

Hackers, Crackers, and Sneakers

An Introduction to Hacking

Hacker has become one of the most widely used terms in the English language. This word strikes terror in the hearts of business owners, embodies hope and rebellion for some, and spells mayhem for a select few. In dissecting any phenomenon, the first step is defining the phenomenon itself.

hacker *n.*

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically [even obsessively] or who enjoys programming rather than just theorizing about programming. 3. One who enjoys the intellectual challenge of creatively overcoming and circumventing limitations.

The role of the *hacker* is not as insidious as his or her reputation may reflect. Hacking involves learning all of the ins and outs of computers. The pursuit of knowledge and quest for precise understanding is essential for any industry to continue progressing, but there is leeway for the *hacker* to take this knowledge and apply it in destructive ways.

Continued on page 2

INSIDE THIS ISSUE

An Introduction To Hacking

Should I Be Wary of Hackers?

Firewalls: The First Line of Defense

Hackers Storm White House Web Site

For online shopping visit:
www.SaveByClicking.com

Should I be Wary of Hackers?

Everyone is susceptible to hacking. Some methods of internet connection put users at a higher risk than others.

Cable Modems: With a Cable modem you have a full-time permanent address on the Internet, or a *static IP address*. In addition, with a Cable modem, you are connected to the Internet as long as your computer is on. Those two factors make you more prone to hackers than you would be with a dial-up connection. Cable modem providers do provide some safeguards against attack such as proxy servers.

Dial-up: With a dial-up connection you have a *dynamic IP address* that changes each time you dial in, so a hacker wouldn't necessarily know where you are on the Internet. You are also only susceptible to attack when you are actually on the Internet.

What can I do to prevent hackers from scanning and manipulating my system?

Here are some helpful tips for preventing hacker intrusions:

1. Anti-Virus programs are a *necessity*. These programs will serve as a first line of defense against anything a hacker tries to introduce into your system.
2. Use Firewalls. A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the

Continued on page 3

Firewalls: The First Line of Defense

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

Think of it as the Internet's Customs and Immigration. The firewall is the agent that checks each item entering or leaving the network. Each item must pass the right criteria in order for it to pass through the firewall. So a hacker attempting to enter the network of California with a Florida orange would be stopped at the border.

There are three major types of firewalls:

- A **packet filter** looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- A **proxy server (also known as application gateway)** intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Proxies forward messages between clients and servers by appearing to the client (e.g. a Web browser) as a server and appearing to the server (e.g. Web server) as a client. Hence, the client talks to the proxies, which then decide whether the communication should be forwarded to the server. If the communication is deemed acceptable, the proxies contact the server and forward the messages to it.

Proxies can handle complex protocols, which packet filters cannot, because they implement a complete set for a client and a server for each protocol. The drawbacks are performance and limited number of supported protocols.

- **stateful inspection** combines the speed and broad protocol support of packet filters with the security and support of complex proxies. It does it by inspecting all the traffic, looking for security-related information, and using this security-related information to make smart decisions regarding which traffic should be accepted and rejected.

In practice, many firewalls use two or more of these techniques in concert.

For more information on firewalls, and purchasing firewalls visit:

www.symantec.com/product/home-is.html

or

www.mcafee.com/

Your Business Card Here...

ADVERTISE WITH UIS
Info@LightHead.com

Continued from page 1 Introduction To Hacking

cracker *n.*

1. A malicious meddler who tries to discover sensitive information by poking around. Hence "password *cracker*", "network *cracker*."

The *Cracker* is the manifestation of hacking that is so widely feared. A *Cracker* can cause disruption to everything from home computers to the massive servers keeping the Pentagon humming. The difference lies in the victim's defenses. While it is possible to detect and prevent a *Cracker* from violating your home computer, intrusions typically go unseen, undetected, and unpoliced. These intrusions range from simple information gathering programs that search your system for passwords, credit card numbers, and most often, your IP address, to fraud, vandalism and complete destruction.

Your best line of defense against hacking is knowledge. We will explore measures that anyone from a business owner to a PC user can take to prevent malicious attacks.

sneaker *n.*

1. An individual hired to break into places in order to test their security.

Who better to test your system? These hackers apply their knowledge to guide businesses and clients into hacker-safe waters.

Hackers storm White House Web site

While government and FBI representatives would not confirm whether the site was indeed under a denial-of-service attack, two Internet service providers said they found evidence of a coordinated strike, May 4th, on government information servers that support the site.

Between 5 a.m. and 8 a.m. PDT, page requests to the Whitehouse.gov address went unanswered, said Dan Todd, chief technologist for public services for Internet performance service Keynote Systems.

"The type of errors we were seeing was indicative of extremely heavy traffic to the Web site or a denial of service," he said. The attack continued, but with less success, until about 10 a.m.

So-called denial-of-service attacks overload a site's servers with a flood of data, effectively blocking surfers from accessing any files on the targeted computer. Distributed versions of such attacks--where the online vandals use tens, hundreds or even thousands of compromised servers to automate the flood of data--are harder to stop.

In February 2000, such distributed denial-of-service attacks crippled Yahoo, CNN.com, ZDNet and five other major sites for several hours at a time. In January 2001, Microsoft fell prey to attacks after the software giant's sites were taken offline by several technical glitches.

Internet security company iDefense confirmed that the site suffered an outage, but stopped short of characterizing it as a DDoS attack. Michael Cheek, the director of intelligence production at iDefense, added, however, that pro-China hackers on Friday had been planning an attack on Whitehouse.gov, according to information gathered by the company.

Mark Costlow, co-owner of ISP Southwest Cyberport, said the company's technicians identified six customers' servers that were loaded with tools that could be used for such a DDoS attack. The servers were sending data to Whitehouse.gov early Friday morning.

"From these servers--and some of them have already been shut off--we were seeing 3 megabits per second of traffic," he said. "Not that much for a denial-of-service attack, but enough for us to notice and to saturate certain links."

The attack began around 6 a.m., Costlow said. He said that the data sent to the Whitehouse.gov servers, known as ICMP (Internet control message protocol) data, is generally used to report errors and test connections.

"All six servers were aimed at the same White House IP address," Costlow said. The IP address corresponds to one of the Whitehouse.gov Web servers.

Costlow added that the data flood could easily be traced back to the company's site, because the attack tools did not camouflage the source of the attack. However, Costlow could not immediately identify who was controlling the compromised servers. Within two hours, the company had identified the hacked servers and shut them down.

Continued from page 1 Should I Be Wary of Hackers?

firewall, which examines each message and blocks those that do not meet the specified security criteria.

3. If you use DSL, T1, or a Cable Modem connection, make certain to shut down your computer after each use. These connections are continuous and give hackers access to your system whether you are online or not.
4. Internet Relay Chat (IRC) programs are a common doorway hackers choose to access your system. The most common IRC programs are ICQ, Yahoo Messenger, and AOL Instant Messenger. To protect yourself, set your (IRC) preferences to hide your IP address.
5. When manufacturers are informed of vulnerabilities in their software they create *patches* to cover these vulnerabilities. These patches can be downloaded directly from the manufacturer. By joining the manufacturer's mailing list, you will be informed of all current patches.

**"Where can I find
more information
and protect myself?"**

A Complete Hacker's Handbook

By Dr K. & Dr. X.

ISBN:1858684064

find it at

SaveByClicking.com

NEXT ISSUE: COMPUTER VIRUSES

Publisher: United Internet Services, Inc.

Editor in Chief: William M Brandon

Editor@LightHead.com

Production Manager: Daniel Ramos

Dramos@LightHead.com

**For more information visit: LightHead.com
or call: 718-788-1086**

**United Internet Services, Inc. in conjunction with
Liberty Computing Center and LightHead.com is
due to launch a High Tech Incubator in Brooklyn, New York.**

**For more information about this or other projects please visit:
www.LightHead.com/incubator.htm or call: 718-788-1086**

The Incubator will look for companies with strong technology offerings such as computer consulting, ISP, Technical service, programming, e-commerce, communication, and other products and services with breaking technology. The center will be the ideal launching pad for entrepreneurs and inventors looking to develop innovative services and products while maintaining a low overhead in the critical startup stages.

For more information visit: www.LightHead.com/incubator.htm or call: 718-788-1086

Can't afford a full time computer specialist? Are you paying big bucks to a technician who spends most of his/her day playing solitaire on your system? If you answered YES to any of the above questions, then outsourcing is your solution to getting the job done at the right price. United Internet Services Inc. provides computer outsourcing for all of your needs. From recommending which computer is best for your needs to setting up complicated networks and giving you Internet presence with e-commerce accounts and shopping carts.

Outsourcing: www.LightHead.com/Outsourcing.htm

We offer a variety of computer training programs to help individuals, non-profit organizations, small businesses and corporate America understand the needs and the know-how of today's information technology demand.

Training: www.LightHead.com/training.htm

United Internet Services, Inc.
P.O. Box 320
Brooklyn, NY 11215

To:
