Global Information Assurance Certification Paper

What Do You Do After You Deploy the IDS?

Chris Morris

Jan 3, 2001

Your company has finally decided to implement an intrusion detection system (IDS). You have listened to vendor after vendor describe his wares in detail and explain why their system will work best in your environment. You have chosen your IDS based on price, support, ease of use, installation and best company t-shirt design. You have tested your new IDS successfully and have now deployed it into the production environment. The question is: what now?

Hopefully before you have deployed your IDS into your environment, you took the time to develop a solid IDS monitoring policy and procedure. These documents are written to answer that "what now" question. You must determine how you are going to monitor your systems, who will monitor them, what will you do when you get an alert and who is going to fix the vulnerability. Additionally, you must determine the level of response that you will enable once an intrusion has been detected. The ideas outlined in this paper should be useful for network, host-based and so-called hybrid intrusion detection systems and for the development of response procedures.

IDS MONITORING

The goal of an IDS is to positively identify real attacks while negatively identifying so-called false positives (an event, incorrectly identified by the IDS as being an intrusion when none has occurred). Therefore, the IDS will have to be monitored. To monitor the IDS effectively, you will need to develop effective plans in the following areas:

- IDS monitoring and response
- Incident handling
- Forensic analysis and data retention
- Reporting

If your company is like most you will not have the benefit of highly trained security experts monitoring the console 24/7. That task is likely to fall to the level one operator working in the Network Operations Center. This individual will typically not have formal security training and most likely will not know what to do with an alert. Therefore, it is important to provide this person with well-documented monitoring procedures that detail actions for specific alerts. Another tactic for monitoring the IDS is to have the system page or e-mail designated personnel of specific alerts. Either way the IDS management should develop a list of threats that you want to be alerted for and have the operator or analyst watch for them. These threats can range from port scans to unauthorized ftp events to denial of service attempts.

INCIDENT HANDLING

Why bother detecting an attack in the first place, if you know you are not going to do anything about it? Good question. You are going to have to develop a well-documented incident handling procedure if you are going to utilize the information that you have captured during monitoring. The incident handling procedures must be understood, accessible and rehearsed. It may be of value to develop an outline of goals and objectives similar to the following in how your company will handle an incident:

- Determine how the incident happened.
- Establish a process for avoiding further exploitations of the same vulnerability.
- Avoid escalation and further incidents.
- Assess the impact and damage of the incident.
- Recover from the incident.
- Update procedures as needed.
- Determine who was responsible (if appropriate and possible).

Of course, depending on the seriousness of the attack, all of the objectives above may not necessarily have to be instigated. A tiered response and escalation procedure for detected potential security breaches may be implemented as part of your emergency response. These levels should be outlined in your well-documented incident handling procedure manual. An example of incidents followed by the response is shown below.

Level 1 One instance of potentially unfriendly activity (finger, unauthorized telnet, port scan, etc.).
- Record user/IP address/domain of intruder.
- Maintain vigilance for future break-in attempts from this user.

Level 2 One instance of clear attempt to obtain unauthorized information or access (download password files, access restricted areas, etc.) or a second Level 1 attack.
- Collect and protect information associated with the intrusion.
- Research origin of connection.
- Contact ISP and ask for more information regarding attempt and intruder.
- Research potential risks related to intrusion method attempted.
- Upon identification of intruder, inform intruder of our knowledge of his actions and warn him against future recriminations if attempt is repeated.

Level 3 Serious attempt to breach security (multi-pronged attack, denial of service attempt, etc.) or a second Level 2 attack.
- Contain the intrusion and decide what action to take.
- Collect and protect information associated with the intrusion.
- Notify your client (if in data center or similar) being attacked of the situation and maintain notification of progress at each following step.
- Eliminate the intruder's means of access and any related vulnerabilities.
- Research origin of connection.

- Contact ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist us in this regard.
- Research potential risks related to or damage caused by intrusion method attempted.

SIRT

Of course, all potential, suspected, or known information security incidents should be reported to the company Information Security Incident Response Team (SIRT) or designated security individual(s). These personnel will be identified in the procedure document for handling incidents. The SIRT will assign personnel who will assemble all needed resources to handle the reported incident. The incident coordinator will make decisions as to the interpretation of policy, standards and procedures when applied to the incident.

Law enforcement and investigative agencies will be notified, as needed and required, by the SIRT. In the event of an incident that has legal consequences, it is important to establish contact with investigative agencies (e.g., the FBI in the U.S.) as soon as possible. Local law enforcement should also be informed as appropriate. Legal counsel should be notified of an incident as soon as it is reported. At a minimum, legal counsel should be involved to protect the legal and financial interests of your company.

DOCUMENTATION

All information security incidents must be documented. This documentation provides a reference to be used in case of other similar incidents. System and network log files, network message traffic, user files, results produced by intrusion detection tools, analysis results, system administrator console logs and notes, and backup tapes that capture the before-intrusion and after-intrusion states of the affected system must be carefully collected, labeled, cataloged, and securely stored at each stage of intrusion analysis. Evidence and activity logs should be protected before, during and following the incident. To ensure that evidence will be acceptable to the legal community, collecting evidence should be done following predefined procedures.

RESPONSE ACTIONS

The incident handling process will provide some escalation mechanisms. In order to define such a mechanism, the SIRT should create an internal classification scheme for incidents. Associated with each level of incident will be the appropriate procedures. The following is an example of level of incidents with corresponding definitions:

- **Priority One** – protect human life and people's safety; human life always has precedence over all other considerations.

- **Priority Two** – Protect restricted and/or internal data. Prevent exploitation of restricted systems, networks or sites. Inform affected restricted sensitive systems, networks or sites about already occurred penetrations while abiding by any applicable government regulations.

- **Priority Three** – Protect other data including managerial, because loss of data is costly in terms of resources. Prevent exploitations of other systems, networks or sites and inform already affected systems, networks or sites about successful penetrations.

- **Priority Four** – Prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc.). Damage to systems can result in costly down time and recovery.

- **Priority five** – Minimize disruption of computing resources (including processes). It is better in many cases to shut a system down or disconnect from a network than to risk damage to data or systems. Each data and system owner must evaluate the trade-off between shutting down and disconnecting, and staying up. This decision must be made prior to an incident occurring. There may be service agreements in place that may require keeping the systems up even in light of further damage occurring. However, the damage and scope of an incident may be so extensive that service agreements may have to be over-ridden.

CONCLUSION

An Intrusion Detection System is a tool that is part of a good security architecture and Multi-Layered Defense Strategy. However, once the IDS is deployed onto the network the system must be monitored and alerts responded to. Documented monitoring guidelines and alert criteria must be developed so you can respond effectively to an incident. Response actions should be developed for incident handling procedures.

REFERENCES

Bace, Rebecca. "An Introduction to Intrusion Detection and Assessment".
URL: http://www.secinf.net/info/ids/intrusion/

Carnegie Mellon, CERT Coordination Center, "Establish policies and procedures for responding to intrusions".
URL: http://www.cert.org/security-improvement/practices/p044.html

Carnegie Mellon, CERT Coordination Center, "Prepare to Respond to Intrusions".
URL: http://www.cert.org/security-improvement/practices/p045.html

Carnegie Mellon, CERT Coordination Center, "Responding to Intrusions". July 30, 1999

URL: http://www.cert.org/security-improvement/modules/m06.html

Carnegie Mellon, CERT Coordination Center, "State of the Practice of Intrusion Detection Technologies". Nov. 16, 2000
URL:
http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028chap01.html

FAQ: Network Intrusion Detection Systems. Version 0.8.3, March 21, 2000
URL: http://www.ticm.com/kb/faq/idsfaq.html#3.6

Ranum, Marcus J. "Intrusion Detection: Challenges and Myths". 1998
URL: http://secinf.net/info/ids/ids_mythe.html

Sondra Schneider, Erik Schetina and Donald Stahl. "Life After IDS". Sept. 1999
URL: http://www.infosecuritymag.com/sept99/cover.htm