Secure IDS deployment best practices

searchitchannel.techtarget.com /tip/Secure-IDS-deployment-best-practices

by Patrick Harper

Using open source IDS Snort as an example, this tip offers eight best practices for securely deploying a network intrusion detection system.

Vendor Resources

- Monitoring network traffic: Appliance placement and choke points –Sourcefire
- IDS vs. IPS –Sourcefire

Whether you're deploying an intrusion detection system on a large network with many sensors or a small network with a single sensor, you should deploy the device in as secure and logical a manner as possible. In this article I will discuss some techniques value-added resellers (VARs) and security consultants can use for securely deploying a network IDS on a customer's network. I will focus on Snort deployments, but these same principles can be used for other IDSes and applications.

VLAN placement

Determine what your customer wants monitored. Traffic can either be monitored from the outside of the firewall, or it can be monitored on the inside of the firewall. I personally prefer the inside but like to keep a sensor on the outside in case I need to look at that traffic. I use tcpdump or a sniffer like Wireshark (formally Ethereal) to monitor the interfaces. This makes it easier to determine network problems and detect denial-of-service attacks.

Management network

Your customer's IDS information should not be available to just anyone. To help protect this information, set up a management VLAN for the non-sniffing interfaces to sit on. If this is not possible or practical, then consider using iptables and TCP wrappers to restrict who can view what and from where.

Secure communications

HTTPS should only be used to view the IDS management and reporting interface. All communication between sensors and management consoles should be tunneled through SSH or Stunnel.

Secure access to management and reporting interface

Never leave the reporting interface unprotected. Even if you're using the built-in access control of the application itself, it should always be protected with Web server or file level permissions, depending on the Web server your customer is using. If it is on the main LAN, then you can also limit access to it via iptables or TCP Wrappers.

Securing the management interface

Remove all applications and utilities that are not needed, close all ports that are not being used, and allow communication to only what the sensor or manager needs to talk to. This is a basic policy in all matters of systems administration, and it is especially important when considering the sensitive data IDS sensors might pick up.

Reporting and checking

If you are also managing your customer's IDS, check it regularly. I review mine every hour or two, and keep a log of the last time I checked in. I view all alerts from that time forward so I miss nothing. I give it a more thorough review first thing in the morning. For monitoring Snort, I use BASE. It is based upon the old ACID code that most

people have used and are familiar with. It is, however, being actively developed and works much better than previously.

Tuning and updates

While not truly a secure deployment concern, tuning is one of the most important steps in deploying an IDS. If you or your customer becomes overwhelmed with irrelevant alerts, you will be more apt to ignore alerts as time goes by. Insofar as updates are concerned, keep both the rules and engine up to date. The use of Oinkmaster is recommended for Snort deployments. It will update your rules on a regular basis and you'll be notified via email of any changes. I have written an installation document for Oinkmaster available at Snort.org. The use of SourceFire VRT rules is recommended for Snort installs due to the research and development that goes into them. They are built to the vulnerability rather then a particular exploit and are thoroughly tested by the SourceFire VRT team. You can register to receive them on Snort.org.

Time Syncing

Finally, set up an NTP server on the management system and configure the sensors to update from it. This is key to determining what is happening and when on the network.

By following some of the basic steps and using the tools and rules I have mentioned, you can help keep your customer's security devices and their data more secure. If you want to install and test snort, I have an easy to follow guide that will get you up and running in a few hours on Snort.org.

About the author
Patrick Harper is currently an information security engineer with an IT consulting and management firm specializing in the area of healthcare IT. He started in IT in 1994 doing PC builds, small Novell network installs and PC repair. He progressed to working with Internet technologies and opened an ISP in 1996. While running the ISP, Patrick gained first hand security expertise, securing servers and systems. This led to his expertise in intrusion prevention/detection systems and protocol analyzers, specifically focusing on Snort and other open source solutions.

-ADS BY GOOGLE