

In the Realm of Hacking

by

Chaelynn M. Wolak
wolakcha@scsi.nova.edu

A paper submitted in fulfillment of the requirements
for DISS 740 - Assignment Four, Task One

School of Computer and Information Sciences
Nova Southeastern University

January 27, 1999

Abstract

Internet breaking and entering is on the rise. In this breaking and entering crime, there is hacking. Hacking is a term in the online world that spells trouble. These days, the law takes hacking very seriously. One could find themselves behind bars for quite some time. This research paper briefly describes the language of hacking and just how easy it is to find information about you. In addition, it also briefly describes how to prevent becoming the next victim on the hacker's list.

In the Realm of Hacking

Gregory Adam, 33, pleaded guilty to milking Internet Service Providers (ISPs) and long distance heavyweights out of \$9 million. How? He signed up for 125 toll free '800' numbers and then resold them to Net service providers. Evans never even paid AT&T or MCI for the '800' lines either. After one month of service, the telephone companies cut off the service. Thus leaving the ISPs to face angry customers and AT&T/MCI to foot the bill.

Gregory Adams ran a company called Connect America utilizing those '800' numbers. He portrayed himself as a toll-free number broker where the ISPs would pay a few thousand dollars for a number. On Monday, November 23, 1998, Evans plead guilty to federal conspiracy and wire fraud charges, for using false names and billing addresses to run the operation between November 1996 and June 1997. "The victims - located in various states including Idaho and Oregon - will have to be repaid. The bulk of the redress will go to AT&T, which was stuck with most of the unpaid bills for Connect America's '800' numbers" (Macavinta, 1998).

It is Sunday, September 13 and the Starr report has been out on the Internet for two days. Hackers had left the New York Times site out of commission for nine hours and left some features inaccessible for days. "The attack came during a weekend of record volume for the Times site; the Starr report had been released two days earlier. The vulnerability of the Times left observers wondering whether this was just the beginning" (Phipps, 1998).

Hackers did not break into the New York Times site for credit card numbers. No, the primary motivation was these people had an ax to grind. "They wanted to complain that jailed fellow hacker, Kevin Mitnick, got a raw deal from New York Times technology reporter John Markoff" (Phipps, 1998).

Lastly, two teenage boys, age 16 and 17, hacked into the United States Pentagon site. "The two hackers, who have not been officially identified, pleaded guilty in July to charges of juvenile delinquency stemming from a string of cyber-attacks in February which set alarm bells ringing over the state of U.S. computer security. After an intensive investigation by the FBI, the Defense Department and NASA, all alarmed over hacker assaults on sensitive military and institutional computers, the boys were cornered on February 25, when FBI agents descended on Cloverdale, about 75 miles north of San Francisco, searched their homes and seized computers, software and printers (Reuters, 1998).

These stories are just a few of the havoc hackers are reeking through the Internet. It seems that security breaches are on the rise. No network is safe - not even the personal computer you have sitting at home in the office plugged into the telephone line. This research paper briefly describes the language of hacking and just how easy it is to find

information about you. In addition, it also briefly describes how to prevent becoming the next victim on the hacker's list.

Hacking

To fully understand a network security breach, the language of hacking needs to be defined. Most news stories deal with computer crimes either involving password cracking, money extortion, worms, or viruses. In the world of hacking, there are crackers. Cracking is someone who breaks into computers. "Crackers should not be confused with hackers. The term cracker is usually connected to computer criminals. Some of their crimes include vandalism, theft and snooping in unauthorized areas." Crackers use cracker tools. Cracker tools are programs that are used to break into computers. "They include password crackers, trojans, viruses, war-dialers, and worms" (Anonymous, 1998).

As in the Connect America case, joyriding was exhibited. Joyriding means hacking into an ISP or phone service to obtain free unauthorized usage. Other common terms in hacking include logic bomb, password cracker, phreaking, sniffer, snooping and spoofing. A logic bomb is "a virus that only activates itself when certain conditions are met. Logic bombs usually damage files or cause other serious problems when they are activated." Password cracker is a program that uses a dictionary of words, phrases, names, etc to guess a password. Phreaking is breaking into phone or other communication systems. Sniffer is "a networking tool that can capture data as it goes through the network. Sniffers are often programmed to search for and decode specific types of information. Snooping is passively watching a network for information that could be used to a hacker's advantage, such as passwords. This usually done while 'camping out'" (Anonymous, 1998). Lastly there is spoofing. Spoofing means to penetrate a computer by posing as an authorized user.

The underground world is full of terms - a language only known to those who hack. Other methods used to penetrate networks include portscanners, nukers, pingflooding, IPspoofing, and Trojan horses. Portscanners look for open Internet and fax/modem ports. Nukers flood those same ports with data and render them defenseless to intrusion. Pingflooding shuts down the firewall server by flooding it with too many requests for information. IPspoofing are machines that are tricked into thinking the attacker's machine is another trusted machine on the network. Lastly Trojan horses are hidden executable codes such as mail attachments.

"At DEFCON (an annual hacker conference) in July, a hacker group called Cult of the Dead Cow unveiled Back Orifice, a Trojan horse that allows anyone sitting at a remote location to watch and control all machines connected to a network. Businesses should be particularly afraid of this one. There are versions [of Back Orifice] that are now packed with the e-mail buffer overflow flaws found in Microsoft, Netscape and Eudora Mail products. With these, a victim would have no conceivable clue that his machine was attacked" (Anonymous, 1998).

As the Information Age progresses into the next century, security is a vexing problem. In a recent computer security study, security breaches were up 16 percent from 1996 to 1997. The computer crime related breaches had cost 241 surveyed organizations \$136 million last year. "Another study released showed personal security to be of paramount interest to Internet users" (Festa, 1998).

"To be perfectly honest, anything connected to the Internet in any way, shape or form is vulnerable, says Micah Noland, a freelance computer-security consultant for Fortune 500 companies, based in Schaumburg, Illinois. Depending on the security, some systems are more vulnerable than others, but anyone with the correct knowledge, patience, resources and determination can break into a system connected to the Internet or outside phone lines. Experts agree that the only way for a computer system and its contents to be safe from attack is to be completely isolated from any external access. Isolated doesn't mean behind a firewall. It means being completely disconnected from any outside source" (Laabs, 1998).

Information about You

So you have decided to take heed and disconnect yourself from the outside world. You feel safe; no one will be able to get into your personal computer. Besides, this will be the last time you leave your computer connected into the phone jack all night. Well, there's more. Just recently a solicitation from Information Ltd. of St. Louis, Missouri promises "You can easily learn how to investigate and learn everything about your employees, neighbors, friends, enemies or anyone else. The sender offers a 'kit' in exchange for \$18 (yes, only \$18) that shows you how to look up unlisted phone numbers and locate social security, birth, adoption and death records" (Kenworthy, 1998).

You will be amazed to learn that sensitive and important information about YOU is just a click away. "The scary part is it's true-and you don't need to spend \$18 up front to get most of this data. The only pieces of information about you that are protected by the federal law are your cable TV and video store records, and your credit report. All an individual needs to find the rest - your social security number, your addresses past and present, your date of birth, your medical records, your motor vehicle records - is a web browser and some cash" (Kenworthy, 1998).

The Internet - the gold mine just waiting to happen. Yes, the Internet opens up a world of opportunity for that one lazy hacker. Listed below are sites that can and will provide information about you:

| <u>Name</u> | <u>URL Site</u> | <u>Services Offered</u> |
|------------------|---|--|
| 1-800-U.S.Search | http://www.1800ussearch.com | Current address - \$79.95 Background check - \$139.95 |

| | | |
|----------------------------------|---|---|
| The American Information Network | http://www.ameri.com | SS # - \$20 Worker's compensation records - \$25 Bankruptcies, tax liens, judgments - \$35 |
| A1-Trace U.S.A. | http://a1trace.com | Info Probe - \$79 |
| Discreet Data Research | http://www.discreetdata.com | Skip tracing - \$300 (an all out search for an individual who is really attempting to vaporize from society) |
| Discreet Data Systems | http://www.discreetdatasystems.com | Non published phone # - \$65 Complete asset research - \$650 |
| Public-Records.Net | http://www.public-records.net | SS # - \$15 Current and previous address - \$15 License plat of VIN trace - \$35 |
| Lycos Network People Finder | http://www.whowhere.com | Phone number, address, and driving directions - FREE. |

The above information is provided by Karen Kenworthy and Nancy Lang of Windows Magazine Online (1998). These are just a sampling of the vast ways individuals can find information about you. You just will not be able hide anymore.

Better Security

The stories and vast array of information can make you feel defeated when it comes to network security and in general your own personal security. It seems as though data is just a mouse click away. However there are ways to protect yourself and your networks. The information described in this section is just some of the tricks of the trade.

For example if you want to make yourself less likely to be on the hacker's hit list, here are some general rules. First watch your mouth. "If for no other reason than to avoid being

bombarded with junk mail, avoid discussing your union problems at health forums or your penchant for antique clocks at a collectors forum" (Kenworthy, 1998). Second, stay informed. Third, keep information to yourself. Don't trust anyone with your secrets. Fourth, poll your favorite web sites. Be informed as to how the web site is going to use your information. Fifth, drop out of cybersociety. Take steps to lower your profile. Sixth, dig up that old decoder ring. Encrypt your email messages. Lastly, go anonymous. "Another powerful cloaking device is an anonymous remailer, which keeps your name and e-mail address a mystery to others" (Kenworthy, 1998).

Another technique to combat the rise of hacking is sharing. Information sharing can improve security. "Several online clearinghouses do provide some information on publicly known software weaknesses and attack methods. The various Computer Emergency Response Team organizations around the world compile their information, and much of it is posted online at Carnegie Mellon's CERT Coordination Center website <<http://www.cert.org>>. A similar organization called the Forum of Incident Response and Security Teams shares information between government, academic, and some commercial members <<http://www.first.org>>" (Borland, 1998). Lastly, another web site where individuals can responsibly discuss and learn about hacking and computer security is AntiOnline <<http://antionline.com>>.

Well if you still do not feel as if you have a handle on network security. You can always buy a hacker policy. None other than Cigna Insurance <<http://www.cigna.com>> is providing the world's first hacker insurance called Cigna's Secure Systems Insurance. "The cost? \$12 million worth of coverage recommended, say, for a retailer or a manufacturer with \$100 million in revenues and average risks will cost between \$20,000 and \$25,000 a year. That covers external intrusions only, not inside hacker jobs" (Moukheiber, 1998). If this does not sound appealing, then you can do what other individuals do, install a firewall and monitor, monitor and monitor.

Conclusion

Each day the Internet becomes larger and larger. As more computers, business and personal, come online it is inevitable that someone will try to break in. It is very similar to the world you are currently living in. Crime such as shoplifting, bank robbing, pick pocketing are part of the living world. In the electronic world, hacking and cracking are just another form of crime. It seems to be part of every environment whether it is online or offline. The key is to make yourself aware. Security breaches can be stopped and prevented. There is an enormous amount of information and forums to help you better your security. Thus, the next time you are online, beware, someone could be hacking you!

Reference List

- Anonymous. (1998, October). The language of hacking. *Management Review*, 87, 18.
- Anonymous. (1998, November 2). Not rocket science. *Industry Week*, 247, 25.
- Borland, J. (1998, September 25). Crackers ahead in online security arms race. *CMP Net*. <http://www.techweb.com>. Accessed November 30, 1998.
- Festa, P. (1998, March 5). Computer security problems growing. *CNet News.com*. <http://www.news.com>. Accessed November 30, 1998.
- Kenworthy, K. and Lang, N. A. (1998, December 1). How safe is the Net? Using the Internet can be hazardous to your data's health. We reveal the risks, and show you how to keep your corporate data as well as your personal information safe and secure. *Windows Magazine Online*. <http://www.techweb.com>. Accessed November 30, 1998.
- Laabs, J. (1998, November). Web site hacking incident highlights need for HRMS security. *Workforce*, 77, 18.
- Macavinta, C. (1998, November 27). Man admits scamming millions from ISPs, telcos. *CNet News.com*. <http://www.news.com>. Accessed November 30, 1998.
- Moukheiber, Z. (1998, November 16). Got a hacker policy? *Forbes*, 162, 77.
- Phipps, J. L. (1998, November). Hackers: Can you stop them? *Editor & Publisher*, 4.
- Reuters. (1998, November 6). Withdrawal ordered for U.S. Pentagon hackers. *ZDNN*. <http://www.zdnet.com>. Accessed November 30, 1998.