

Internet Penetrations: Profiles of an Attacker

Executive Insight Series

Brad C. Johnson

Introduction

Understanding the motivation and the level of technical skill of the hackers who might likely target your organization enables you to plan and deploy appropriate detection and defense capabilities. This white paper was originally prepared at the request of the editors of Secure Enterprise Magazine for publication in April 2005. It is a companion piece to the white paper entitled, *“Internet Penetrations: Thinking Like an Attacker.”*

Who are these people trying to break-into my Internet systems?

In the world of Internet penetrations there are some well-known terms describing the general intent of people attacking your systems.

The typical explanation is that White Hat “hackers” are people who have been legitimately hired or asked to look for problems and Black Hat hackers are those who are doing it maliciously or are being clandestine about their activities. After that came Gray Hat hackers who used to be Black Hat attackers and now are trying to get paid as White Hat attacks. As time goes on, these definitions are becoming less helpful. If you break into a system without permission, but then tell them how you did it, are you White Hat or Black Hat? If you work for a company and break into a system without permission to show them how susceptible they are to attacks, what are you?

Instead of focusing on a single term to describe the attacker’s motives, let’s consider a few of the more important profiles of who is performing these attacks and what it means to you: their intentions, skills, and the resources available to them to perform an attack.

Script Kiddie

This term is meant to be derogatory and implies somebody who has no original hacking capabilities and simply just copies what others have already done. In all seriousness, most people, including those you hire to analyze your systems, are Script Kiddies. The simple fact is despite thousands of new exploits every year, most vulnerabilities are detected by using tools or techniques that somebody else has already developed.

From your point of view, this actually is a very valuable role to emulate. You want to know the answer to the question “What bad things could somebody do to me without much effort?” That is something you should not only ask yourself but also try to do. For the most part, Script Kiddies are looking to increase the value of their reputation by successfully getting access to your sensitive data or systems. They want to embarrass you. Unfortunately, in today’s world, the simple act of embarrassing a company could be disastrous to its reputation and actually influence how much business it conducts over the Internet.

In a nutshell, the way to be prepared for Script Kiddie attacks is to do what they do. Run the 1-button tools that exist against your resources, use the Internet to search for well-known procedures or techniques that attack your types of systems and try them yourself, and make sure you can both detect that these tools are being used against you and that you are not vulnerable to these very easy to find problems!

For example, Whisker is a tool that can look for hundreds of well-known Web server exploits (e.g., IIS or Apache vulnerabilities). Would you be able to detect that your Web server had 500 failed file references in 10 minutes from the same IP address from somebody using Whisker? Most sites would not detect this tool being used against them.

You should run the easy to use tools and try the easy to understand procedures to find problems on your network. If you decide to hire somebody outside your organization to test your systems, you need to decide if it is acceptable if any of the “testers” have ever performed unauthorized hacking.

Insider

Despite all of the attention to attacks from the Internet, most successful attacks happen from “inside” your own network. In a very real sense, any outside attacker is always trying to become just like the insider because the additional knowledge about how things really work should lead to problems that can be successfully exploited. The reason that so many attacks are successful from the inside is that there is too much trust amongst users, systems, and services.

The problem with this trust is twofold. First, access to data or systems should be based on both authentication and authorization decisions and most sites assume that if you have authenticated yourself (i.e., logged in), you are also authorized to perform actions. Adding to that problem is that most sites do not do a good job of auditing actions so it is either hard or impossible to figure out who has done what. Second, as time goes on it is almost impossible to tell the difference between inside and outside on your network. Most networks have so many external connections (special partner extensions, VPNs, modems that bypass all other security mechanisms, direct access for outsourced management services) it is extremely difficult to define your network boundaries.

The hardest part of being prepared for an insider attack is that it probably means setting up your systems completely differently than they are currently configured and to also add strong(er) authentication and authorization controls into every part of your network. Everything should be managed as if it were actually on a public network and has sufficient controls to know exactly who is doing what under what circumstances.

The easiest way to prepare for an inside attack (assuming the above changes are not made) is to greatly increase the amount of auditing you do and introduce after-the-fact log analysis to detect unauthorized access. That way, you can at least know if there have been attacks on your network. The other recommendation is to run penetration tests on your internal networks on a regular basis and

make sure you are prepared for, at least, the easy to find problems.

The Determined Intruder

While Script Kiddie style attacks are always going to be a fact of life and in all likelihood most attacks will still happen from the inside, the changing world that we live in has created a fundamentally different type of attacker on the Internet: The Determined Intruder. Instead of trying to embarrass you or impact your ability to do business (e.g., denial of service attack) the determined intruder is interested in subtleties.

The determined intruder may be a foreign government, a political organization, organized crime, or some consortium of people or groups (which may or may not have identified themselves to anybody). The key characteristics to these determined intruders are that they may be well funded (e.g., they can afford to ante up \$50 million dollars for an encryption deciphering system), they are organized amongst themselves (i.e., there is somebody in charge or a hierarchy of decision making), and possibly the most important aspect is that they are willing to take their time. For example, a foreign government may be more than willing to monitor or make very small changes to transactions conducted by US based financial companies and take 10 years or even 50 years to accomplish their goals!

The motivation for these types of attacks are more sophisticated in that they may be trying to just subtly nudge some activity to go in a slightly different direction. Imagining pushing a ship off course by 1 degree. It may wind up close to where it wanted to go, but certainly not in the right place. What if the determined intruder was trying to nudge our monetary system or slightly influence which countries are awarded governmental contracts? The subtler the change and the longer the period of time to make the change, the less likely somebody would ever notice their activities.

Final Word

How do you prepare yourself for these types of attacks? Obviously, there is no simple answer, but it starts with the fundamentals. Security is a philosophy of defense in depth and incremental protection. The more layers you have in place and the more successful you are with the three pillars of security – authentication, authorization, and auditing – the better positioned you will be to defend against these kinds of attacks.

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, VPNs, and Windows security at USENIX, NetworkWorld-Interop, CSI, and many other conferences are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long-term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. www.systemexperts.com/services.html

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. Some of the more frequent tests that we perform include "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventory, wireless LAN inventory, VPN assessments, and denial of service reviews.

Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise. With our Security Blanket™, service, you'll be able to sleep at night knowing a team of security experts is on your side and *watching your back*. In addition to performing quarterly penetration tests, we'll notify you of virus attacks and vendor vulnerabilities that affect your infrastructure, and monitor a collection of hacker sites and alert you if your organization is ever mentioned.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, Unix, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

Accelerated Security AssessmentsSM & Code Reviews

Using our innovative and highly interactive Accelerated Security AssessmentSM methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value both the short duration and the immense knowledge transfer that occurs during these intense Accelerated Assessments.

SystemExperts uses this Accelerated Security AssessmentSM methodology in a wide range of services including:

- ISO 17799 Assessment
- Sarbanes-Oxley Security Assessment
- COBIT Assessment
- Wireless Security Assessment
- Best Practices Security Assessment
- Application Service Provider Security Assessment
- Authentication and Authorization Security Assessment
- Application Security Assessment
- PeopleSoft Security Assessment
- Billing System Security Assessment
- Anti-Virus Security Assessment
- Security Architecture Assessment

Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing their overall security architectures.

Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston

New York

San Francisco Tampa

Washington DC

www.SystemExperts.com

info@SystemExperts.com

©Copyright 2005 SystemExperts Corporation. All rights reserved.