IDS RESPONSE BEHAVIOR

Each IDS will respond to external stimulation in different ways, depending on its configuration and function. Some may respond in active ways, collecting additional information about the intrusion, modifying the network environment, or even taking action against the intrusion. Others may respond in positive ways, setting off alarms or notifications, collecting passive data through SNMP traps, and the like.

Response Options for an IDS

Once an IDS detects an anomalous network situation, it has a number of options, depending on the policy and objectives of the organization that has configured it as well as the capabilities of the organization's system, In configuring an IDS's responses to alerts, the system administrator must exercise care to ensure that a response to an attack (or potential attack) does not compound the problem or create a situation that is more disastrous than that of a successful attack. For example, if a NIDS reacts to a suspected DoS attack by severing the network connection, the NIDS has just accomplished what the attacker had hoped. If the attacker discovers that this is the default response to a particular kind of attack, all he or she has to do is repeatedly attack the system at intervals in order to have the organization's own IDS response interrupt its normal business operations. An analogy to this approach would be the case of a potential car thief who walks up to a desirable target in the early hours of a morning, strikes the car's bumper with a rolled up newspaper, and then ducks into the bushes. When the car alarm is triggered, the car owner wakes up, checks the car, determines there is no danger, resets the alarm, and goes back to bed. The thief then repeats the triggering actions every half hour or so until the owner gets so frustrated that he or she disables the alarm, believing it to be malfunctioning. The thief is now free to steal the car without worrying about triggering the alarm.

IDS responses can be classified as active or passive. An active response is one in which a definitive action is initiated when certain types of alerts are triggered. These automated responses include collecting additional information, changing or modifying the environment, and taking action against the intruders. In contrast, IDSs with passive response options simply report the information they have already collected and wait for the administrator to take actions. Generally, the administrator chooses a course of action after he or she has analyzed the collected data, and thus with passive-response IDSs, the administrator becomes the active component of the overall

system. The latter is currently the most common implementation, although most systems allow some active options that are kept disabled by default.

The following list illustrates some of the responses an IDS can be configured to produce. Note that some of these are unique to a network-based or a host-based IDS, while others are applicable to both[11].

Audible / visual alarm: The IDS can trigger a .wav file, beep, whistle, siren, or other audible or visual notification to alert the administrator of an attack. The most common type of such notifications is the computer pop-up window. This display can be configured with color indicators and specific messages, and it can also contain specifics as to what type of attack is suspected, the tools used in the attack, the level of confidence the system has in its own determination, and the addresses and/or locations of the systems involved.

- SNMP traps and Plug-ins: The Simple Network Management Protocol contains trap functions, which allow a device to send a message to the SNMP management console to indicate that a certain threshold has been crossed, either positively or negatively. The IDS can execute this trap, telling the SNMP console an event has occurred. Some of the advantages of this operation include the relatively standard implementation of SNMP in networking devices, the ability to configure the network system to use SNMP traps in this manner, the ability to use systems specifically to handle SNMP traffic, including IDS traps, and the ability to use standard communications networks.
- E-mail message: The IDS can e-mail an individual to notify him or her of an event. Many administrators use personal digital assistants (PDAs) to check their e-mail frequently, thus have access to immediate global notification. Organizations should use caution in relying on e-mail systems as the primary means of communication between the IDS and security personnel, for not only is e-mail inherently fraught with reliability issues, but an intruder may compromise the e-mail system and block the sending of any such notification messages.
- Page or phone message: The IDS can be configured to dial a phone number, producing either an alphanumeric page or a modem noise on a phone call.
- Log entry: The IDS can enter information about the event (e.g., addresses, time, systems

involved, protocol information, etc.) into an IDS system log file, or operating system log file. These files can be stored on separate servers to prevent skilled attackers from deleting entries about their intrusions and thus hiding the details of their attack.

- Evidentiary packet dump: Those organizations that have a need for legal uses of the IDS Data may choose to record all log data in a special way. This method will allow the organization to perform further analysis on the data and also submit the data as evidence in a future civil or criminal case. Once the data has been written using a cryptographic hashing algorithm (discussed in detail in Chapter 8), it becomes evidentiary documentation-that is, suitable for criminal or civil court use. This packet logging can, however, be resource-intensive, especially in denial-of-service attacks.
- Take action against the intruder: It has become possible, although not advisable, to take action against an intruder. Known as trap and trace, hack-hacking, or traceback, this response option involves configuring intrusion detection systems to conduct a trace on the data leaving the attacked site and heading to the systems instigating the attacks. The idea here is that once these attacking systems are identified, some form of counterattack can be initiated. While this sounds tempting, it is ill advised and may not be legal. An organization only owns a network to its perimeter, and conducting traces or back-hacking to systems outside that perimeter may make the organization just as criminally liable as the individual(s) who began the attack. In addition, it is not uncommon for an attacker to compromise an intermediary system and use that system to conduct the attack. If an organization attempts a back-hack and winds up damaging or destroying data on the intermediary system, it has, in effect, attacked an innocent third party, and will therefore be regarded, in the eyes of that party, as an attacker. The matter can be further complicated if the hacker has used address spoofing, a means by which the attacker can freely change the address headers on the source fields in the IP headers and make the destination address recipients think the packets are coming from one location, when in reality they are coming from somewhere else. Any organization planning to configure any sort of retaliation effort into an automated intrusion detection system is strongly encouraged to seek legal counsel.

- Launch program: An IDS can be configured to execute a specific program when it detects specific types of attacks. A number of vendors have specialized tracking, tracing, and

response software that could be part of an organization's intrusion response strategy.

- Reconfigure firewall: An IDS could send a command to the firewall to filter out suspected packets by IP address, port, or protocol. (It is, unfortunately, still possible for a skilled attacker to break in by simply spoofing a different address, shifting to a different port, or changing the protocols used in the attack.) While it may not be easy, an IDS can block or deter intrusions by one of the following methods:

  Establishing a block for all traffic from the suspected attacker's IP address, or even from the entire source network from which the attacker appears to be operating. This blocking might be set for a specific period of time and be reset to normal rules after that period has expired.

port, should that connection be linked to a system that is malfunctioning or otherwise interfering

  Establishing a block for specific TCP or UDP port traffic from the suspected attacker's address or source network, blocking only the services that seem to be under attack.

  Blocking all traffic to or from a network interface (such as the organization's Internet connection) if the severity of the suspected attack warrants that level of response. Terminate session: Terminating the session by using the TCP/IP protocol specified packet TCP close is a simple process. Some attacks would be deterred or blocked by session termination, but others would simply continue when the attacker issues a new session request. Terminate connection: The last resort for an IDS under attack would be to terminate the organization's internal or external connections. Smart switches can cut traffic to/from a specific

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf