



Self-Scanning

A white paper exploring vulnerability assessment technology.

©2004 IPxray LLC

<http://www.ipxray.com>

866.297.0765

Self-Scanning: See What Hackers See

*It's the easiest, most cost-effective, and surest way to test your cyber security. Use the same tools hackers use to "case" their victims, and defend yourself before you **become** a victim*

In cyberspace, there are two kinds of criminals. One is the amateur — the stereotypical teenager — looking for the thrill and bragging rights of breaking into someplace he doesn't belong. The other is the professional — a career criminal — looking to do victims real harm. Both types have one thing in common: before they strike, they usually "case the joint." It doesn't matter whether the neighborhood of choice is a big city financial district, a suburban street, or a range of Internet addresses. All criminals go where the risk/reward ratio works in their favor. Before they strike, they'll probe for weakness, and then use that weakness as a guide to select targets, strategies, and methods of attack.

When it comes to surveillance, however, cyber criminals have three big advantages over their counterparts on the street: 1) they're not limited by time or distance — any system anywhere on the Internet is fair game, day or night; 2) they can thoroughly examine hundreds of potential victims in a few hours using automated scanning tools; and 3) the percentage of potential victims is very high, since many companies still take only a hit-or-miss approach to cyber security.

These three points offer a clear strategy to avoid getting attacked: *don't look like an easy mark*. Make it more difficult for hackers by applying the policies computer security experts have advocated for years. These include:

- Use a firewall;
- Close Internet ports you don't need;
- Keep software up to date with the latest patches;
- Use current anti-virus software;
- Filter out suspicious content from e-mail;
- Protect passwords, change them frequently, and use non-obvious passwords;
- Control physical, dial-in, and wireless access behind the firewall.

Even if you do all these things all the time, there is still one nagging question: How do you know *for certain* you haven't missed something? The answer is, you won't know, and you can't know, until you look at yourself the way criminals do, and see what criminals see. Modern technology has made scanning tools cheap and easy. Bad guys use them, and they're cheap and easy for the good guys, too---systems administrators and network managers, like you. A hacker needs to find only a single opening; you need to find them all. The only sure way to do that is to scan your company the way hackers do.

A Pervasive and Under-reported Problem

It's very likely that even as you read this paper, hackers are testing your systems for entry points.¹ In fact, anyone with a persistent Internet connection may get scanned hundreds of times a week. To see a list of these scans, you should check your firewall's log file consistently. Most scans are done by kids looking for fun — the vast majority of whom are “script kiddies,” or amateurs who, with the help of more experienced hackers, download ready-to-run programs from underground bulletin boards and news groups. But don't let the nickname fool you. The “script kiddies” may not be sophisticated, but the tools they use certainly are. They can scan for exploits, steal information, crash a computer, or plant programs that launch attacks against other computers on the Internet (turning them into what is known as a “Zombie”). Even a “routine” hack where no real “damage” is done can be very disruptive. It can mean taking systems offline for hours, checking to see if anything was compromised, and never being absolutely sure afterwards.

More serious hackers use the same tools. The tools are, after all, free, and they do work. But in the hands of “grown-up” hackers, homegrown tools can be honed more skillfully to wreak even more havoc. Almost every day, stories appear in the press about the damage caused by hackers. In June 2004, hackers infected over 200 websites with a program that attempted to download malicious code to users logging onto those sites. One of the sites was Kelly Blue Book, the California company that provides online pricing reports on new and used cars. The Kelly Blue Book site gets 300,000 visits a day. Once downloaded to users' PCs, the malicious code was designed to steal credit card information and other private data.

That same summer, data thieves broke into computers at BJ's Wholesale Club, the country's third largest wholesale club retailer. This was the largest online retail fraud case, to date. Hackers got away with thousands of credit card numbers — forcing banks across 16 states to send out hundreds of thousands of replacements. The Philadelphia-based Sovereign Bank was forced to cover approximately 700 fraudulent transactions resulting from the BJ's theft and issued nearly 81,000 replacement cards at a cost of about \$1 million. Another institution, the Pennsylvania State Employees Credit Union, reissued cards to 14,000 members at a cost of \$100,000. Altogether, BJ's will face claims from 10 to 15 banks.

In a 2004 report, the PBS show *Frontline* found the problem of computer hacking both pervasive and under-reported. The show interviewed several experts, including Chris Davis, a security consultant and ex-hacker, who tracked down “Curador,” an 18-year old hacker from South Wales who, in 2000, stole an estimated 26,000 credit card numbers from e-commerce sites, which he posted online. According to Davis, companies need to start taking both kinds of computer criminals seriously:

*... it's a little scary. It happens every day, though. We have 14-year-old, 13-year old, 12-year old kids that are defacing major web sites; government web sites, NASA web sites, things like that. They're breaking into the computers and changing the sites. They're sort of this cyber graffiti On average, a little less than 20 times a day are reported. I don't know how many times it happens where they're not reported.*²

¹ As an example, the SANS Institute reported 1,399,907 attacks occurred in the U.S. on August 18, 2004 (www.isc.sans.org).

² *Frontline*, 8/8/2004.

But the damage doesn't stop with graffiti. In the summer of 2003, the Blaster Internet worm (a.k.a. LovScan virus) crippled more than a million computers. Blaster proliferated when one infected, unprotected computer automatically sought out and infected other unprotected computers. Without a fertile environment of unprotected computers, this type of attack — among many others — would not be possible. The question is: Why are so many computers vulnerable?

Turning the Tables on Hackers

For hackers, finding these exploits is easy. Hackers simply download an open-source scanning tool, specify a range of Internet addresses to check, and launch the program.⁴ The scanner will probe each address for all open ports and, if it finds one, probe for each exploit. Nessus, just as an example, has a database of 1900+ known exploits. Each probe is accomplished by running a particular script or plug-in which will send data at the target--any Internet connected server (web, mail, ftp, etc...)--and see what comes back. A report is produced of each address, each open port, each resource checked, and each exploit found — along with a link to a description of what the exploit does and remedies to fix it, such as patches available for download. And the process continues through the entire address range; could yours be among them?

Once hackers have an exploits report in hand, it's literally open season. They know where vulnerabilities exist and how to exploit them. Depending on their skill level, hackers can download attack programs or write their own.

All this raises the question: *If hackers can get this information, why can't the targeted organizations?* What stops a systems administrator from downloading a scanning tool to get a picture of the organization's own vulnerabilities? The organization would *know* where vulnerabilities are. There must be *some* reason organizations don't do this, or don't do this more frequently and effectively, especially in light of how widespread and costly hacking has become.

³ *Business Week*, "Gambling Sites, This Is a Holdup," 8/9/2004, p. 60. (These should be reverse ordered, I think)

⁴ Among the scanning tools popular with hackers — and those trying to stop them — are Nikto and SARA (The latest evolution of SATAN the original open source exploit scanner).

What's Next: Cyber Extortionists

One industry on the wrong side of cyber crime's cutting edge is online casinos. It started during the 2003-2004 football season and has continued ever since. Just as the bets start to flow in from online gamblers — in the days right before the Super Bowl or Smarty Jones' bid to win the Triple Crown — the computers taking these bets slow to a crawl. Next comes an email to the casino operator demanding that payments — typically \$30,000 to \$60,000 — be wired to the criminals' bank accounts. Either the online sites pay up or they won't be able to operate.

How do criminals do this? They use thousands of "Zombie" computers in a denial of service attack. They infect thousands of unprotected computers with malicious programs. These programs put them under the control of the hacker (hence the term zombie), who then directs his/her zombie computers to target designated sites with streams of messages. If the sites' operators do not pay the extortionists' demands they could be down indefinitely.

This is a highly disturbing trend, even for companies that aren't in the gambling business. Most companies don't want criminals' viruses at work inside their computers — sucking up bandwidth or turning the owners into accomplices. Nor do companies want to become targets themselves. As *Business Week* recently reported:

The extortionists may be just beginning to flex their muscle. Industry experts fear that they could soon target government operations, e-commerce companies, banks — practically any organization with an online presence. ... "It's only a matter of time before we have an extortion threat," says Peter J. Chambers, chief executive of Affinity Internet Inc., a Fort Lauderdale-based company that manages websites for 300,000 companies.³

There are many reasons for this apparent lapse on the part of many organizations when it comes to checking their security in this way:

- **Knowledge** - Many organizations simply are not aware of the existence of these tools, since they are open-source and not advertised or sold by any well known IT vendor;
- **Hardware** - The need to install dedicated hardware outside the firewall in order to get the proper perspective for the scan can create issues between IT departments and corporate policies, which prohibit such systems. If multiple data centers require scanning, then in many cases, multiple sets of hardware would need to be installed to avoid overloading the bandwidth from any one location to scan other locations.
- **Linux** – Most tools run primarily on open source (Linux) operating systems, and some organizations have been slow to incorporate such systems into their official IT and security infrastructures;
- **Support** - The complexity of configuration, along with the total lack of available support services in the open-source world, means that the process of downloading, installing, and maintaining such software can be time consuming and frustrating, even assuming an acceptable level of knowledge of the Linux operating system. Even once the software is installed, configured, and run, the data generated by a security scan can be overwhelming. Because the security information provided by many of these tools is somewhat cryptic, it is frequently difficult to translate the information into a security strategy.

There is also the realization that multiple tools should be installed and used (The need to understand your network perimeter as seen from as many of the “hacker tools” as possible). This need for hardware, software, support, and multiple views makes self-scanning a difficult proposition for many organizations.

Four Targets of Buffer Overflows

Exploits that use buffer overflows cannot exist if the targeted software checks all incoming data and rejects data that will overflow its buffer. Once identified, the exploit is easily patched by downloading and installing the correct update. Of course, that means that the systems administrator must be diligent about downloading updates.

Some potential targets of a buffer overflow attack include the Windows Task Scheduler, the Microsoft RPC interface, the ASN.1 library and the Winlogon process.

The Windows Task Scheduler is a component that lets users schedule commands, programs, or scripts to run at a specified time. A buffer overflow here could allow a hacker to crash or to take control of the system. This could be accomplished simply by including the malicious code on a web page that a Windows computer might access. Another example occurs in Microsoft IIS 4.0 web servers. A hacker could send a specially constructed message to the system, causing a buffer overflow and the implant of new code— again, shutting down the system or taking control of it. In a technique similar to the one used in the Blaster worm, the hacker can exploit this vulnerability — and infect computers — without tricking users to click on a link or visiting a web page.

Windows uses the RPC interface to allow one program to call subroutines in another program — a necessary function if computers are to cooperate over a network. Windows uses the ASN.1 library to “parse” or interpret the instructions that one computer receives from another, an important function for network computing. The Winlogon process is the process Windows uses to log users onto a computer. Like the others, this function also uses a buffer to receive messages from other programs (in this case, so those programs can log onto the system). If a hacker overflows the buffer with the wrong code, the hacker can take over—or take down--the targeted system.

A Self-Scanning Option

There are options for organizations willing to employ a self-scanning model which addresses the usability issues described above. One commercial example is IPxray (www.IPxray.com). It takes a *best of breed approach* to provide a number of inter-related services under a single interface — including exploit scanning, inventory scanning, and firewall rule verification. IPxray also adds monitoring features not found in open source packages. IPxray provides an online *panel of technical security experts* available either by bulletin board or e-mail. Additionally, IPxray offers phone-based technical support. Finally, the service employs a *hosted delivery model* — which makes sense for both economic and functional reasons. First, there is nothing to install, maintain, or upgrade. Whenever enhancements are introduced (even entirely new tools), these are available automatically to IPxray users without investing in new software. The hosted model approach makes sense from a functional standpoint, as well, since this is, after all, *external* scanning. Hosting the service outside the firewall gives the legitimate scanner exactly the same perspective as a hacker. In other words, ***you see what the hacker sees***. Also, having the scan run by a third-party security company lends credibility to the output, in the event that a client or regulatory agency requests documentation of organizational security practices.

Most subscribers can expect to spend less than \$200/month for this service. This means, in the context of information security, that it's hard to make a case against it. Even if IPxray's services merely supplement and verify more expensive security procedures and equipment, it is still valuable, cost-effective, and unique.

IPxray Service users will typically run a complete security scan of their IP address ranges and key servers, note all weaknesses, install any needed patches, and implement necessary remedies, such as closing ports and upgrading equipment. The IPxray Technical Advisor Group is available to assist IPxray subscribers, making recommendations for interpreting the scan output and deciding on what actions to take. Scans are then repeated until effective baseline security is achieved.

Clients can then run — usually on a daily or weekly basis — benchmark reports for specific servers. Reports will show differences between the security fingerprint and the current state for those specific critical servers. If new exploits, firewall changes, or some other event causes the security of critical servers to be compromised, clients will know immediately. Users can then download a patch or make the needed configuration modification to secure the server.

IPxray users can also run inventory reports to ensure no new undocumented servers or ports have been opened to the Internet. Firewall verification scans should be done anytime there is a configuration change made to the firewall.

Another important security-related factor is external monitoring. This elevates security to the “am-I-under-attack-RIGHT-NOW” level. IPxray provides this level of external monitoring to its clients, which can determine if a website is under attack, or has already been hacked, redirected, or defaced.

No matter which route you choose, commercial or in-house, it is critical that organizations develop and implement practical options for thorough, regular self-scanning. It is absolutely essential that security staff see their networks from the same perspective that hackers do.

In today's environment, where someone could be scanning, cracking, or hacking your network right now, protecting yourself is not optional. It is essential. If you don't look like a victim, you won't be a victim.

Table 1. Two Options: When it comes to self-scanning, companies can either do it themselves or subscribe to a hosted service.

Note: Attached table compares the merits of a hosted, subscriber-based model with a do-it-yourself approach

Factors to Consider	Do-It-Yourself	Hosted (www.ipxray.com)
When can you start?	<p>Days to weeks to:</p> <ul style="list-style-type: none"> Acquire hardware and software Set up and configure server Install and configure scan tool Connect the server to a port outside the firewall 	First scan within 10 minutes after registering via browser-based interface
Costs	<p>Total 1st year cost range for do-it-yourself scanning: \$7,700 - \$23,700:</p> <ul style="list-style-type: none"> Hardware costs: \$1,000 - \$5,000 Scan software costs: \$0 - \$6,000 Software updates: \$0 - \$6,000 Installation & configuration @ approximately 15 hours: \$1,500 Yearly labor costs for updates and maintenance @ approximately 1 hour/week: \$5,200 	Pay a monthly or yearly subscription, which varies based on the size of the organization: between \$40-\$250 per month.
Upgrades	You're responsible for acquiring patches and upgrades for the scanning tool. New pluggins are usually posted multiple times per week.	Patches & upgrades happen automatically
Tech Support	None available for open-source tools.	Tech support provided with the service.
Scan Output Interpretation Support	None available for open-source tools.	IPxray Online and other resources available for interpreting scan output.
Scanning Options	Limited to the specific tools you download and configure. Open-source tools are not integrated with each other, i.e., no suite approaches.	Many tools available in one location and via one browser-based interface with IPxray hosted service.
Complexity	Users must configure each tool, and learn its interface. Linux is a requirement	Users see a single easy-to-use interface. Browser-based service is operating system agnostic.
Security	Requires placing a server outside the firewall.	No need to change network in any way.
Performance	Scanning multiple locations from headquarters can create a bandwidth bottleneck or require multiple servers.	Hosted services designed to support multiple locations scanning and monitoring.

IPXRAY[®]

Actionable Intelligence To Secure Your Network

See what your network looks like from the hacker's perspective.

Try IPxray for 2 weeks FREE:

Visit <http://www.ipxray.com>

IPxray, IPxray and the IPxray logo and combinations thereof are trademarks of IPxray, LLC. All other brand and product names are used for identification only and are the property of their respective holders.