Defending Networks with

Intrusion Detection Systems

Securing an enterprise network requires significant technical skills as well as an ongoing effort to keep up with the ever-expanding universe of security exploits, threats, software, methodologies, and tools. This article explains how to increase the level of network security proactively by integrating a network intrusion detection system.

BY JOSE MARIA GONZALEZ

An early-warning system that alerts IT organizations to the presence of intruders can help prevent security breaches on the corporate network and help protect servers from being compromised. To help minimize unauthorized access attempts from both inside and outside the enterprise firewall, administrators can install an intrusion detection system (IDS)—which essentially acts as a network surveillance "camera." This article explores how administrators can thwart break-in attempts using an IDS, such as the Sourcefire® Snort™ product, and Dell™ PowerConnect™ Ethernet switches with port mirroring enabled.[1] In addition, the information in this article can help IT organizations raise corporate awareness of security threats and vulnerabilities.[2]

Understanding intrusion detection systems

While security vulnerabilities have been a topic of increasing concern over the last several years, no effective gauge exists to evaluate the risk that enterprise networks actually face. In spite of using the latest and most powerful security tools and encryption algorithms, companies are still being hacked and Web sites are still being put offline. Best practices require that administrators gather and analyze the data generated by an attacker's unsuccessful access attempts before a successful network breach occurs. This proactive approach to security threats can be far more cost-effective and useful than patching systems after a break-in.

Like a surveillance camera, an IDS enables security teams in an IT environment to capture every action an intruder makes. In this way, an IDS allows administrators to identify how and when a network is being scanned as well as how and when to observe an intruder without being noticed. By using a network adapter in surveillance—or *promiscuous*—mode, an IDS can monitor and analyze in real time every suspicious frame that travels into and out of a network. This setup allows administrators to monitor for attack signatures—specific patterns that usually indicate an unauthorized attempt to gain access to systems. Administrators can download the latest attack signatures from the Internet in the same way that they download virus definition files to keep anti-virus software up-to-date with new security protections.[3]

[1] For more information about Snort, visit http://www.snort.org. Snort was rated the best IDS open source product of 2003 by *Information Security Magazine* (see "The Best: Celebrating Security's Best People, Policy, Process, Products" in *Information Security Magazine*, December 2003, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss288_art517,00.html).

[2] For more information about network security, visit the Honeynet Project at http://project.honeynet.org. Honeynet is a nonprofit research organization of security professionals dedicated to learning the tools, tactics, and motives of the hacker, or *black hat*, community and sharing lessons learned with administrators and other IT workers responsible for network security.

[3] To download the latest attack signatures, visit http://www.snort.org/snort-db.

Two main types of IDS implementation exist:

- **Host-based intrusion detection system (HIDS):** A host-based system monitors activity on a specific server. An HIDS is a software-based solution that continuously scans the system log on a single host.
- **Network-based intrusion detection system (NIDS):** A network-based system monitors and analyzes traffic on the network, instead of on a single host, and provides a reporting mechanism that enables real-time detection and response. For instance, this capability can help an NIDS to stop a distributed denial of service attack (DDoS) before the targeted host crashes.

This article focuses on network-based intrusion detection systems. One of the key decisions for administrators when deploying an NIDS is where to place it. For some organizations a pair of NIDSs is best—one outside the enterprise firewall and one behind it. This type of implementation can report which threats are filtered out by the firewall and which attacks pass through the firewall into the organization's network. By examining the alert logs on both NIDSs, administrators can determine which traffic has been filtered and which has not. *Note:* NIDS system placement can vary widely, and individual networks may use different implementations.[4]

Setting up the NIDS and configuring rules

Figure 1 shows one NIDS server outside the firewall with port mirroring enabled on a Dell PowerConnect Ethernet switch positioned between the firewall and the router. The switch mirrors all frames traveling inbound and outbound between the router and firewall to the port where the NIDS server is connected to the switch.

Setting up the Snort NIDS is easy. Simply download the latest tar file from http://www.snort.org and untar it. The tar file comes with an installation shell script to facilitate installation. A Microsoft® Windows® version of Snort is also available.[5]

Administrators should avoid running any services on the NIDS server except the NIDS software so that invading viruses, worms, and other security threats will find little or nothing to exploit. The NIDS server should be configured only with a hardened operating system and the NIDS software. In addition, the latest security patches to the operating system should be installed. As another precaution, the server should be configured without an IP setup or TCP/IP stack to ensure that the NIDS will be undetectable to would-be intruders. *Note:* If this server were to be compromised, the NIDS would also be compromised and hackers could make system administrators see only what they wanted the administrators to see.

Snort has three main modes: sniffer, packet logger, and network intrusion detection. The third is the most complex, configurable mode

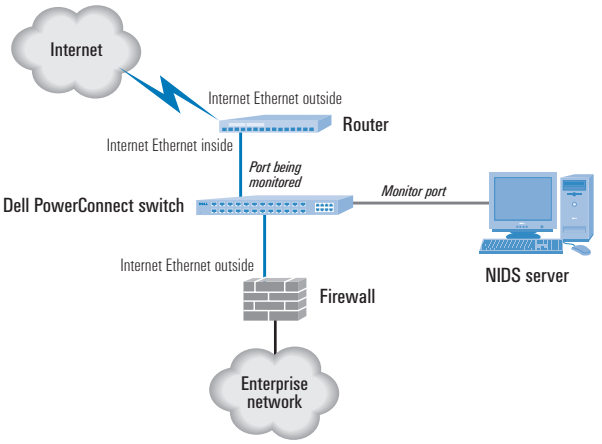

Figure 1. A typical IDS setup

and is the main focus of this article. Network intrusion detection mode analyzes network traffic for matches against a defined rule set stored in a configuration file (snort.conf) and triggers actions based on what the NIDS has captured.

Once Snort is installed, administrators can enable network intrusion detection mode simply by typing the following command line:

```
./snort -d -b -A full -i eth0 172.168.1.0/24
   -l /var/log/snort -c snort.conf
```

Snort.conf is the name of the rules file and the IP address is the network's IP range. Fictitious network address 172.168.1.0/24 is used to represent the Internet IP address pool discussed throughout this article.

Putting an unprotected server on the network

To assess the potential level of threat to unprotected systems, in February 2004 a Dell engineer at the Dell Application Solution Centre in Limerick, Ireland, placed an isolated, off-the-shelf server—running with no security patches and some security weaknesses—outside an enterprise firewall (see Figure 2). Of course, in a real-world environment, administrators should set up enterprise servers behind a firewall to protect them from the public network and contain and control outbound connections if the servers become compromised.

In this exercise, a firewall was not used to protect the target server. However, in the final analysis the target server would have been compromised even if it had been placed behind a firewall (see "Analyzing the captured data"). Certain security exploits—for example, the so-called port 80 problem—trespass firewalls because they are carried out through ports that can get through filters.

[4] For more information about NIDS placement, visit http://www.snort.org/docs/#deploy.

[5] For more information, visit http://www.snort.org/dl/binaries/win32.

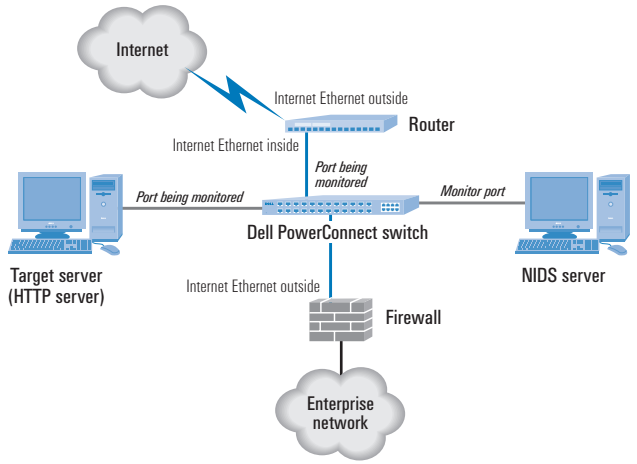

Figure 2. Test environment with target system installed

Analyzing the captured data

The target server was online for five days. In the first 15 minutes, it was randomly scanned 20 times from different locations on the Internet. Over the course of five days, the server received 400 random scans from would-be attackers scanning servers for security vulnerabilities. For a representative sample of the attack data, visit *Dell Power Solutions* online at http://www.dell.com/magazines_extras.

Analyzing captured data requires time, knowledge, and various tools. For this analysis, the following tools were used: the Snort NIDS; Ethereal network protocol analyzer; Argus open source network utility; Tripwire® HIDS file system security tool (installed on the target server); and The Coroner's Toolkit (TCT), a forensic analysis tool. They are all available on the Internet at no cost.[6] Each tool provides different pieces of information and when used together, these utilities can help administrators resolve how, when, and by whom a system was compromised.

Fortunately, the target server was not compromised during the test because hackers did not try to exploit the particular services running on the server. However, the analysis tools found evidence of several attempts to gain unauthorized access to the system using exploits such as directory traversal, Nimda, CodeRed II, MS-SQL, and a Simple Network Management Protocol (SNMP) worm—nothing serious because the system was not running any of the services that these attempts tried to exploit. Further analysis using forensic techniques supported by Tripwire and TCT showed no added, removed, or modified binary files on the target system.

Had a successful attack occurred, hackers could have installed a rootkit utility—which deletes any evidence of unauthorized attempts from the log files—or one or more back doors, which are modified binaries of trust utilities[7] that enable hackers to repeatedly log on to a system without arousing suspicion. Fortunately, the use of an NIDS and forensic analysis tools can help administrators detect such hacker ploys—and therefore help prevent a hacker who gains access to one system from applying the same techniques to compromise other systems and networks.

Taking a layered approach to network security

Network security is one of the most compelling concerns facing IT organizations today. As the security exercise in this article demonstrated, unknown attackers scan networks randomly to exploit security vulnerabilities on a daily basis. Unfortunately, there is no silver bullet or single product that can protect enterprise data against malicious intent. Even a well-configured firewall cannot provide adequate protection because many threats exploit weaknesses such as ports that are generally open at the firewall.

Diverse hardware and software tools—including Snort, Tripwire, and port mirroring on Dell PowerConnect switches—are available to help administrators detect security breaches and protect enterprise networks. Using layers of protection, such as those listed here, can improve the chances of keeping networks and systems secure. Some of the techniques that network security staff should consider include:

- Scanning to assess network vulnerabilities
- Conducting penetration testing and log audits
- Setting up security policies within the enterprise
- Installing the latest security patches as soon as they are available
- Educating IT staff about social engineering attacks
- Reviewing newsletters, mailing lists, and other security information on a daily basis to learn of new threats
- Using the scanning and detecting capabilities of an NIDS to find out what is traveling into and out of the network

Today, the level of threat to mission-critical enterprise data and assets is high. Effective network security requires an ongoing effort to defend against attack on a 24/7 basis, and an IDS can provide valuable assistance in helping to achieve network security goals.

Acknowledgments

The author would like to thank Kevin Libert, director of EMEA Enterprise Systems Marketing, and Anthony Quigney, Dell Application Solution Centre manager, for valuable feedback.

Jose Maria Gonzalez (jose_maria_gonzalez@dell.com) is a system consultant on Microsoft technologies and security at the Dell Application Solution Centre in Limerick, Ireland. He has a B.S. in Computer Science from the University of Madrid, and is a Microsoft Certified Systems Engineer (MCSE) and Red Hat Certified Engineer® (RHCE®).

[6] For more information, visit http://www.ethereal.com, http://www.qosient.com/argus, http://www.tripwire.org, and http://www.porcupine.org/forensics/tct.html.

[7] On UNIX® or Linux® servers, trust utilities include bin, ls, top, and ps.