How Hackers Hack

Step 1: Obtain information
– Obtaining information is the first and most important step in hacking. This is done by performing port scans.

Step 2: Analyze information
– Analyzing information is another crucial step in hacking. A hacker takes the information that he obtained and looks for weak points in the network to expose.

Step 3: Use information obtained
– Step three is what causes the most pain. Information obtained is used to issue Denial of Service attacks, Crack Passwords, Obtain sensitive data and Destroy or Deface network systems.

Exploit
– Attack on a system, especially one that takes advantage of a particular vulnerability that the system offers to intruders. Used as a verb, the term refers to the act of successfully making such an attack. Vendors issue “patches” or “fixes” to remove vulnerabilities.

Virus
– A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. Viruses can be transmitted as attachments to an e-mail note, as downloads, or on a diskette or CD.

Denial of Service Attack (DoS)
– An attack in which a user or organization is deprived of the services of a resource they would normally expect to have. Usually caused by sending a flood of traffic to the target. A DoS is a type of security breach to a computer system that does not usually result in the theft of information or other security loss. However, these attacks can cost the target person or company a great deal of time and money.
Distributed Denial of Service Attack (DDoS)

- A DoS attack that is initiated from many different sources, all attacking the same target. The attacks that occurred last year on Yahoo and EBay are examples of DDoS attacks.

Sniffer

- A program that monitors and analyzes network traffic. A sniffer can also be used legitimately or illegitimately to capture data being transmitted on a network.

Spoof

- To deceive during a DoS attack or an exploit (for example, to fake an Internet address so that it looks like the source is someone else).

Script-Kiddie and Click-Kiddie

- Derogative terms for the often immature and inexperienced attacker that uses existing and frequently well-known and easy-to-find techniques and programs, or scripts, to search for and exploit weaknesses in other computers on the Internet.
- Click-Kiddies use programs with graphical user interfaces to point-and-click their way to chaos and mayhem.

Port Scan

- In hacker reconnaissance, a port scan attempts to connect to all 65536 ports on a machine in order to see if anybody is listening on those ports.

SYN Attack

- A denial of service attack that uses up all available TCP sockets so that no new sessions are able to be established.

Worm

- A program that propagates itself by attacking other machines and copying itself to them. In the late 1980s, the Morris Worm shutdown the Internet for a couple of days by exposing a bug in SENDMAIL.
**Trojan Horse**
- A class of malware, the word *trojan* refers to the classic Trojan Horse from the story The Iliad. Typically a file that comes in from a trusted source that contains something malicious.

**Brute Force**
- A classic attack technique whereby all possible combinations are attempted until one succeeds. This typically refers to cryptography, either finding the right key to decrypt a message, or discovering somebody's password.

Backup your data – either to CD’s, Memory Stick, floppy, another PC
Don't put data where it doesn't need to be
Make sure sensitive data is not sitting in shared folders or if it is that the folder is password protected/data is encrypted
Stay current with relevant operating system patches: Windows updates
Keep your Virus Protection software up-to-date
Have someone on staff be familiar with security practices