PowerTech®
your security expert

SECURITY REVIEW

Intrusion Detection System

Protect sensitive data from those with the most access

OVERVIEW

Leveraging an easy-to-configure interface in IBM i Navigator, the integrated **intrusion detection system** (IDS) employs policies to trigger alerts and regulate suspicious traffic from any IP address—including virtual LAN (VLAN) addresses.

Typically, servers running IBM i are not Internet-facing and subjected to irregular network traffic, but security officers are strongly recommended to enable this functionality anyway: IDS is crucial for defending against malicious attacks and issues with TCP/IP communications.

What the IBM IDS aims to defend, however, is only half the equation. Intruders, unfortunately, do not always announce themselves via TCP/IP packet anomalies. Users who successfully access the secure network—without legitimate permission—can often move around without triggering an alert by IBM IDS, also known as a traditional network IDS (NIDS).

Even more dangerous than outside threats are legitimate users who could be misusing their legitimate credentials. Despite the ability of the IBM IDS to detect TCP attacks, it is powerless against access by employees, contractors, partners, vendors, and more.

CHALLENGE

To catch threats from inside and outside your organization, you must be able to detect traffic anomalies and alert on suspicious activity from any source. You also must be able to monitor for activities that circumvent your security policy; and you must be able to announce if a user attempts to access accounts, sensitive or application files, and system functions without authorization. PowerTech solutions for host-based intrusion detection (HIDS) are designed to this end, providing comprehensive monitoring and complementing the built-in IBM i functionality for network threats.

Without a HIDS solution, anyone with access to a user account can access information—to view, modify, or download data—without generating an audit trail or an alert. On many servers, users are gaining transparent command privileges.

POWERTECH IDS SOLUTIONS

PowerTech HIDS solutions address the shortfalls of NIDS and report and alert on events in each system. And their seamless integration with the OS allow the solutions to enhance visibility to unauthorized activity, a critical goal of compliance and security for any organization.

The PowerTech Group, Inc.
www.powertech.com

TEL USA: 253.872.7788
TOLL FREE: 800.915.7700

Network Security

Network Security™ is a transaction and object-based Host IDS. Its audit and access control functionality provides the ability to monitor requests that enter the system through interfaces like FTP and ODBC. As a firewall, Network Security supplements object security with flexible authority settings not available in IBM i.

Compliance Monitor

Compliance Monitor™ is a forensics solution for interrogating security audit log entries, including intrusion events and authority violations logged by the NIDS and HIDS. It generates reports over multiple partitions as easily as a standalone server, and it can leverage powerful scheduling, export, and distribution features to ensure information is dispersed efficiently.

Interact

Interact,™ a powerful, efficient notification agent, gives timely escalation and real-time visibility to events. NIDS and HIDS events can be relayed to an ISS console; sent to a message queue and processed with a messaging solution; or converted a common event format (CEF) and escalated to an external SYSLOG server or Security Information Management (SIM) solution.

CONCLUSION

IBM Power Systems leads the industry with world-class security controls, and the inclusion of a network IDS within IBM i demonstrates IBM's commitment to security and compliance. For more comprehensive IDS capabilities, take advantage of this commitment by combining NIDS functionality with PowerTech IDS solutions.

Are you considering an IDS initiative? Leverage the security facilities in IBM i to build a solid foundation. Then deploy PowerTech IDS solutions, which give you:

- Powerful access control and activity tracking (by user and IP address) of transactions originating from the network.
- Forensic reporting on 70+ audit events (and hundreds of security configuration metrics).
- Real-time security event notification.
- Ability to monitor and report on non-compliance.

GET THE WHITE PAPER

Learn more about how PowerTech can simplify your IDS initiative. Find more information and download the white paper at **www.powertech.com/ids**.

About the PowerTech Group, Inc.

Because Power Systems servers are used to host particularly sensitive corporate data, every organization needs to practice proactive compliance security. As an IBM Advanced Business Partner with over 1,000 customers worldwide, PowerTech understands corporate vulnerability and the risks associated with data privacy and access control.

Visit www.powertech.com to find white papers, case studies, and product demonstrations. Or, call 800-915-7700 (USA) or 253-872-7788 to speak to a Security Advisor.

IBM Business Partner