This column focuses on secure computing, providing tools and tips for those in the information security trenches. Each issue, we'll evaluate new technologies (primarily in the open source space) and discuss ways to integrate them into your organization.

We want to hear from you. Got a great utility or "magic" script that's saved you hours of tedious keyboard pounding? Something new we haven't heard about? Let us know at ciocorner@sandstorm.net.

Prosecution or Protection

The desire to increase the security of a system demands that compromises be made with the usability of the system. In the information security field, it is a cliché, but a truism: The only way to have a truly secure system is to bury it 10 feet under ground with the power off. Of course, in this scenario, the system is rendered useless.

In addition to the problems raised by the necessity of usability, the traditional deterrent of prosecution is difficult to transition to an online environment. The global nature of the Internet raises many questions of jurisdictional authority. Soafer and Goodman, in "The Transnational Dimension of Cyber Crime," believe that the global Internet suffers from two primary weaknesses:

1. [The Internet is] a worldwide target pool of computers and users to victimize, or to exploit in denial-or-service or other attacks, which enables attackers to do more damage with no more effort than would be necessary in attacking computers or users in a single state.

2. The widespread disparities among states, in the legal, regulatory, or policy environment concerning cyber crime, and the lack of a sufficiently high degree of international cooperation in prosecuting and deterring such crime (2001, p. 6).

So if we can't prosecute, what can we do? Being that prosecution occurs after the fact, prevention of computer crime might be the best place to start.

COVERING THE BASICS

In order to secure your organization, you must first identify the threats you face. The Internet is a global community. As such, the motivations of its members are extremely varied. For the purposes of securing your information systems, we must be principally concerned with the hacker subset of the Internet community.

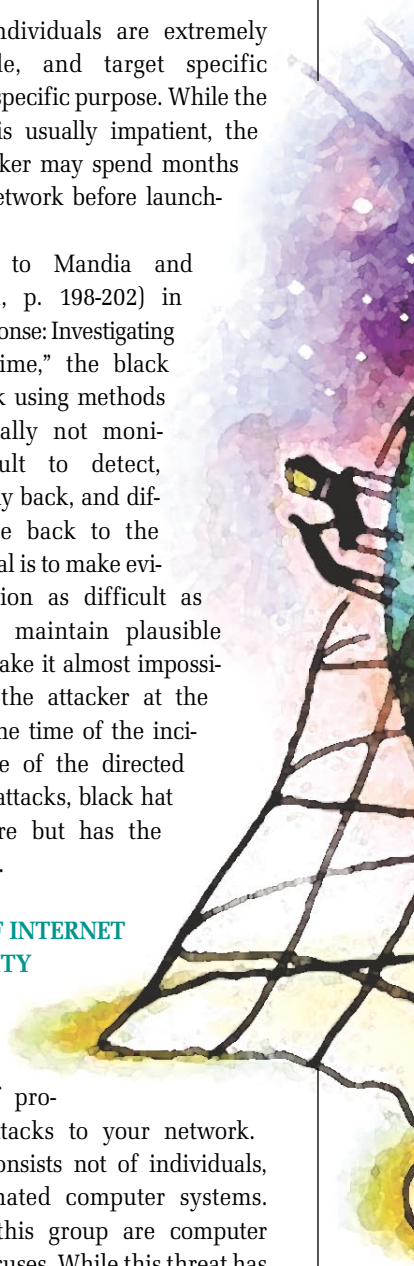
The first category of hackers found on the Internet is referred to as script kiddies. Their defining characteristics are a lack of experience and maturity. The term script kiddy comes from the practice, common among this group, of running scripts (human readable code that is interpreted by an intermediary application, rather than compiled machine code) written by knowledgeable security professionals in order to compromise machines. This is done with little understanding of the workings of the exploit.

This group is motivated by infamy. The goal of script kiddies is to break into any system they can, primarily to claim bragging rights. In addition, they may use a compromised system to store files, such as movies, music or pornography. More sophisticated script kiddies may use compromised systems to launch attacks (such as a distributed denial of service attack) against other networks.

The lack of experience found among this group makes them relatively easy to detect. They will usually give up if the particular attack they are trying to execute does not work, which minimizes the risk they pose to your organization.

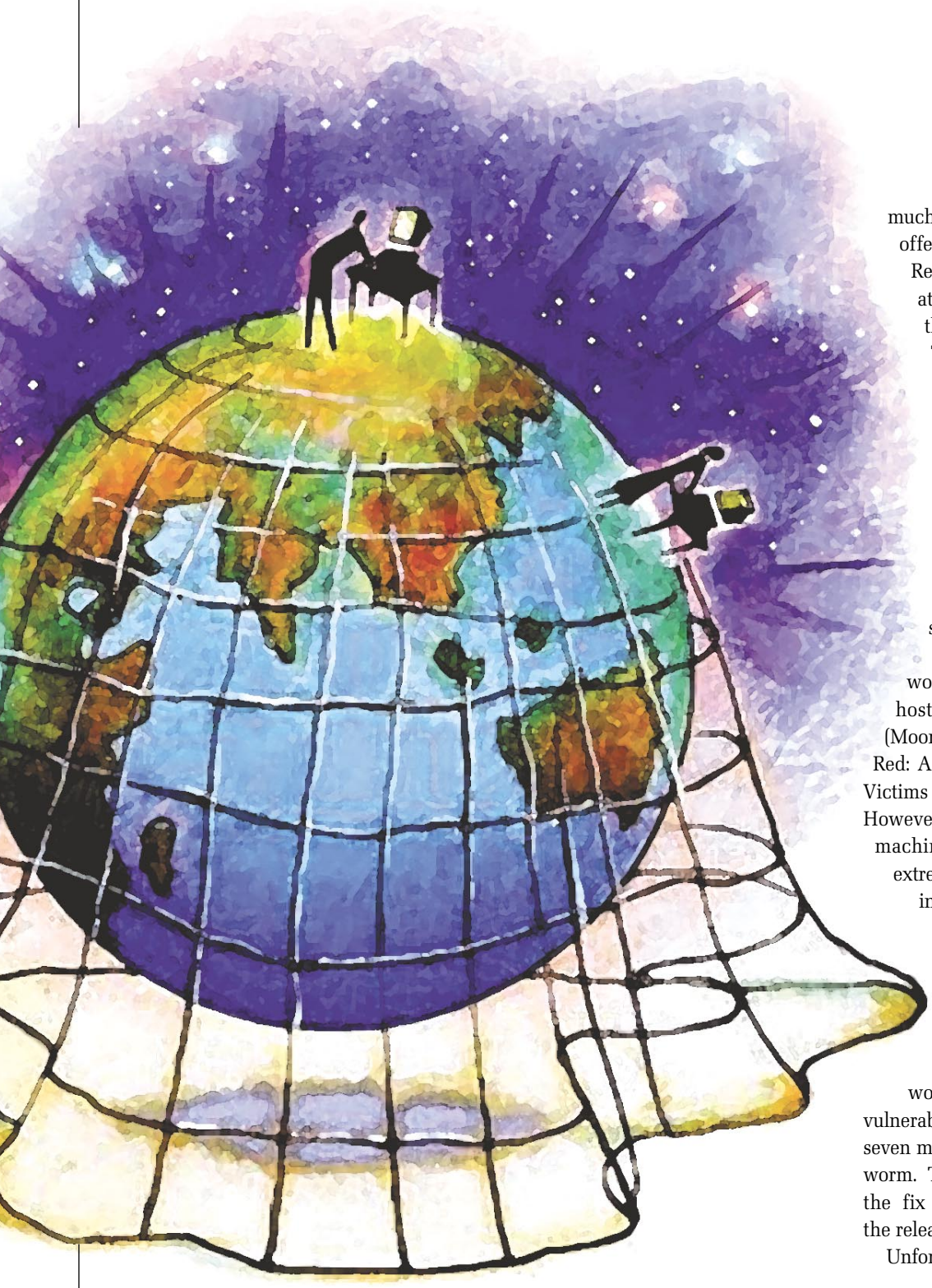
The second category of hacker found on the Internet is known as the black hat. These individuals are extremely knowledgeable, and target specific systems for a specific purpose. While the script kiddy is usually impatient, the black hat hacker may spend months watching a network before launching an attack.

According to Mandia and Prosise (2001, p. 198-202) in "Incident Response: Investigating Computer Crime," the black hat will attack using methods that are usually not monitored, difficult to detect, difficult to play back, and difficult to trace back to the source. His goal is to make evidence collection as difficult as possible and maintain plausible deniability (make it almost impossible to place the attacker at the keyboard at the time of the incident). Because of the directed nature of his attacks, black hat activity is rare but has the largest impact.



DANGERS OF INTERNET CONNECTIVITY

Internet connectivity also brings the threat of programmatic attacks to your network. This group consists not of individuals, but of automated computer systems. Included in this group are computer worms and viruses. While this threat has existed for some time, it has received



much notoriety in recent years with offenders such as Melissa, Code Red, NIMDA and Sapphire. These attacks are extremely varied in their operation and threat level. The Sapphire worm, for example spread to over 75,000 Internet connected hosts, 90 percent of which were infected in the first 10 minutes (Moore, Paxson, Savage, Shannon, Staniford, and Weaver; The spread of the Sapphire/ Slammer Worm, 2002). However, its goal was merely to spread to other machines.

Conversely, the Code Red worm, which infected 359,000 hosts, took 14 hours to spread (Moore, Shannon and Brown; Code-Red: A case Study on the Spread and Victims of an Internet worm, 2002). However this worm left an infected machine in a state that made it extremely easy for an inexperienced individual (such as a script kiddy) to control it.

Although programmatic attacks are varied, they usually attempt to exploit a single, known vulnerability. The Sapphire worm, for example, exploited a vulnerability addressed by the vendor seven months prior to the release of the worm. The worm propagated because the fix had not been applied before the release.

Unfortunately programmatic attacks

are launched automatically after a host has been infected. Owners or administrators of the infected host are usually unaware of the infections, and of the attacks being launched from their computer. Generally speaking, a worm could be introduced from any location on the Internet and successfully spread across the network.

This makes it almost impossible for law enforcement officials to apprehend the authors of the worm. Consequently damages are unlikely to be recovered following a worm attack. The best strategy for dealing with a new worm is to insure your network is not vulnerable, and block all traffic at the external firewall from infected hosts.

While companies are particularly sensitive to problems from the outside (hackers, viruses, denial of service), often they downplay or deny the potential for harm from within. Employees may be exhibiting inappropriate conduct in the form of harassing email, violating usage policies via visits to gambling or shopping sites during business hours, or engaging in outright sabotage by sending sensitive financial data to a competitor.

SOLUTIONS TO THE PROBLEM

As a company, it is easy to draft policies to cover these events, but difficult to find the misbehavior ... until now. With tools like NetIntercept (www.netintercept.com) or InfiniStream (www.networkassociates.com), you can capture all the traffic on the monitored network, reassemble the packets into connections between machines, and discover employee (mis)behavior before it jeopardizes your company's future. Prosecution of these types of crime is becoming more common; however, in order to be successful here, all of the rules of evidence collection must be followed. Often, damage control and employee termination must suffice.

Laws continue to evolve and eventually they will catch up with the new wave of computer crime. For now, protection and close network surveillance seem to be the best course of action.

Laws continue to evolve and eventually they will catch up with the new wave of computer crime. For now, protection and close network surveillance seem to be the best course of action.

QUESTIONS FROM OUR READERS

On July 14, 2004, Elli Fenner, a student at the University of London, wrote: "I understand that using Knoppix, it is possible to bypass security constraints as it doesn't even deal with the hard drive, but I was wondering whether you could explain how, in fact, it would be possible to put in security constraints to prevent people from attacking a computer using Knoppix?" Her question was in reference to our "Knoppix Rocks" article (www.cyberdefensemag.com/march2004/citech.php).

Well, there are several ways to prevent booting from removable media. System manufacturers provided varying levels of security for boot media, including key-lock and biometric devices. But on the practical side, CD-ROM booting can be disabled in BIOS (which should then be password protected). Or, you could remove the CD-ROM or floppy drives from the machine to make it less convenient for an attacker.

However, if someone is able to use Knoppix to attack a system, he already has physical access. Once an attacker gains physical access, he significantly changes the nature of the threat. He could steal the hard drive, destroy the hardware, or do just about anything with or without Knoppix. If you're concerned about this kind of attack, your best bet is to beef up your physical security.

On the technical side, many operating systems allow the creation of encrypted disk images, which can be mounted and used like a normal disk (with the notable exception that the information being stored is encrypted). Coupled with key-based authentication, disk encryption will safeguard against someone snooping with Knoppix.

Great question Elli and good luck in school. CDM

Walker Whitehouse *is CIO and* **Mike Yamamoto** *is a Network Systems Engineer at Sandstorm Enterprises, which develops aggressive software products for network monitoring, network forensics analysis, and security auditing including telephone scanning, penetration testing, and vulnerability assessment.*