Ethics in IT

Class 9

Lab 4

UNITED TRUST

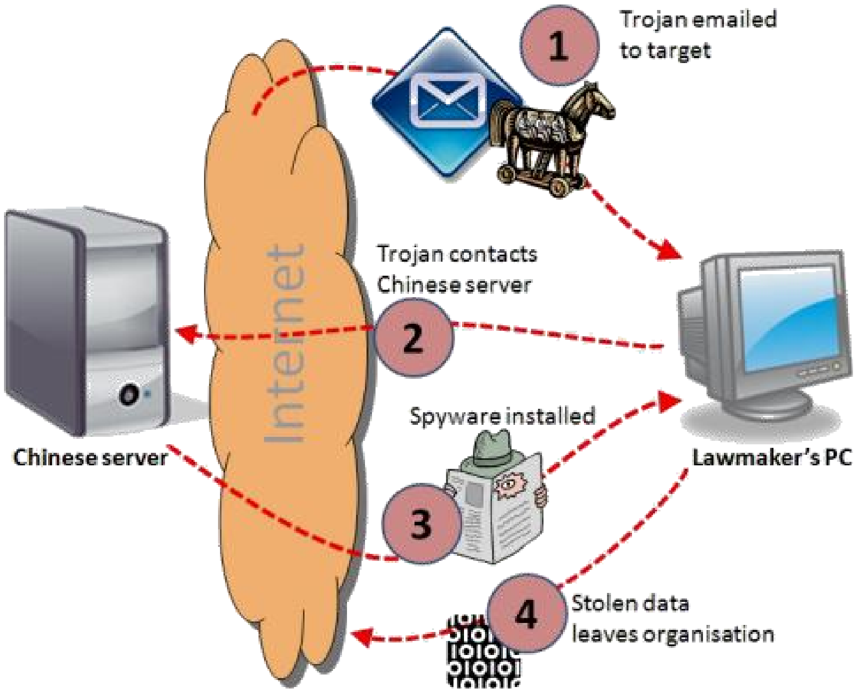
bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

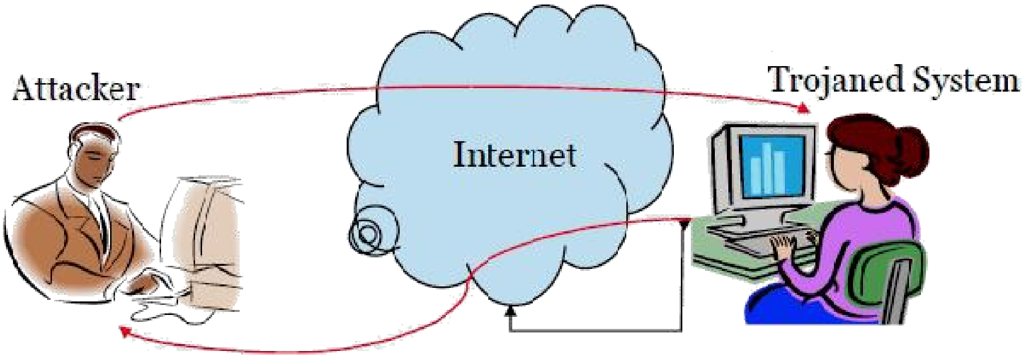
- Trojan Attack

Ethical Hacking - Trojan Attacks

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.

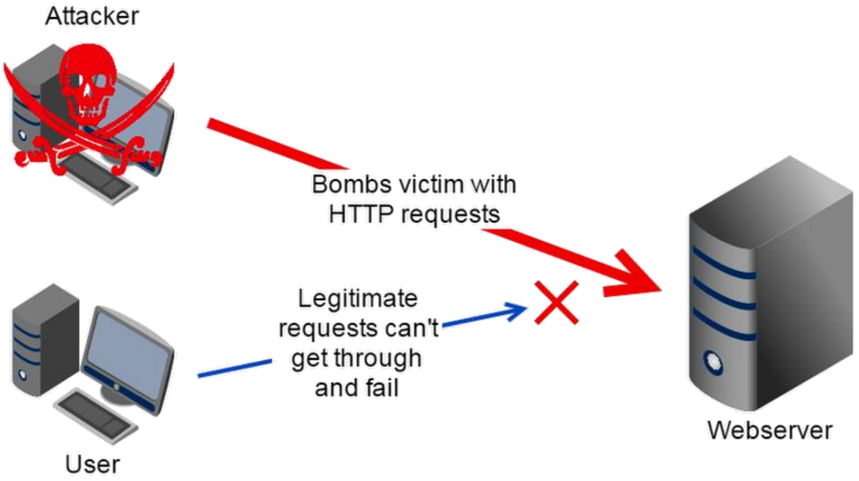


Trojans have several malicious functions −

- 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

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

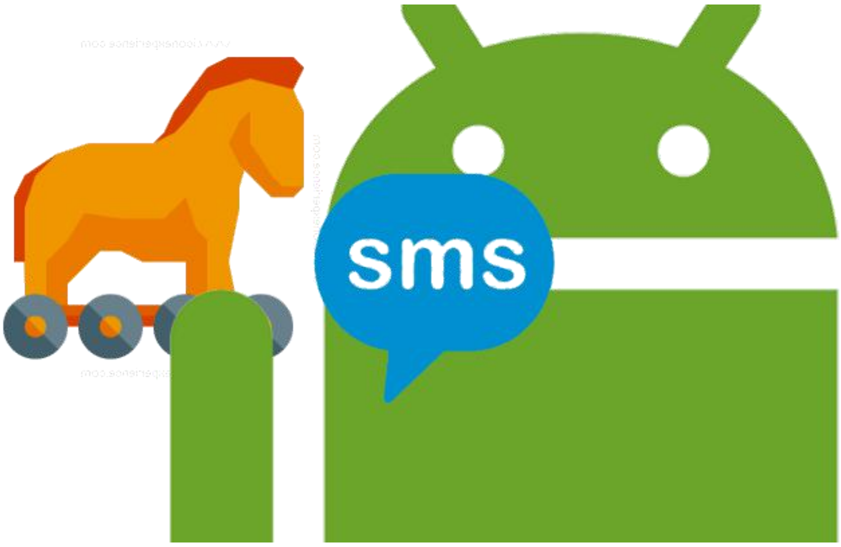
- ➢ Trojans can use the victim computer to attack other systems using Denial of Services.


Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

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

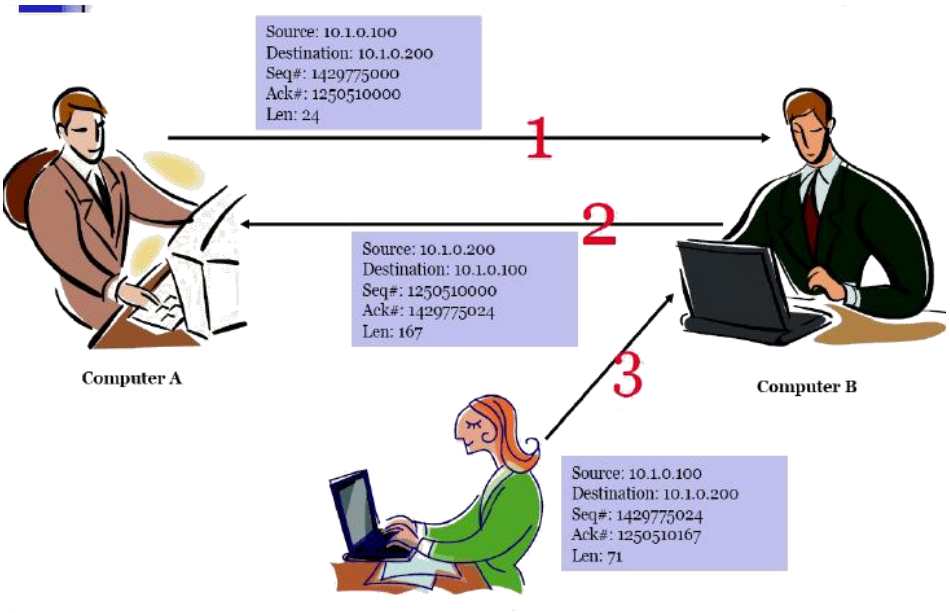
Ransomware

- ➢ They can use your phones to send SMS to third parties. These are called SMS Trojans.

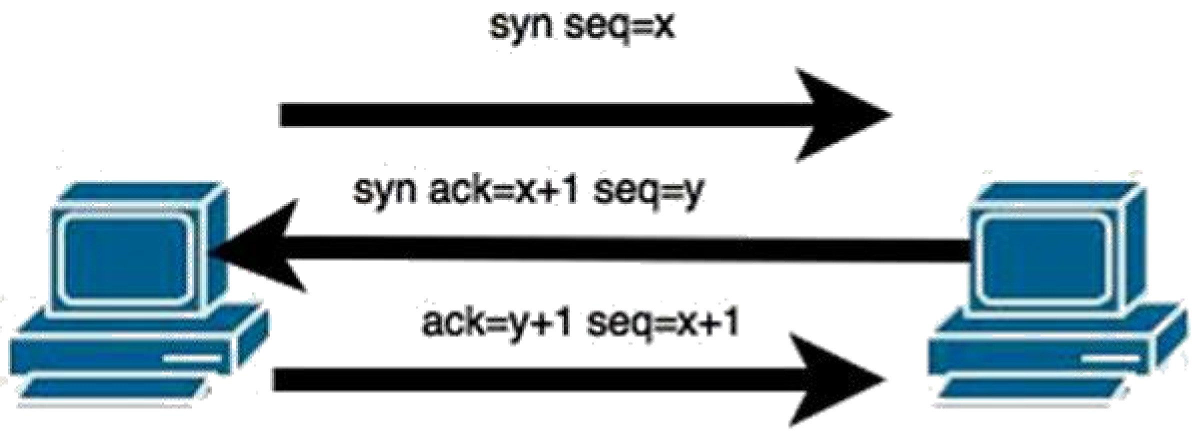


Ethical Hacking - TCP/IP Hijacking

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 −



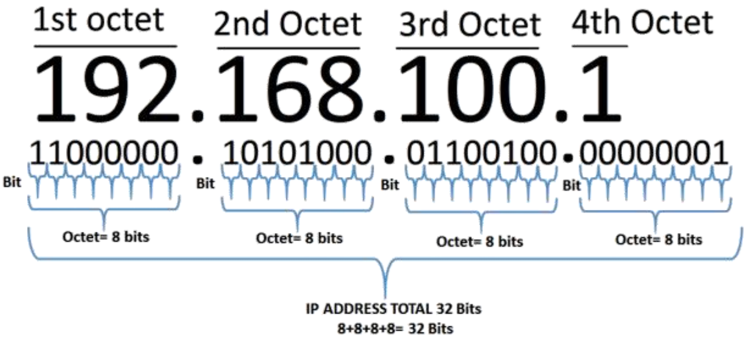
To hijack this connection, there are two possibilities

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

2. 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.