



TenStep Supplemental Paper

8 July 2005

Hacking Away

Hacking takes many forms. It has morphed from using up system resources, Net time and saving repulsive content on hard drives to Denial of Service (DoS) attacks, mail bombs and invasion of secure information areas.

A survey on IT security in Indian companies by CII-PricewaterhouseCoopers revealed that only 57 percent employ either informal or no security policy at all. This is despite 60 percent of the companies falling prey to security breaches over the last year. These breaches included unauthorized access, virus attacks, theft of corporate data and denial of service attacks.

Hackers can be grouped into three genres, namely, the script kiddies, the technicians and the professionals.

The Script Kiddies

Script kiddies come last in the hacker's pecking order. They research hacker sites and work on tools and scripts developed by seasoned hackers. They then search for systems on the Internet to try their newly acquired skills on. Script kiddies normally hack Web sites and substitute the home pages with messages such as these, "Site hacked by XYZ." Besides being aggravating, there's not much script kiddies can do to actually bring your system down.

The Technicians

Experienced and skilled, they have excellent programming skills and a thorough understanding of computer networks. They might just be indulging themselves to a little learning. They could also be using your system as a gateway to attack other systems. They can be very harmful and are unpredictable.

The Industrial Spies

Hacking is also employed for industrial espionage which targets companies for confidential financial or research information. These individuals are expert and spend time researching tools and methods before attacking. They are even hired by companies to steal competitor information. Typically banks, e-commerce sites, MNCs and intellectual property-based companies are targets.

Preventing Hacker Attacks

India's Information Technology Act, 2000 (ITA-2000) has a provision on hacking. It takes cognizance of a significant government initiative against hacking activity. It defines hacking as an act which is likely to cause loss or damage to the public or any person, destroys or deletes information in a computer resource or diminishes its value or utility or affects it by any means. Legally, the act is punishable with up to three years or with a fine which may extend up to Rs 2 lakhs, or with both.



TenStep Supplemental Paper

Software systems that are connected to the Internet is a common entry point for hackers, especially via their back-end components. Bookmark the sites of the vendors of the software that you use to get their updates and patches. You can also sign up for services that will send you newsletters on updates.

Some sites specialize in computer and network security. They often post system vulnerabilities well before a vendor brings out a fix. L0pht.com and 403-security.org can give you the latest on security information.

Always use unique passwords. These should be a combination of alphanumeric, special characters, lowercase and uppercase letters. Change passwords regularly. Do not provide credit card information to sites that do not use encryption. Install firewall software to prevent entry of unauthorized users via the Internet. Archive your data on removable media at frequent intervals.