Ethics in IT

Class 8

Lab 5

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

Lab Objectives:

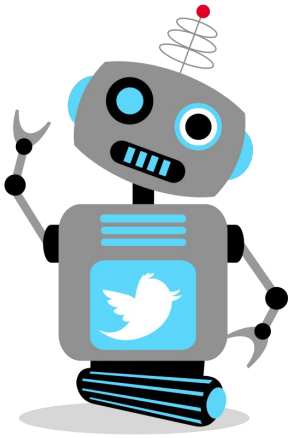
- Terminology of hacking

√***Adware*** – Adware is software designed to force pre-chosen ads to display on your system.

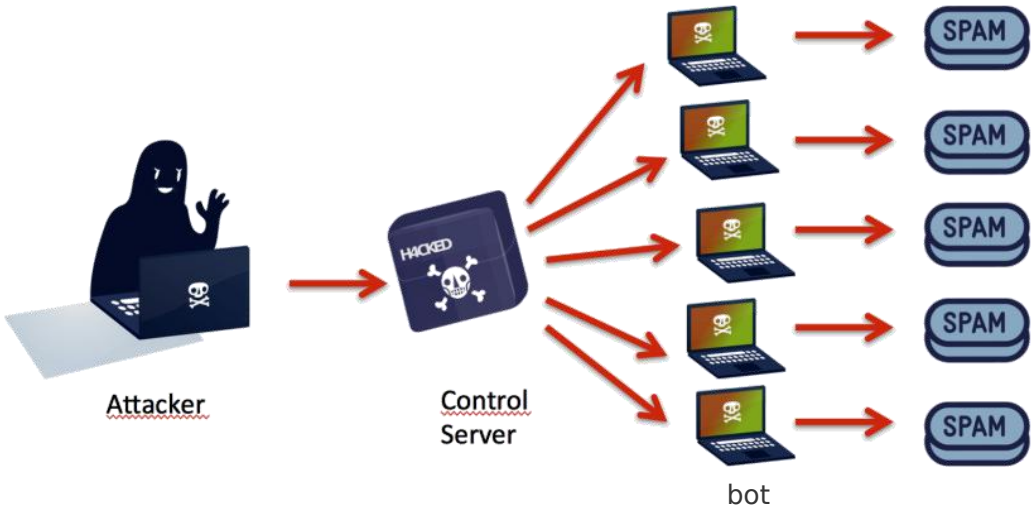
√ ***Attack*** – An attack is an action that is done on a system to get its access and extract sensitive data.

√ ***Back door*** – A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.

√ ***Bot*** – A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it.

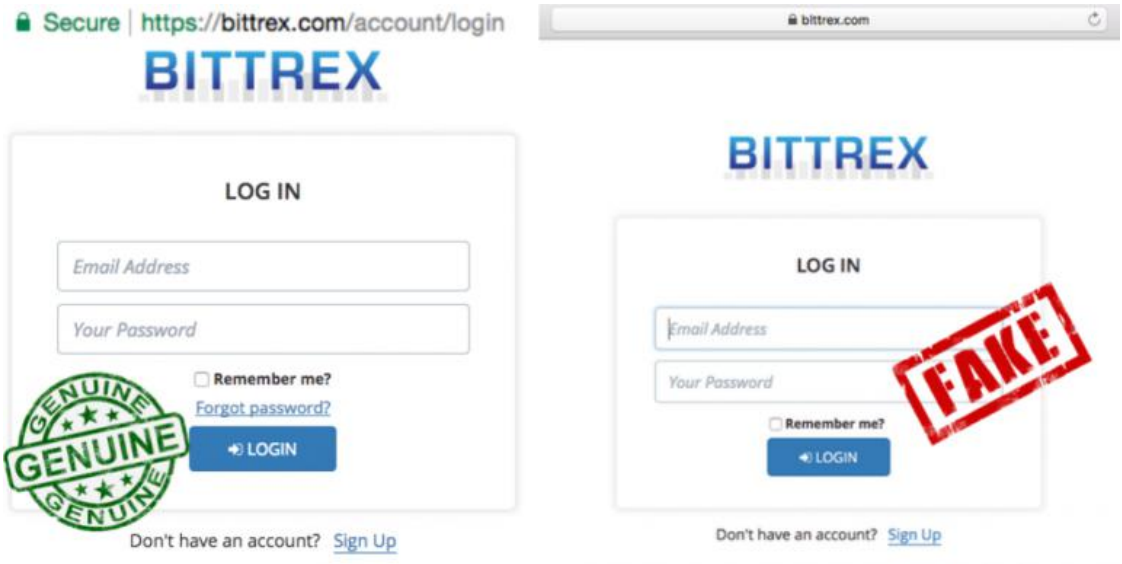


√ ***Botnet*** – A botnet, also known as zombie army, is a group of computers controlled without their owners' knowledge. Botnets are used to send spam or make denial of service attacks.



√ ***Brute force attack*** – A brute force attack is an automated and the simplest kind of method to gain access to a system or website. It tries different combination of usernames and passwords, over and over again, until it gets in.

√ ***Clone phishing*** – Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.

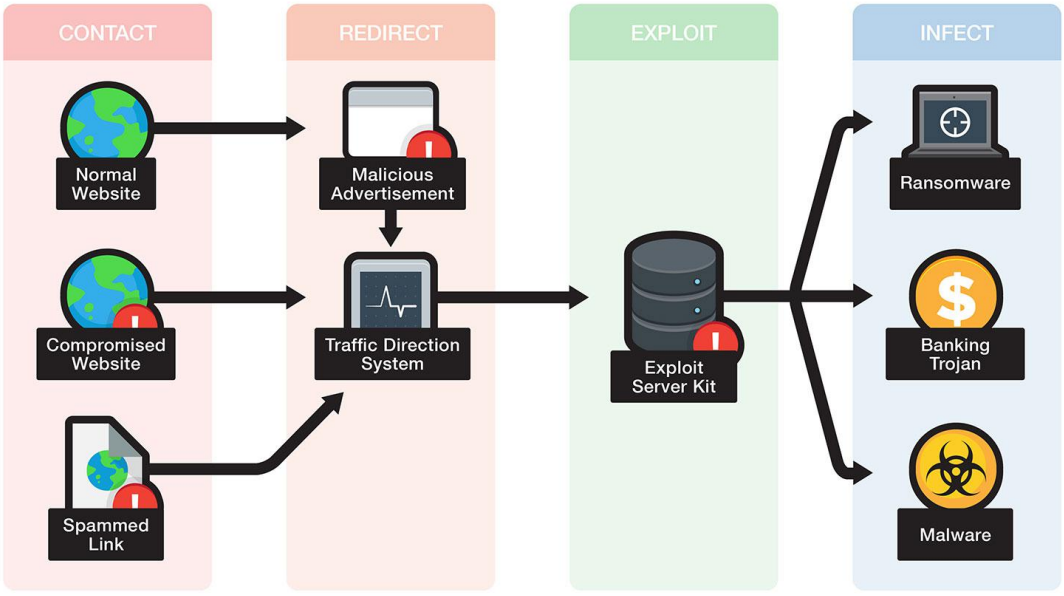


√ ***Cracker*** – A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.

√ ***Denial of service attack (DoS)*** – A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

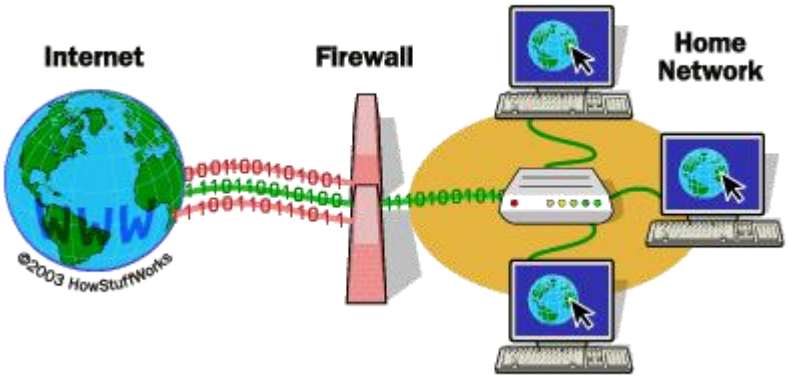
√ ***DDoS*** – Distributed denial of service attack.

√ ***Exploit Kit*** – An exploit kit is software system designed to run on web servers, with the purpose of identifying software vulnerabilities in client machines communicating with it and exploiting discovered vulnerabilities to upload and execute malicious code on the client.



√ ***Exploit*** – Exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to compromise the security of a computer or network system.

√ ***Firewall*** – A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.



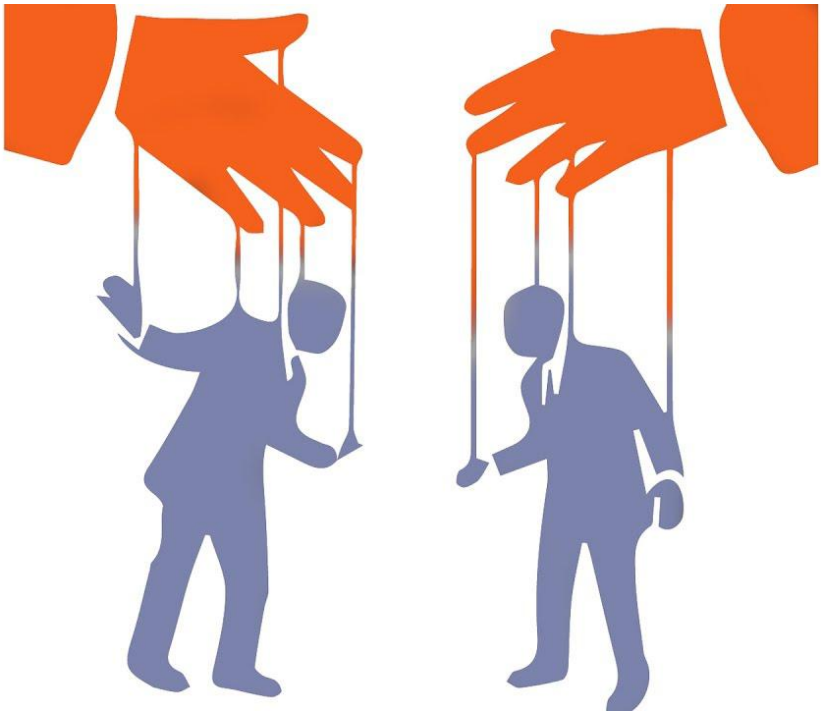
√ ***Logic bomb*** – A virus secreted into a system that triggers a malicious action when certain conditions are met. The most common version is the time bomb.

√ ***Malware*** – Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

√ ***Phishing*** – Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.

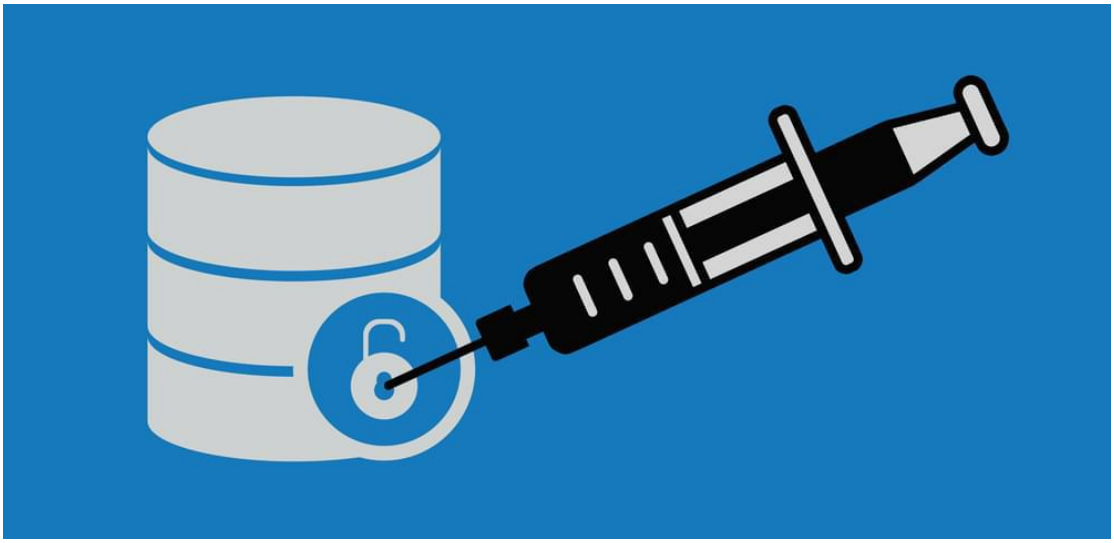
√ ***Rootkit*** – Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.

√ ***Social engineering*** – Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.



√ ***Spam*** – A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.

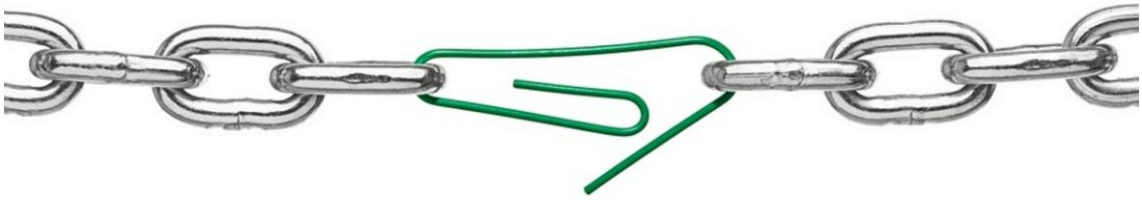
√ ***SQL Injection*** – SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).



√ ***Trojan*** – A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.

√ ***Virus*** – A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

√ ***Vulnerability*** – A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.



√ ***Worms*** – A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

√ ***Cross-site Scripting*** – Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side script into web pages viewed by other users.

√ ***Zombie Drone*** – A Zombie Drone is defined as a hi-jacked computer that is being used anonymously as a soldier or 'drone' for malicious activity, for example, distributing unwanted spam e-mails.