

Raising the Bar: Extending Cisco Intrusion Detection with a Host-Based Solution



Introduction

Firewalls are a key perimeter security solution. Although firewalls provide access control at the network level, they leave several communication ports open. These ports allow external users to communicate with servers within organizations. For example, both mail and Web servers require that specific ports are accessible from the outside. Through these ports, hackers can bypass firewalls and attack servers, using them as an entry into the corporate network.

Intrusion detection systems (IDS) emerged as a complementary solution to firewalls to protect both the network infrastructure (routers, switches, and network bandwidth) and the servers (operating system and application layers) from exploitation or denial of service (DoS). Because of the complexity of the problem, state-of-the-art IDS solutions include two components: Network IDS (NIDS) to protect the network and Host IDS (HIDS) to protect the servers and the applications running on them.

Recently, Cisco Systems extended its existing NIDS offering through the addition of a HIDS component. This paper examines the combination of the existing NIDS and the new HIDS components in the Cisco IDS solution by exploring the security issues that a complete IDS solution should address. These issues include the identification of operations a hacker performs during a typical hacking scenario, and the categorization and listing of the major attack techniques. The Cisco IDS solution highlights the key features of the two components. Finally, this paper analyzes the extent of coverage provided by the combined solution and examines how well the different components complement each other.

Anatomy of an Attack

Hackers break into systems to obtain confidential data, to gain appreciation within their social circles (many times by defacing a Web site), or to harm a site by employing DoS techniques. DoS attacks target networking devices and the servers to block, or at least degrade, the server's availability to legitimate users.

When attempting to penetrate a system, hackers operate in a quiet, systematic manner using the following steps.

Perform Network Reconnaissance

The goal of network reconnaissance is to learn as much as possible about the victim site. Hackers use various network mapping tools to identify the existence of servers or devices. When a networked device is located, its ports are scanned to identify the daemons that are listening on ports. After this is accomplished, a hacker knows the address ranges, different hosts on the network, and the daemons that run on them.

“Own” a System

The goal at this stage is to compromise a device. Given the daemons, hackers can focus their efforts on exploits relevant to the specific daemons. They run vulnerability assessment tools to look for specific issues to exploit. After a vulnerability is identified, a hacker can exploit it either through their own custom exploitation or through one of the hundreds of readily available “kiddie scripts” found on the Internet. Such programs allow hackers to run code on devices and, in some cases, upload programs into the attacked devices.

Next, hackers escalate their privileges and administrative access rights. With the previously loaded programs, hackers can exploit other local vulnerabilities to gain privileged access rights. If they cannot upload a program, they scan configuration and log files looking for clear text passwords. They can run a password-cracking tool against the password hashes to identify pairs of user names and passwords for an administrative account. Finally, hackers install root kits that cover their tracks and keep them *invisible* while intruding on the device. At this stage an attacker “owns” the device and can continue hacking for more interesting information or additional new targets.

Exploit Trust

One of the goals of intrusion is to determine which other devices trust a compromised machine and take advantage of these relationships. For example, hackers might install a *sniffer*, looking for communications with trusted parties involving passwords sent in clear text. Assuming a compromised machine is a Web server, hackers identify backend database servers and the communication programs used to communicate with the databases, allowing them to break into the database servers.

Gain Access

After a hacker gains access to a database, they can access confidential data, such as credit cards and other customer records, or manipulate the data.

“Own” the Network

The next step is to take over any vulnerable systems within the enterprise. At this stage hackers face no real barriers such as firewalls or encryption. They can continue to perform reconnaissance and exploit additional vulnerabilities. Based on the Cisco Security Consulting group’s data, ownership of at least 75 percent of the network is entirely possible.

Attack Techniques

The different attack techniques used during the hacking cycle are classified into three categories: network, operating system (OS), and applications.

Network Attacks

Network attacks target the communication infrastructure, which can be either networking devices such as routers and switches or the networking layer protocols on the server (Layer 3 and below). When breaking into a router, hackers typically gain privileged access and manipulate the configuration settings, impacting the routing of the communications flow. Layer 3 (or below) attacks, which are mostly DoS attacks, target the networking modules of the server. In this case the goal is to crash the server, or at least flood it, blocking legitimate communication with the server.



Distributed DoS (DDoS) is a new network attack technique in which multiple agents simultaneously overwhelm a target with enormous amounts of packets. Using common hacking techniques, hackers locate vulnerable machines, break into them, and install the DDoS agents. Next, hackers activate the agents who are listening on the network waiting for an activation command and a destination address. Once activated, the agents overwhelm the destination by flooding it, and deny access to the destination.

OS Attacks

The popular operating systems share a common design flaw: They support the concept of a super-user (root on UNIX, Administrator on Microsoft Windows). This privileged user can bypass the security measures built into the operating system (OS). For example, root can access any file or device, create users, and assign access privileges. The existence of root makes the OS the primary target for hackers, because once a hacker gains privileged access, they control the server.

The most effective technique to gain privileged access is to exploit buffer overflow vulnerabilities, because buffer overflows are very common. For example, more than 50 percent of the Computer Emergency Response Team (CERT) advisories deal with buffer overflow vulnerabilities¹.

A buffer overflow vulnerability allows a hacker to inject malicious code into another program's address space and execute it in the security context of the attacked program. When the attack process runs in the context of an administrator, the malicious code can execute administrative operations. Typically, the injected code adds a new privileged user with a given password. This allows a hacker to have a privileged account for future access to the box.

Application Attacks

With the emergence of the Internet, several pervasive applications, such as Web servers, e-mail servers, and Domain Name System (DNS) servers, appeared. These daemons are the most exposed targets because they always listen for incoming communication and external users can access them with no interference from the firewall. Consequently, hackers focused their attention on exploring vulnerabilities within these applications.

The primary target is the Web server. Recent advisories on the IIS Web server reveal that it is subject to several new vulnerabilities per month. When attacking the Web server, a hacker sends malicious HTTP requests that seem innocent to the firewall but exploit vulnerability in the Web server and allow a hacker to gain confidential data or execute their malicious code on the Web server.

Other severe attacks that pose security risks to Web servers are Common Gateway Interface (CGI) programs. CGI programs are the primary means for implementing user applications on the Web. When the Web server gets a CGI request, it invokes the CGI program, passing it to the relevant parameters. Many of these custom applications are poorly implemented and lack reasonable input validation of the parameters. As a result, many of them allow hackers to perform malicious activities, such as obtaining confidential information or uploading executables to the server.

Another vulnerable daemon is the Berkeley Internet Name Domain (BIND) DNS program that runs on more than 80 percent of the UNIX DNS servers on the Internet². DNS is a key service on the Internet that provides name resolution. For example, when a user requests the www.cisco.com domain, a DNS server is consulted and returns the IP address of the requested domain. BIND is known to be vulnerable to multiple remote attacks including buffer overflows. Even though several of these issues have been known for many years and patches have been available, there are still many BIND servers on the Internet that are not patched and can be easily penetrated.

1.

2.

Cisco IDS Solution

Given the complexity of an enterprise site, the variety of attack techniques, and the typical hacking scenario, there is a clear need for a comprehensive solution. The solution should protect against the different attack techniques and prevent the malicious actions performed during a typical hacking cycle. The Cisco IDS solution addresses this need by offering a combined solution that includes NIDS and HIDS components. The NIDS primarily addresses the network attacks, whereas the HIDS protects the servers against OS and application attacks.

The NIDS sensors are installed in multiple locations. One important location is in front of the firewall monitoring communication into the organization. In addition, every important network segment is covered with a sensor. The HIDS is first deployed on Internet-facing servers such as the Web, mail, and DNS servers. Because the Internet-facing servers are connected to backend servers, HIDS is also deployed on all the other critical servers within the corporate firewall.

The Cisco IDS Network Sensor

The Network Sensor provides comprehensive protection of the network devices and the communication modules on the server. Its key features include:

Active response—The system incorporates proactive response functionality into the sensor appliances so users can configure the system to automatically shun or eliminate specific connections by changing access control lists (ACLs) on Cisco routers. The shunning capability can be temporarily imposed or, if desired, maintained indefinitely. The rest of the network traffic flows normally; only the unauthorized traffic from internal users or external intruders is quickly and effectively removed. This gives security operators reach across the network to quickly stop misuse and end intruders' access to the network.

Comprehensive detection of network attacks—This includes detection of malicious attacks against routers and switches; detection of Layer 3 (or below) attacks targeting the server's communication modules; and detection of probing or mapping attempts such as ping sweeps and port sweeps, which are usually a precursor to an actual exploit attempt.

Comprehensive detection of application attacks—The system covers multiple application protocols such as HTTP, DNS, File Transfer Protocol (FTP), and others. In addition, it detects an extensive set of communication patterns targeting vulnerable CGI programs.

Unique protection against DoS—Detection of communication between the DDoS agents and the hacker for known DDoS tools such as Trin00 and Tribe Flood Network (TFN).

Sophisticated IP fragmentation reassembly and "Whisker" anti-IDS detection capability support—Techniques such as packet fragmentation and other coding tricks, which are used to bypass typical NIDS technology, were addressed and are not effective against the Cisco IDS network sensor.

The Cisco IDS Host Sensor

The host sensor provides comprehensive protection for the server operating system and the applications running on the servers. The host sensor is installed on each server and guards both the OS and the applications. The system employs call interception techniques to provide the only proactive server security system. Its key features are:

On-the-spot prevention of OS and application attacks—Unlike log-based HIDS, which looks at logs and reacts after the fact when the attack has probably succeeded, the host sensor prevents attacks at the call level before they execute.

Prevention of buffer overflow attacks—The host sensor identifies the execution of the injected code and prevents the system compromise. Two of its unique capabilities are:

- The protection is independent of the means used to deliver the exploit code; the attack is prevented even when the injected code is not transmitted over the wire.



- The mechanism uses a generic signature that prevents the execution of the malicious code even when the specific attack is unknown; this provides protection against unknown buffer overflows for which the vendor has not provided any patch.

Upgraded integrity—The host sensor locks down the system by controlling the access to the system binaries, configuration data, and other system objects. Even the super-user to some degree is restricted from tampering with the system. The host sensor can be configured so that certain system settings are not modified, ensuring that the settings comply with the recommended defaults. These features harden the server operating system and significantly enhance the system's integrity.

Web server shielding—The server sensor includes specific shielding modules to protect the leading Web servers (IIS, Apache, and I-Planet). These modules are based on a behavioral model and provide two key features:

- Protection of the specific application resources against access by other programs (even when running in the context of a privileged user)
- Prevention of malicious use of the Web server. Using a behavioral model that is specific to the Web server, the host sensor prevents unknown attacks because the identification is based on the behavioral model and does not require a specific signature per attack.

Protection against Secure Socket Layer (SSL) encrypted HTTP attacks—NIDS systems cannot decipher HTTP requests that are encrypted using SSL. Hackers exploit this weakness to bypass the NIDS by encrypting the attacks. The encrypted malicious request sneaks past the NIDS and is then decrypted by the Web server and executed by the Web server, exploiting the vulnerability. The host sensor, on the other hand, hooks into the Web server, intercepting the request immediately after it is decrypted but before it is serviced. When the request is found to be malicious, it is dropped and not forwarded to the Web server, making sure the attack is prevented.

Coverage Analysis

This section analyzes the coverage of the Cisco IDS solution. The coverage of the IDS system in a typical hack scenario is reviewed, and the coverage of the different attack techniques is examined.

Table 1 lists different hacker operations during a typical intrusion scenario. The combination of NIDS and HIDS provides good coverage with almost no overlap. The case when the hacker concentrates on DoS is covered later in the section on network attacks.

Table 1 Coverage of a Hack Scenario

Malicious Operation	NIDS Detects/Prevents	HIDS Detects/Prevents
Ping sweeps	Yes	–
Port scan	Yes	–
Exploiting a vulnerability in the OS or the application to run code on the device	Some	Yes
Uploading executables	Some	Yes
Gathering information from configuration and data files	–	Yes
Accessing password hash files	–	Yes
Privilege escalation	–	Yes
Installing a sniffer	–	Yes

Malicious Operation	NIDS Detects/Prevents	HIDS Detects/Prevents
Installing a root kit	-	Yes

Table 2 summarizes the coverage of network and DoS/DDoS attacks. Network sensor is the key tool in this category, but the server sensor provides significant value by preventing the installation of the DDoS agents.

Table 2 Coverage of Attacks Techniques

Attack	NIDS Detects/Prevents	HIDS Detects/Prevents
Attacks against routers and switches	Yes	-
Layer 3 and below network attacks	Yes	-
DDoS agent installation	-	Yes
DDoS communication	Yes	-

Table 3 lists the major value of the host sensor to protect the OS and improve the system integrity.

Table 3 Server Attacks Coverage

Attack/Protective Measure	NIDS Detects/Prevents	HIDS Detects/Prevents
Buffer overflows	Yes/Specific	Yes/General
Privilege escalation	-	Yes
Lockdown of system resources and hardening	-	Yes
Configuration compliance	-	Yes

Table 4 summarizes the extensive coverage that the Cisco IDS provides against applications attacks. There is a special emphasis on the protection of the Web server. Both the network sensor and the host sensor monitor HTTP attacks. The system can even handle SSL encrypted attacks. The network sensor provides an extensive coverage of vulnerable CGI programs. Furthermore, the application-shielding component within the host sensor even prevents unknown attacks by locking down the Web server resources and preventing malicious use of the Web server. The network sensor also covers the other Internet-facing daemons.



Table 4 Application Attacks Coverage

Attack/Protective Measure	NIDS Detects/Prevents	HIDS Detects/Prevents
HTTP	Yes	Yes
CGI	Yes	-
Protection against SSL encrypted Web attacks	-	Yes
DNS	Yes	Some
FTP	Yes	Some
Web server resource protection for IIS, Apache, and Netscape/iPlanet	-	Yes
Prevention of malicious use of the Web server for IIS, Apache, and Netscape/iPlanet	-	Yes

Conclusions

The above analysis demonstrates the significance of extending the existing Cisco IDS solution by adding the host sensor. The combined system:

- Provides full coverage of the hacking cycle
- Detects and protects against network attacks targeting network devices and the networking layer modules on the server that implement Layer 3 or below protocols
- Protects the server OS, locking down the system and improving its integrity
- Provides unparalleled protection for the Web server. This includes monitoring of incoming HTTP attacks and preventing malicious requests; extensive coverage of vulnerable CGI programs; protection against unknown attacks by the application shielding technology, and the ability to protect against SSL encrypted attacks
- Provides extensive coverage of other key daemons on the Internet, including FTP, DNS, and point of presence (POP).

The system also provides unique prevention capabilities. At the network level, shunning is used to block malicious connection. On the server, call interception techniques are used to monitor and reject calls prior to their execution, ensuring that damage is prevented.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France

www-europe.cisco.com

Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com

Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd
Level 9, 80 Pacific Highway
P.O. Box 469
North Sydney
NSW 2060 Australia

www.cisco.com

Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia
Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru
Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa
Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Printed in the USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0108R)

LW2507 09/01

Printed in the USA