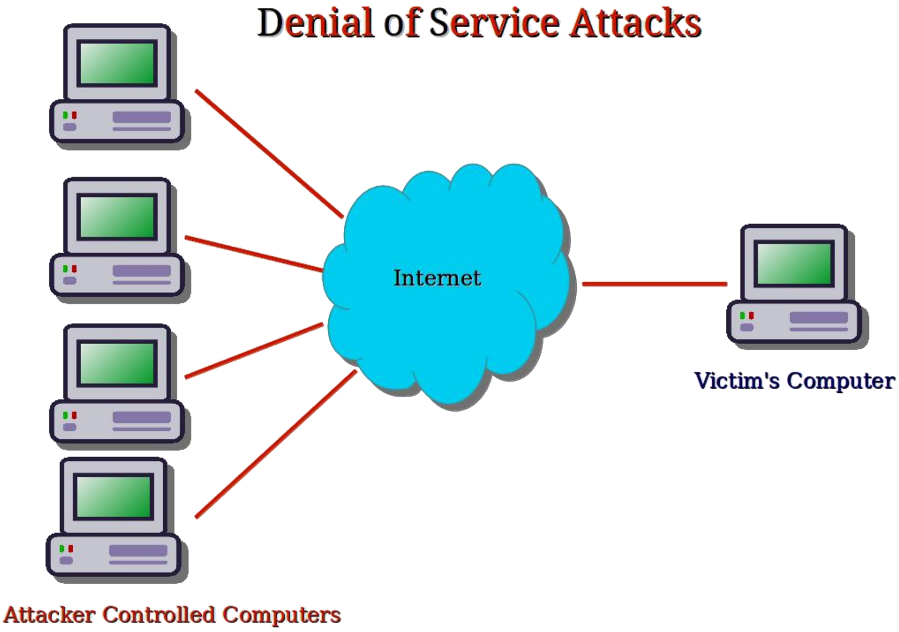
***Trojans have several malicious functions −***

√ They create backdoors to a system. Hackers can use these backdoors to access a victim system and its files. A hacker can use Trojans to edit and delete the files present on a victim system, or to observe the activities of the victim.



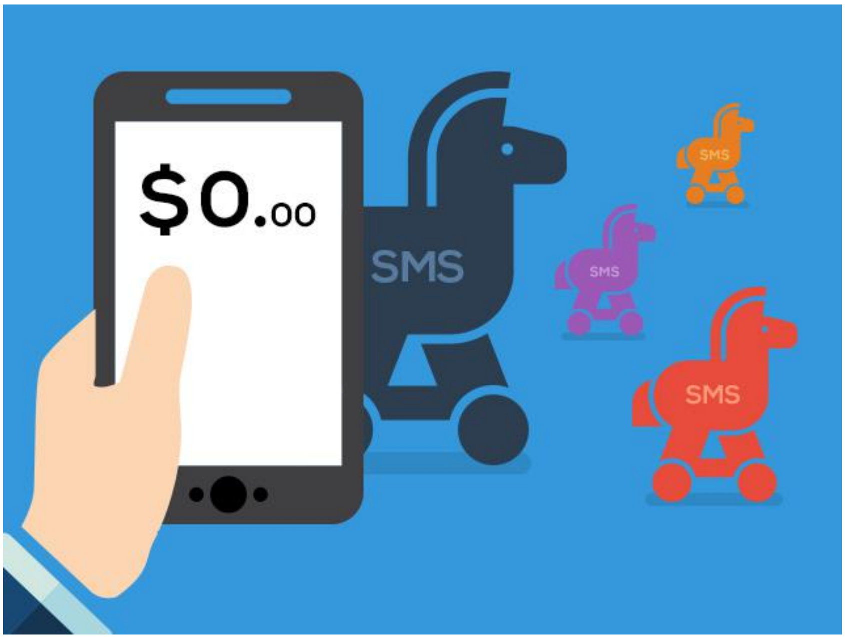
√ Trojans can steal all your financial data like bank accounts, transaction details, PayPal related information, etc. These are called Trojan-Banker.

√ Trojans can use the victim computer to attack other systems using Denial of Services.



√ Trojans can encrypt all your files and the hacker may thereafter demand money to decrypt them. These are Ransomware Trojans.

√ Trojans can use your phones to send SMS to third parties. These are called SMS Trojans.



## Trojan Information

If you have found a virus and want to investigate further regarding its function, then we will recommend that you have a look at the following virus databases, which are offered generally by antivirus vendors.

- Kaspersky-Virus database – https://www.kaspersky.com
- F-secure – https://www.f-secure.com/en/welcome
- Symantec–Virus Encyclopedia – https://www.symantec.com/

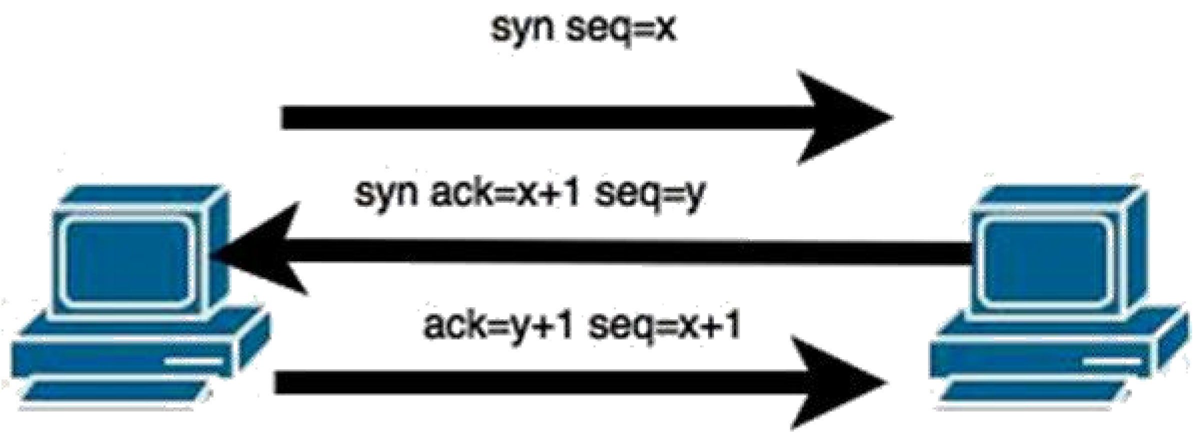
## Quick Tips

- Install a good antivirus and keep it updated.
- Don’t open email attachments coming from unknown sources.
- Don’t accept invitation from unknown people in social media.
- Don’t open URLs sent by unknown people or URLs that are in weird form.

# TCP/IP Hijacking

TCP/IP Hijacking is when an authorized user gains access to a genuine network connection of another user. It is done in order to bypass the password authentication which is normally the start of a session.

In theory, a TCP/IP connection is established as shown below −



To hijack this connection, there are two possibilities −

- Find the seq which is a number that increases by 1, but there is no chance to predict it.

- The second possibility is to use the Man-in-the-Middle attack which, in simple words, is a type of network sniffing. For sniffing, we use tools like Wireshark or Ethercap.

## Example

An attacker monitors the data transmission over a network and discovers the IP's of two devices that participate in a connection.

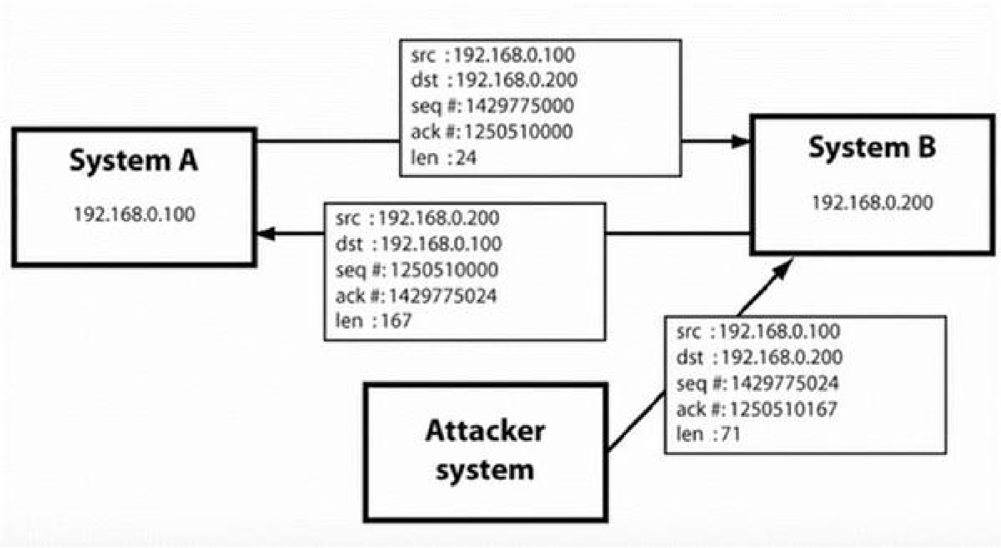
When the hacker discovers the IP of one of the users, he can put down the connection of the other user by DoS attack and then resume communication by spoofing the IP of the disconnected user.

### *Shijack*

In practice, one of the best TCP/IP hijack tools is Shijack. It is developed using Python language and you can download it from the following link − https://packetstormsecurity.com/sniffers/shijack.tgz

Here is an example of a Shijack command −

```
root:/home/root/hijack# ./shijack eth0 192.168.0.100 53517 192.168.0.200 23
```



Here, we are trying to hijack a Telnet connection between the two hosts.

## Hunt

Hunt is another popular tool that you can use to hijack a TCP/IP connection. It can be downloaded from – https://packetstormsecurity.com/sniffers/hunt/

## Quick Tip

All unencrypted sessions are vulnerable to TCP/IP session hijacking, so you should be using encrypted protocols as much as possible. Or, you should use double authentication techniques to keep the session secured.