



Get Inside Their

HEADS

Catch cyber criminals by thinking like them

PHOTO COURTESY STEVE HAILEY

hackers approach breaking into computers and networks, as well as how they compromise applications, can beat hackers at their own game.

Hackers Are Systematic

When you get down to it, thinking like a hacker is not much different than thinking like a detective. Good hackers will follow a specific methodology developed over time. They will be patient and will document each step of their work, paying attention to minutia.

A hacker's primary objective is to compromise the intended target, be it a computer, entire network or an application, such as a database used to store credit card numbers. Typically, a hacker starts out with little information about the target, but will soon have a detailed roadmap.

The systematic approach followed by most hackers can be divided into five phases: reconnaissance, scanning and enumeration, gaining access, maintaining access and covering their tracks.

Reconnaissance

In this phase, hackers identify domain names of the target, such as targetvictim.com. Then they gather as much information as possible through public sources. Newsgroups are a good source of data for hackers—information technology (IT) staff ask for help with network/system-related problems and often divulge too much information regarding their configurations and applications. Job announcements often provide detailed information about the company's computer systems, operating systems and applications. If the job announcement is for an information-security position, a hacker can often ascertain the type of network defenses the target has in place.

A quick visit to Internet Archive's Web site (archive.org) can reveal information about the target that goes back years, some of which the target probably wishes was never made available to the Internet community at large in the first place. The Securities and Exchange Commission's Web site (www.sec.gov) may reveal that the target company is merging with another company. This may mean both companies will lower their defenses in order to merge IT

resources and ensure everything works between dissimilar systems—a perfect time to launch an attack.

And, of course, hackers can use social engineering to retrieve data from a person. Social engineering relies on human interaction and often involves tricking other people to break normal security procedures. *Example:* A hacker gains the confidence of an employee authorized to access the network in order to get them to reveal information that compromises the network's security. The hacker might call the employee with some kind of urgent problem—social engineers often rely on the natural helpfulness of people as well as their weaknesses. Appeals to vanity, appeals to authority and old-fashioned eavesdropping are typical social engineering techniques. In short, humans can be an organization's biggest vulnerability.

Once the reconnaissance phase is complete, the hacker possesses a fairly detailed roadmap of the target. Through the public information sources used in the reconnaissance phase, they may have learned domain names, IP address ranges, business partners, phone numbers, types of software and operating systems in use, and network defense mechanisms in place.

Scanning & Enumeration

Now hackers will scan servers and resources on the target network. They can obtain the software needed to do so from literally thousands of so-called "WareZ" Web sites for free. (For expensive, professional scanning tools, a hacker can simply visit one of many Web sites to obtain valid serial numbers or "cracked" versions of the program.) While the intricacies of how to scan a network and obtain detailed information on the systems residing therein remain beyond the scope of this article, suffice it to say that even networks protected by the best firewalls can be had. Once a hacker learns the details of the target operating systems and applications via scanning, finding a way to exploit known weaknesses is often as simple as a visit to a hacking-tool Web site.

Often a computer system will even offer up information concerning password length and whether passwords are even required if a hacker simply

poses the question to the computer in a correctly formatted manner. After all, internal security can be a bit lax—no one would ever make it past the firewall, right?

Gaining Access

With the information gained from the scanning phase, hackers may quickly own the keys to the kingdom. Often they can access systems with complete administrative or root access, allowing them to do whatever they wish. Sometimes gaining this level of access could be as easy as a call to the company help desk and impersonating a manager to get a password reset after an e-mail sent to the manager by the hacker triggered an automatic "out of the office for two weeks" reply. Perfect.

While this scenario may sound a bit far-fetched, it's all too real. I've obtained passwords and password lists from company employees simply by asking them as part of vulnerability assessments and penetrations tests conducted legally. It works. It's amazing what an unsuspecting employee will do for someone with an authoritative tone who apparently signs their paychecks.

If the hacker can't obtain the level of access desired, they may send company employees a Trojan disguised as a service pack or system update—sent from the System Administrator's e-mail account, of course, which they obtained from a newsgroup message during the reconnaissance phase.

The Trojan appears to do no harm, but

when the employees run it, it installs a key-logger program in the background. The program periodically sends the hacker user-IDs and passwords used by the employees throughout the day. By nightfall, the hacker has all of the information needed to gain access with administrator or root privileges.

Maintaining Access

Now that the hacker has access to many critical computer systems, they obtain the password file from them. In the Windows world, this is known as the Security Account Manager (SAM) file, and it contains the user-IDs and passwords for all system users. This literally could be thousands of users.

Once they've obtained the password files, hackers crack them for all users. Given enough time, they can obtain administrative or root access to all computer systems, even though the entire process may have started by compromising a single computer system.

Now hackers install backdoor programs on all of the compromised systems that give them a way in even when the administrator or root account passwords are changed. Using these backdoor programs, the hacker communicates with the compromised systems in such a manner that even experienced IT professionals will see the communication as normal network traffic—completely legitimate.



By Sanjay Bavisi & Steve Hailey

You're a computer forensic examiner for your department, working on a network intrusion case. The evidence you extract from several computers and firewall logs clearly shows the suspect broke through the victim company's defenses and accessed proprietary data.

The suspect claims the activity was due to a Trojan that must have infected his computer system. (A Trojan is a malicious program disguised as or embedded within seemingly legitimate software.) While you or the defense expert found no trace of a Trojan, the defense offers that the Trojan simply wiped itself from the computer after the deed was done. The suspect is acquitted.

Fact or fiction? Many of you reading this have already been involved in similar cases within your department and know these scenarios are all too real. In the realm of cyber crime, members of law enforcement are seeing more and more cases involving network intrusions and hacking.

Fortunately, malicious activity on a computer system leaves a trail. To find it, forensic computer examiners and those prosecuting computer-related crimes need to know how hackers think as well as the methods they use. Armed with this knowledge, you will know what trail to look for on a computer system, and will also be able to help the prosecution dispel any doubts or "what ifs" presented by the defense. The forensic examiner who knows how

THE TROJAN DEFENSE

Thanks to the increasingly common Trojan Defense, more and more defendants will be acquitted of crimes by claiming someone took over their computer via a Trojan horse. In one real-world example, a teenage hacker was accused of crippling the Port of Houston's Web-based computer systems. He claimed attackers used an unspecified Trojan to control his PC and launch the attack against the Port. A forensic examination of the suspect's computer found hacking tools but no trace of a Trojan. The defense argued that it was possible for a Trojan to wipe itself from a computer. After deliberating for three hours, the jury returned a verdict of not guilty.

The validity of the verdict in this case summarized here is not disputed, but concern exists that outcomes such as these may open the floodgates to Trojan arguments in other cases yet to be seen. It's seemingly difficult to counter a suspect's argument that someone else did it and then ran away, clearing their tracks.

This is especially true in criminal cases because the burden of proof is "beyond reasonable doubt." If creative defense attorneys use the Trojan Defense as a doubt-creation tool, it can prove very difficult to overcome.

Forensic examiners should be able to offer either inculpatory or exculpatory evidence to make an intelligent argument either way. Saying that this or that *could* have happened with no supporting evidence would not cut it in the physical realm, and it doesn't in the digital realm, either.

Covering Their Tracks

In this phase, the attacker deletes logs, completely shuts down logging-related activities and replaces programs and processes on the system that could give away their presence and continued activities. In a case I was involved in, hackers went undetected for approximately six months by replacing common computer system utilities with a rootkit—a collection of programs that, among other things, mimic their

genuine counterparts, but only show information the hacker wants system administrators to see.

Training

With tight budgets and many training courses costing thousands of dollars, keeping pace with technology can prove daunting, so how do the folks responsible for processing and prosecuting hacking or illicit computer-related activity learn how to deal with them? *One*

answer: Certified Ethical Hacker training and certification, a professional certification provided by the International Council of E-Commerce Consultants (www.eccouncil.org). A Certified Ethical Hacker course (taken via either self-study or through a training organization affiliated with the Council) teaches the techniques used by hackers and intruders to infiltrate, control and compromise computer systems. It also prepares students to conduct vulnerability assessments and penetration tests of computer systems—finding, documenting and rectifying security problems before hackers can exploit and take advantage of them. In short, the course takes students into the minds of hackers, enabling them to see things from the hackers' perspective.

For forensic analysts and other professionals involved in combating computer-related crime, the knowledge gained from the Certified Ethical Hacker training will go a long way in helping to pinpoint what happened, when it happened and who was involved. **LOM**

STEVE HAILEY is an IT veteran of 23 years, with 16 years' experience developing and delivering technical training. He is president/CEO of CyberSecurity Institute and currently instructs the information security and digital forensics curriculum at Edmonds Community College in Washington. Hailey is actively involved with developing and delivering training in digital forensics to members of city, state and federal law enforcement agencies. He has authored certification practice tests for several vendors and has processed digital forensic cases ranging from inappropriate resource use and network intrusions to cases involving identity theft, credit card fraud, child pornography and money laundering. He's a Certified Information Systems Security Professional (CISSP), a Certified Ethical Hacker and holds more than 20 other technical certifications including one in computer forensics from Oregon State University.

Hailey is also president of the Washington State High Technology Crime Investigation Association (www.wahtcia.org), which offers an intensive five-day Certified Ethical Hacker course to law enforcement personnel.

SANJAY BAVISI, a law graduate from the University of Wales, College of Cardiff, United Kingdom, is a leading consultant, columnist and speaker for many local and international companies and government organizations. He has conducted training and presented papers at numerous events around the world on information security and forensics. Bavisi regularly shares the platform with legislators, policymakers, senior government officials and educators, and his audiences include executives of multinational corporations such as Microsoft, Shell, IBM, S.E.A. Insurance, American Express Bank Philippines and many more.