Know your enemy: Why your Web site is at risk

By Michael Cobb

To the tag line for the Internet -- “Build it and they will come” -- I would add “...and try to crack it, deface it, abuse it, break it and steal it.”

Hackers have more resources and time than even the largest organizations, and they don't suffer from the usual organizational constraints, such as office politics and budgets, that security practitioners face. In fact, hackers can show an almost enviable example of online collaboration, sharing information in order to achieve a result. This article will help you understand the tools, tactics and motives of the black hat community so that you have a better appreciation of the threats to your Web site and the system it runs on, and the importance of protecting them.

Statistics to keep you awake at night

In a test conducted over a two-week period in September 2004 by USA TODAY, there were 305,922 attempts to break into six computers connected to the Internet. The attacks literally began as soon as the computers went online, averaging more than 300 per hour against both a Windows XP Service Pack 1 machine with no firewall and an Apple Macintosh. There were more than 60 attacks per hour against a Windows Small Business Server. During the test, both of the Windows-based machines were compromised.

These figures show how active the hacker community is. Any computer connected to the Internet is at risk, particularly a Web server. Although e-commerce Web sites receive more targeted attacks than any other type of Web site, it is no longer a question of if, but when your site will be probed.

Script kiddies and organized crime

The vast majority of attacks are automated and random as attackers don't care what systems they compromise. In all likelihood, the remote systems attacking a Web site are unwitting accomplices whose system administrator has no idea his systems are infected with a Trojan. According to Symantec’s Internet Security Threat Report, more than 40% of worm-related attacks against machines connected to the Internet propagated from IP addresses controlled by Fortune 100 companies!

The individuals behind these attacks are often referred to as script kiddies, a disparaging term that doesn't reflect the devastation they can wreak. Many script kiddies lack technical competency. But by using only a single tool or exploit, randomly probing large numbers of systems and attacking the weakest, they can achieve dramatic results. Spikes in attacks are tied to the school calendar, suggesting that many teenagers are behind them.

In most circumstances the techniques used by script kiddies are the same techniques used by serious criminals who have financial gain as their main object. Often financed by organized crime, these attacks aim to defraud or steal online assets rather than be destructive.

Tactics, tools and motives behind attacks

The script kiddie's goal is to gain control of a computer the easiest way possible. Script kiddies' random selection of targets and lack of concern about the damage they cause make them a dangerous assailant to any Web site that resides on a system permanently connected to the Internet.

The tactics used in an attack are simple: build a database of IP addresses that can be scanned (systems that are up and reachable), scan those addresses for a specific vulnerability and exploit it. Once script kiddies find a vulnerable system and gain control, their first step normally is to cover their tracks. They want to ensure that the system owner cannot detect the intrusion. After checking to see if the coast is clear, the script kiddie clears the log files and replaces or modifies various critical files.

Tools used by script kiddies are often easy to use, require little interaction and are widely available. A tool is used to build a database of IP addresses. Some tools randomly select which IP network to scan while others conduct zone transfers of a selected domain name and all its sub-domains. Scan results are often archived or shared with other attackers to exploit a new vulnerability at a later date without having to build a new database.

After determining which systems in their database are running the vulnerable OS (by using a tool such as Fyodor's nmap), an intruder can easily target and compromise them. Tools to exploit vulnerabilities often appear within days of a new vulnerability being made public.

Just as there are automated scripts for hacking, there are also automated tools, such as lrk4, that mask the intruder's presence on a system. These are often called rootkits.

Once intruders are safely hidden, they tend to do one of two things. They may use the system to scan or exploit other systems; or they may choose to attack the system. Often they will silently monitor the system with a sniffer, returning later to see if any valuable data such as passwords or bank details have been captured.

Web site defacements are the most common result of an attack by script kiddies. The motive behind these attacks may be purely malicious - a grudge perhaps or to make a political point. Others may do it for the fun of the challenge, or as a way to compete with other hacker groups to set records for the most high-profile site attacked. The criminal’s motive is simply fraud, theft or blackmail. Some in the industry maintain that hackers are different to crackers in that their motives are not malicious, but for system administrators this is merely semantics.

Risks and threats to your Web site

Web site attacks fall into two broad categories. Some threats affect the accessibility and reliability of a site, and are classified as denial-of-service (DoS) incidents. Other threats work against the content and data of a site, as intruders try to steal, modify, delete or leave something on a site. Such incidents are most

commonly called cracking incidents. Two threats of particular concern are distributed denial-of-service attacks and worms.

Distributed denial-of-service (DDoS)

DDoS attacks are based on a single user controlling hundreds, if not thousands, of compromised systems remotely coordinated to execute attacks against a victim or victims. The more systems compromised, the more powerful the DDoS attack. It is extremely difficult to defend against and identify the source of such attacks. Worms are often used to initiate a DDoS attack.

Worms at war on Windows

Most current system compromises appear to be based on worm activity. Worms are automated probes that identify and exploit vulnerable systems, exponentially replicating themselves.

The most dangerous type of worm is an Internet Relay Chat (IRC) bot - short for robot. A bot is network worm whose payload runs continuously in the background, providing backdoor access to the compromised computer through IRC channels. Bots start up an IRC client, connect to a specified IRC server, which has probably been set up on a shell account and paid for with a stolen credit card, and wait there for further commands, allowing the attacker to remotely control it. By combining multiple bots, an attacker can create what is called a botnet. By leveraging the power of even a relatively small botnet, an effective distributed denial-of-service attack can easily be launched.

One of the best-known bots is W32/Agobot-RJ. There are over 500 different versions of Agobot, partly because the source code is available under the GNU General Public License - another example of hacker cooperation. Also recent worms have illustrated the ability of malicious code writers to rapidly upgrade bot networks to take advantage of new exploits.

What needs protecting?

Having looked at the enemy and the risks of running a Web site, I want to look at the four key resources that need protection. Each of these resources are looked at in further detail in other parts of Web Security School (searchsecurity.com/WebSecuritySchool).

Web server

This is an obvious place to start, but often times servers are not stored in secure locations. Concentrating on the technical security measures is pointless if the server can be compromised by anyone with physical access to it. Every piece of equipment attached to the server, such as routers, network cables and firewalls, needs to be protected in the same manner as the server.

Services

Every service running on the server needs to be understood and protected. Each service means more open ports and more potential holes. If possible, the Web server should be a single-function server. Under no circumstances should a system running Microsoft IIS also be a network domain controller. A domain controller manages the account security of your entire Windows networking domain. I look at how to protect your server and its services in the Lesson 1

webcast, Insider's guide to Web server security, and Lesson 2 webcast, Web attacks and how to defeat them.

Content

A Web site's content should be delivered without compromising the server's security. Remember that your Web site's content is what most attackers are actually after. Lack of attention given to securing Web content often undoes a lot of the security measures in place elsewhere. The Lesson 3 webcast, Locking down your Web applications, deals with this issue in depth.

Internal users

Security strategies conventionally focus on the network perimeter. However, you can expect to see an increase in attacks via desktops, making the security of client-side systems increasingly important. Attackers will continue to exploit the vulnerabilities in client-side software code in an attempt to find new angles of attack against Internet-based systems. The growing trend towards social engineering, and strategies such as phishing and spyware are increasing the need for security awareness amongst staff. The Lesson 3 webcast also includes security guidelines for internal workstations. (All three lesson webcasts are available on-demand at searchsecurity.com/WebSecuritySchool.)