SystemEXPERTS
LEADERSHIP IN SECURITY

A Perspective On
Practical Security
2003

Intrusions and their Detection: Addressing Common Hacker Exploits

SystemExperts Corporation
Brad C. Johnson

Abstract

Despite the industry "buzz", the myriad of tools, and the extensive publication of books on the subject, implementing and maintaining a successful intrusion detection system is difficult, expensive, and undoubtedly time consuming. However, determined intruders both outside and inside your firewalls are not apathetic to your challenges and those with malicious intent will continue to do what they do best: HACK!

This White Paper discusses the state of affairs for intrusion detection and in doing so, illustrates why most Internet sites do not have proper detection infrastructures and are only prepared to detect generic intrusion attempts. More importantly, this document outlines practical advice for you and your organization to follow that will immediately improve your ability to detect many of the most successful intrusions.

Since 1994, SystemExperts has helped companies react to some of the most publicized intrusions. Additionally, we have helped some of the leading companies in the world proactively prepare for intrusions by empowering them to detect unauthorized network activity and respond accordingly. The content of this paper is distilled from the extensive experiences of the author and the SystemExperts team of consultants.

Inside

- Why are most Internet sites without intrusion detection capabilities or limited to detecting only the most generic intrusions?
- Best Practices to quickly and inexpensively improve your organization's intrusion detection capabilities.
- Web Server Exploits: How to be prepared for well-known exploits.
- 802.11 Wireless: SSID, DHCP, SNMP, and MAC addresses.
- Detecting rapidly growing Web Application exploits.

SystemExperts Corporation

Boston **New York** **Washington D.C** **Tampa**
San Francisco **Los Angeles** **Sacramento**

Toll free (USA only): +1 888 749 9800
From outside USA: +1 978 440 9388

www.systemexperts.com
mailto:info@systemexperts.com

State of Affairs

Intrusion detection. It would be nice if most intrusions were detected, but they are not. Let's take a quick look at some practical facts.

- Determined intrusion attempts are usually successful.
- Most intrusions happen from the inside by insiders.
- Intrusions can happen from the outside without having an interactive session on an inside system.
- Most intrusions are neither detected nor prevented.

Those are depressing facts and, unfortunately, it gets worse.

Intrusion Detection Appreciation

There are a wealth of tools, techniques, experts, courses, and books that are focused on intrusion detection. Yet, despite all of these resources most Internet sites have no intrusion detection infrastructure and are only prepared to notice generic intrusion attempts. There are a number of reasons for this dichotomy.

- Fundamentally, intrusion detection is not as easy as it looks. It requires a significant amount of configuration and testing time to deploy intrusion detection software that works well and most organizations do not adequately budget for or plan the time to do it.
- Most intrusion systems require in-house software development to make them work in your environment. Many organizations do not have adequate development skills and even if they do, those resources are often dedicated to other priorities.
- Successful intrusion detection environments can only be built by experts with a detailed understanding of the exact resources that are deployed. Finding people who are genuine experts on many different services, protocols, applications, vendors, and operating systems is extremely difficult.
- The only way to develop a detailed understanding of what is "normal" in your environment and the thresholds and conditions that would identify abnormal behavior is through an iterative process of capturing and analyzing production quality network traffic. Again, this requires a lot of time and effort.
- There are dozens of incredibly easy to use tools that will look for or attempt to exploit hundreds of intrusion vulnerabilities. Many of these tools are not detected by intrusion systems and many have detection avoidance mechanisms built into them (e.g., packet fragmentation, protocol tunneling, and URL encoding).

If you have been involved with working on an intrusion detection system, you understand these challenges and difficulties. Let's take a quick look at some ways to make things better.

There are a myriad of ways in which intrusions happen. However, some ways are more prevalent than others. Many organizations make the mistake of trying to go from having essentially no intrusion detection to comprehensive intrusion detection in one big step. It does not work. Successful IDS deployments are an evolutionary process.

The best way to immediately improve your intrusion detection system is to focus on common problems first because, unfortunately, most existing intrusion detection packages do not cover many of these obvious areas.

Common Hacker Intrusions

Virus Detection

Of course, the single most frequent intrusion type is the email virus. There is no need to belabor this point.

> **BEST PRACTICE**: You should have virus detection software on every single system and you should update the virus database daily.
>
> **BEST PRACTICE**: You should check both incoming and outgoing email and attachments for problems. Additionally, you should scan every single writeable media daily.

Web Server Infrastructure

One of the most common and easy to duplicate types of intrusions involves exploiting well-known Web server distribution files. Every Web server distribution (e.g., Microsoft IIS, Apache, or iPlanet/Netscape) comes with a collection of files used by the server itself including management software, example programs, and configuration scripts. Over time, people figure out that some of these files are actually exploitable and can yield data or access to the Web server system. These vulnerabilities are normally exploited by simply knowing the correct URL to plug into your browser.

There is a class of programs that look for these well-known files called CGI-scanners. These programs poke at the Web server using standard HTTP requests that search for these files. Some of these scanners are dumb (they simply issue a request for every single exploitable file) and some of them are quite smart (e.g., if it discovers it is an Apache Web server it does not look for IIS files). The better CGI-scanner programs look for hundreds of these well-known files (e.g., Whisker).

BEST PRACTICE: You should procure a CGI-scanner and run it against your own Web site. You should run this program every time you update your Web server and you should periodically get updated versions of the exploit database that the program uses.

BEST PRACTICE: You should have an automated means to check your Web server log files to see if anybody is running a CGI-scanner against you.

Hacker Intrusion Packages

Another intrusion area that is usually ignored is the rootkit. A rootkit is a collection of programs, techniques, papers, and references that show how to exploit, break-into, or disable a particular Operating System. There are different rootkits for almost every Operating System (e.g., Linux, FreeBSD, Solaris, or Windows). Even though most technical people have heard of rootkits, very few have actually taken the time to download, review, and understand the details of the kits applicable to their environment. Very few non-technical people have even heard of rootkits and they do not understand the inherent and obvious danger of these distributions.

BEST PRACTICE: Download the rootkits for each of the various Operating Systems you deploy and review them to see what is applicable to your environment.

BEST PRACTICE: Try the programs and exploits on your own systems and make sure you know how you might prevent, detect, or react to each one.

Modems (the forgotten device)

One area that is often completely ignored when designing an intrusion detection system is modems. Modems are potentially the single easiest way to access private, internal information because they typically bypass every implemented security mechanism and yet exist on critical systems such as routers, firewalls, printers, and desktop systems. Your own administrators and vendor support staff often use them to remotely manage or monitor important services. These modem-based services are frequently not using any type of encryption, they often do not require any authentication other than dialing the number, and the actions are almost never logged.

BEST PRACTICE: Periodically call (i.e., dial or "War Dial") all your phone numbers to create an inventory of which ones have modems attached to them and the type of service they offer.

SNMP (the forgotten protocol)

One could almost cut and paste the issues for modems (above) here in the SNMP section. Where modems are the forgotten devices, SNMP is the forgotten protocol, and yet it exists on almost every system you have. It certainly is on many of your most important network systems such as routers, printers, firewalls, and desktop systems and it is the fundamental management protocol for all 801.11 Access Points. Just like modems are a valuable resource for intruders, SNMP agents provide the hacker some of the most important information he needs to understand your network profile. That is, SNMPS agents tell the attacker what exact services and devices are installed on your network. When a network resource is powered up, changes state, or receives information from the network (e.g., TCP/IP connections), that real-time information is stored in the SNMP database, the MIB.

To access this database you need to provide a password to authenticate with the SNMP agent. This password is called a community-string. Like almost all other management interfaces, there are default passwords (community-strings). There is one for the ability to read information from the MIB and another for the ability to write information.

Unfortunately, almost nobody changes these default passwords, which means unless access to that system is somehow blocked, you can use a readily available SNMP program to read and write information. Keep in mind, that most of the parameters that you write to the MIB actually control the operation of the system: for example, turn it off, change its IP address, or other equally vital commands. Also just like modems, SNMP events are almost never logged or part of the intrusion detection system.

BEST PRACTICE: Disable the SNMP agent on systems that are not going to be managed through your network management software.

BEST PRACTICE: Change the default community-strings (passwords) on every system that you have SNMP agents running on.

BEST PRACTICE: Instrument your systems to generate an event if any of the key SNMP counter variables change: which would indicate that either somebody is accessing SNMP agents with the wrong passwords (something you would not expect) or someone trying to access fields in the SNMP database that do not exist (another indication that an individual is probably trying to "hack" into your SNMP information).

802.11 Wireless

Wireless technology is one of the newest and fastest changing parts of many organizations' network infrastructure. Most organizations deploy 802.11 wireless components because they are relatively inexpensive to buy, they are easy to deploy, they do not require sophisticated knowledge to install, and they allow you to extend your network environment without physical changes. Unfortunately, because many wireless components are deployed without either the advice or assistance of IT or security professionals, they are often used in their default configuration. Out of the "box," every Access Point is in its least secure configuration.

What may be even more important than the specific setup, is that without a serious effort to understand where the radio frequencies are actually going, the network is probably being extended beyond the physical boundaries of what was intended: such as to the floor above or below you, to the building next to you, or to public places like the streets and roads around your building.

There are several 802.11 specific changes that you should consider in your intrusion detection system.

BEST PRACTICE: Have a network sniffer on the same network segment as the Access Point. If traffic is seen coming from unknown MAC addresses, generate an event that an unknown client is trying to use your network bandwidth or service.

BEST PRACTICE: Consider changing the default configuration of your Access Point to disable broadcast of the SSID, to not offer DHCP services, and do not reply to probe-response packets (which is how an "unknown" client can find your Access Point).

BEST PRACTICE: Change the default SSID (network name), the default SNMP passwords (community-strings), and the default password to the administrative interface.

Web Applications

If 802.11 wireless is the fastest growing technology area, then problems in Web applications are the fastest growing exploit area. Unfortunately, most Web applications are not tested for the type of exploits that they will be subjected to when deployed in a networked environment. Most testing is focused around ensuring key functions work as documented. The fact is, however, when that application is installed on a system and then deployed on a network (e.g., the Internet) it must protect itself from a variety of issues that have nothing to do with the normal functional behavior of the application.

- What if somebody gets interactive access to the system it is installed on and tried to access sensitive data stored in files on the disk?
- What if somebody finds an exploit with the Web server and now has the ability to view files and directories through the Web server?
- What if somebody discovers a buffer-overflow exploit and now has the ability to execute arbitrary commands on the system?
- What if somebody takes the time to really review how the Web applications is using URLs to access the server, or what state information is being stored in cookies, or HTTP variables, or in the HTML pages themselves?

All too often, by trying to find vulnerabilities in the Web server, the host, or through the Web application itself, an intruder can get the application to give access to data or back-end systems that certainly were unintended for such access.

BEST PRACTICE: Ensure that the Web application generates log entry or event for "unexpected" requests such as a reference to a file that doesn't exist or a parameter that has an invalid value.

BEST PRACTICE: Ensure that the code on the server does not assume that all data sent to the client (e.g., HTML pages) are going to come back in exactly the form as they were sent out. It also needs to generate a log entry or event if, for example, a URL has been changed to a file name (e.g., http://host/file is now /etc/passwd), if the URL has been altered to bypass security conventions (e.g., https://host/file is now http://host/../../../../etc/passwd), or if a URL request has been changed to access files that really belong to somebody else (e.g., https://host/user1/mail/message1 to https://host/user18/mail/message4).

The Last Word

Effective intrusion detection is difficult. In most organizations, it is a project that takes several years to get right with much of the time dedicated not to technology, but to understanding what is "normal" traffic for the environment. While the finish line is far away, it is easy to get started in the right direction. Focusing on the basics and addressing the common intrusion areas first will enable you to quickly make progress in detecting the root cause for many successful intrusions.

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 technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Networld-Interop, CSI, and InternetWorld are among the most popular and 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 and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

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.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

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 and web sites or critical business resources are compromised, 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.

Intrusion Detection and 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.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

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.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1.888 .749.9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com **info@SystemExperts.com**

SystemEXPERTS
LEADERSHIP IN SECURITY