The 'Net Threat

BY ANDREW SCHILLER

We are entering an age where information is the prime asset and every network is accessible by some manner of remote access. Internet access is becoming ubiquitous and therefore the prime target for hackers.

HE'S 17 years old and looks it. His earrings jangle and his disheveled hair sways as he walks. He wears a sleeveless T-shirt and blue jeans several sizes too large. He knows more about computers than is legal in most states. He is a hacker, a "2600," warez cyber-warrior. By his own admission, he's been a hacker since he was 11 years old!

Now, I know what you're thinking — a punk, a vandal, no big deal. Wrong! This guy is a big deal. He and thousands, maybe hundreds of thousands, like him exist all over the world. You and your company's networks and systems are their oyster. You've erected firewalls and installed intrusion detection. You're safe, right? Think again.

As security professionals, it's our job to identify the enemy and his tools. I'm paid to protect my clients. However, how can I protect them against an unknown enemy? That's why most of us use auditing tools such as SATAN, ISS, or the IBM Audit Toolkit that allow us to find any weaknesses in our system or network security. IBM hasn't released its most potent version of the auditor to me yet even though I'm an IBM Certified Firewall Expert. Unfortunately, the hacker community claims it has had the IBM tool for two months; they stole it. It's important that you learn about the tools of the trade in the hacker counter-culture. It will scare you into getting much, much better at what you do.

Let's define some convenient, if not totally accurate, terms for the sake of common ground. Semantics is a favorite subject of debate among self-professed hackers. A "hacker" is a person who is trying to remotely access information on your network. A "phreaker" is a person who is trying to gain access to an outside dial-tone on your PBX phone system for the purpose of making voice and/or data calls that are both free and untraceable. A "cracker" is a person who is trying to take control of your computing resources by gaining "root" access and locking you and your customers out of the system. Hackers are mostly harmless unless they're clumsy, stupid or inept. Mostly they're just kids with too much knowledge and not enough homework who are looking around inside various computer to learn more about how they work. Phreakers are thieves responsible for about $15 billion worth of stolen network service a year.[1] Crackers are misanthropes bent on self-aggrandizement through the conquering of ever more secure systems. They are the enemy.

The fact is, no one is immune from hackers, phreakers and crackers. No one is exempt. The bigger your company, the more attractive you are to crackers. The more secure you ought to be, the more of a target you become. To wit, the Pentagon is the most attacked site in the world by both hackers and crackers. Their goals are different as befits their genre. Hackers just want to get in and look around the system; maybe they'll even leave a calling card. Crackers want to get in and take over; to wreak havoc.

To be sure, dozens of factions of hackers, crackers and phreakers exist in clannish forms. You will see USENET forums for "warez" and "2600" members and subcults. This article will focus on hackers and crackers in general and the their tools of choice. You and I need to know what we are up against.

WHAT WE'RE UP AGAINST

Access to your systems can be gained through the Internet,modem or via physical site incursion. For the purposes of this article, we will focus on Internet attacks. Modems are a whole story in themselves. Suffice it to say, don't put modems on anything but

1. According to a quote from Bill Seymour, managing director of Nortel,from the article, "Telecom Fraud Software Looks and Learns," by Andrew Craig (*Tech Web*, CMP, April 29,1998).

Figure 1: Hacker Archive Web Sites
rootshell.connectnet.com
www.fini.org/fini/english/index.html
neworder.box.sk

Figure 2: Insecure Protocols in UNIX
anonymous file transfer protocol (ftp)
trivial ftp (tftp)
Network Information Service (NIS)
Remote Procedure Calls (RPC)
mail
finger
showmount
Network File Services (NFS)

Figure 3: WinNuke

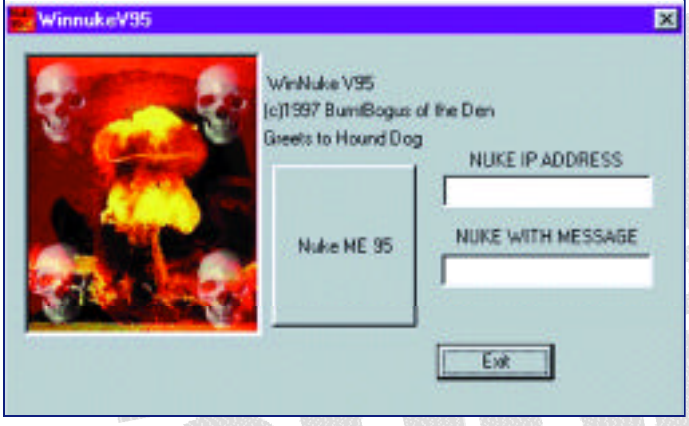
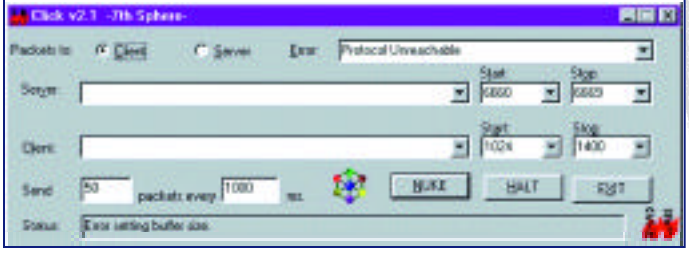


Figure 4: Click



a secure, remote access hub or firewall with strong authentication. Anyone who has worked late has probably noticed dial-up attacks. While annoying, these attacks are only a means to the end of cracking into a server. Physical incursion is also a subject beyond the scope of this article. Social engineering, moles, disgruntled employees and the like are a security nightmare. This will be the topic of a future article.

Our subject is the cracker and the tools of his trade. Not all crackers and hackers are men, of course, but the vast majority are male. Hackers, both ethical and outlaw, primarily work in groups modeled after military insurgency forces called "tiger teams." Tiger teams provide a number of advantages. Many different attack strategies can be tried simultaneously. Any weakness, once found, can be used by the whole team to focus the ferocity of the attack. Less knowledgeable team members learn from more experienced peers. The attack evolves until system penetration has been achieved. The chief goal, it appears, is verification of a successful attack also known as an "escapade." The escapade is then published on a bulletin board system (BBS),advertising the success to the hacker community. A list of easily accessed web sites flaunting these escapades is shown in Figure 1.

We are entering an age where information is the prime asset. Insecure information is worthless. Internet access is becoming ubiquitous and therefore the prime target for hackers.

What happens next depends on whether you hired the team that attacked you. If so, perhaps your boss wants "proof" that control could be wrested from you. If not, you have either a peeper on a mission or a sociopath with "root" access. A peeper is either there for educational purposes or for espionage. The sociopath is there either to conquer and seize control or to wantonly destroy your data. What do you do?

You may have heard about SATAN and its derivative SANTA. The subtle differences in name are not totally by accident. Both are public domain, ethical hacking tools. That is to say that both are intended for use by security personnel to harden their systems. More serious security personnel with funds to purchase ethical hacking tools know about ISS and the IBM Audit Toolkit. All of these are seriously powerful tools. None will cause damage to a network under study. Each will expose weaknesses in a network or system through which a potential hacker or cracker may enter. The nature of the weakness will determine whether the entry point is a "hack" (pain), a "crack" (loss) or a "kill" (death). The entire hacker community has access to these tools. You are foolish if you haven't run these base audits against your systems and networks or hired someone to do it for you.

After running basic audits, the next step is to secure or eliminate all unnecessary protocols which are hacker targets. A list of vulnerable services for the UNIX operating system is shown in Figure 2.

TOOLS OF THE ROGUE

To supplement the "ethical" tools, our egalitarian bands of digital Robin Hoods have run off into the cyber-hinterlands and built vicious tools of their own. Let me introduce you to a few of the more popular and most dangerous of these incursive programs. You will see that, in general, they are well conceived, expertly rendered, and awesomely effective. Many are simple, almost childlike to implement, as a courtesy to the less experienced hackers. Most are Windows 95- or DOS-driven. All are devilishly clever. Some provide the "crack" after the successful "hack" as an option. Other products offer a "kill" option that will wipe out the target system. Gather round, we're going to school....

© 1998 Technical Enterprises, Inc. Reproduction of this document without permission is prohibited.

Figure 5: F-ed Up

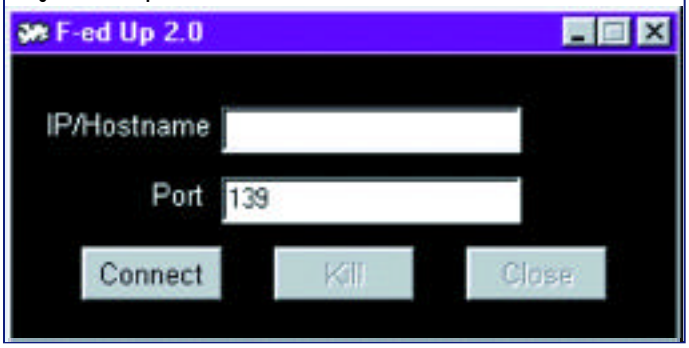


Figure 6: Port Pro

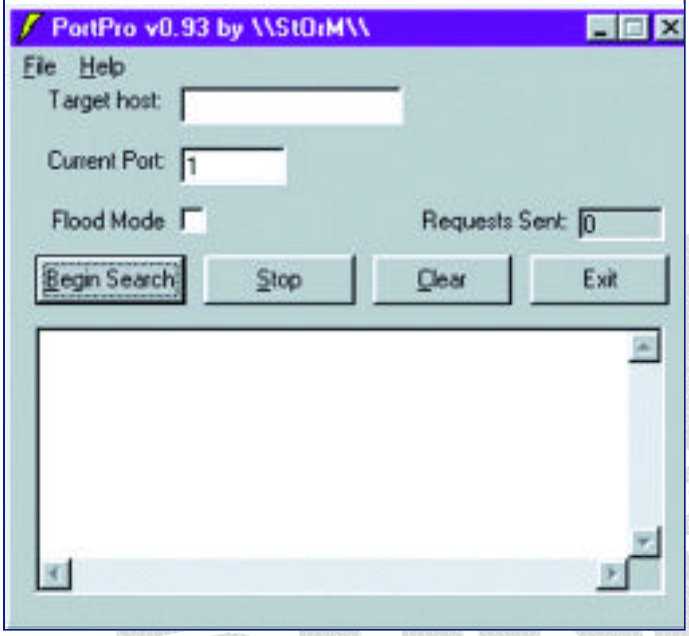
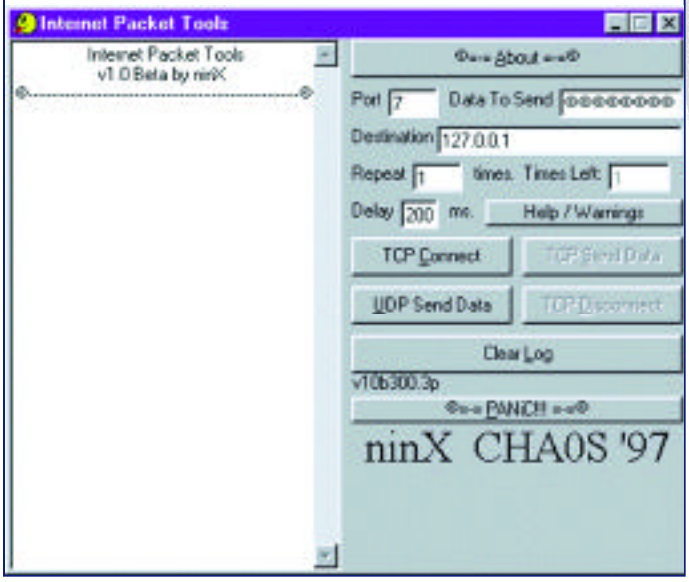


Figure 7: Internet Packet



WinNuke: This little gem is also dressed up to the nines with a GUI interface (Figure 3) for advanced Microsoft platforms. It will flood port 139, which is NETBIOS over TCP/IP, and take down many Windows NT or 95 systems. Have you checked your port 139 lately?

Click: Just point at a client with an IP address or a server with the URL and "click," it's dead from an ICMP (Internet Control Message Protocol) attack. Click (Figure 4) has evolved but the writers are no longer in existence (sic?). Don't ask.

ICMP Watch: Another work from the authors of Click. This is the real-time defense against Click. Apparently, there is no honor among thieves; they even have to protect their own systems.

F-ed Up: First hackers or crackers find a port you aren't using or protecting. Then they pull out F-ed Up (Figure 5): Lock and load. This nails Windows NT 3.5x systems.

PortPro: This is an automated port scanner that finds your weaknesses. It contains options in the GUI (Figure 6) for flooding the ports. The product runs like wildfire and is difficult to stop. It reminds me of a fire hose. The end result is a denial of service attack.

Internet Packet: As shown in Figure 7, the Internet Packet will attack a vulnerable port mercilessly with data packets and fragments, bringing your system to its knees. Close all udp ports unless absolutely necessary. Close all tcp ports that aren't actively being used by your customers.

Net Cat: This is the "Big Gun," and is not for use by "lamers" or "newbies." Experienced hackers can use this Swiss Army knife to snoop on any port on your system or steal your password file to gain root access. Net Cat runs in DOS and is not fancy. Commands are obtuse and the syntax is terse. Unlike the other tools, you never know what to expect from something as agile as Net Cat.

Sir James Murray wrote, "Knowledge is power." Who has more knowledge, the predator or his prey? We are the prey. Hackers and crackers are the predators. Power would arguably fall in favor of the antagonist.

THE BEST DEFENSE

The best defense I can recommend in the face of this conclusion is that "war games"are in order. Test your defensibility. Hire a tiger team. Find your weaknesses before they are used to affect your demise. Don't trust your security vendor to do it for you. Run the audit a least once a year. I recommend quarterly, unannounced audits. New attacks are being devised weekly. If you don't believe me, review the following archives:

- CIAC (the computer security service for the United States Department of Energy http://ciac.llnl.gov])
- CERT (Computer Emergency Response Team [www.cert.org])
- COAST (computer security research program at Purdue University [www.cs.purdue.edu/coast])

Discretion being the better part of valor, back up everything religiously. Review your security logs daily. If not, then don't even bother backing up your systems. Once corrupted, you will only be archiving already defiled data. Restoring it won't help. You have to

© 1998 Technical Enterprises,Inc. Reproduction of this document without permission is prohibited.

know when the corruption occurs by reviewing logs constantly and by watching for illicit activity on sensitive files using an enterprise management tool. Since this is heady stuff and it burns lots of resources, you may want to consider outsourcing.

A solid defense is recommended in this neo-Medieval conflagration with its firewalls and bastion hosts. No host or network is impenetrable. But sloppy defense or leaving the keys to the "kingdom" on the proverbial doorstep is certain defeat.

We are entering an age where information is the prime asset. Insecure information is worthless. Internet access is becoming ubiquitous and therefore the prime target for hackers. Don't resist the movement to the Internet. However, be careful. Hackers are out there and they are the threat on the 'net. ts

Andrew Schiller is the owner of PCPI, an IT outsourcing firm providing firewall and systems management over the Internet. He is a Certified Firewall Expert, industry consultant, and lecturer. His 25 years in the computer field has included many pioneering efforts in computer-aided manufacturing, global network architecture, and telecommunications. Mr. Schiller can be reached at (248) 855-2615 or at datadr@ibm.net.

©1998 Technical Enterprises,Inc. For reprints of this document contact sales@naspa.net.

technical® SUPPORT
Supporting Enterprise Networks and Operating Environments
NaSPA