8.6 Trojan Horses

A Trojan horse is an application that appears to have a benign purpose, but actually performs malicious activity. This deception is what makes these applications a dangerous threat to your system. The Internet is full of useful utilities (including many security tools), screen savers, images, and documents. Most Internet users tend to download these things. Creating an attractive download that has a malicious payload is an effective way of gaining access to a person's computer.

One type of defence against Trojan horses is to prevent all downloads. Unfortunately this is not particularly practical. The value of the Internet is the easy access it provides to such a wide variety of information. Restricting that access in such a draconian manner disrupts one of the most important reasons for giving employees Internet access. Instead of using such a heavy-handed tactic, you will learn other methods in order to protect your systems from Trojan horses.

Once you have a Trojan horse on your system, it may perform any number of unwanted activities. Some of the most common actions Trojan horses take include:

- Erasing files on a computer.
- Spreading other malware, such as viruses. Another term for a Trojan horse that does this is a dropper.
- Using the host computer to launch distributed denial of service (DDoS) attacks or sends spam.
- Searching for personal information such as bank account data.
- Installing a back door on a computer system. This means providing the creator of the Trojan horse easy access to the system, such as creating a username and password he/she can use to access the system.

Installing back doors and executing distributed denial of service attacks are probably the most frequent results of a Trojan horse attack from the above list. However, installing spyware and dropping viruses are also becoming much more common.

The list below names several famous types of Trojan Horses:

- Back Orifice

- Anti-Spyware 2011
- Shedun
- Brain Test
- FinFisher
- NetBus
- FlashBack

8.6.1 Trojan Horses Symptoms

It is difficult to determine whether your system is victim of a Trojan horse. There are a number of symptoms that might indicate that you have a Trojan horse. If you are the legitimate user and you do not make the following changes, symptoms and signs of a potential Trojan horse attack could be the following:

- Home page for your browser changing
- Any change to passwords, usernames, accounts, etc.
- Any changes to screen savers, mouse settings, backgrounds, etc.
- Any device (such as a CD door) seeming to work on its own

Any of these changes are symptoms of a Trojan horse and indicate your system is most probably infected.