CMSGu2011-10

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Intrusion Detection and Prevention Systems

CERT-MU

National Computer Board
Mauritius

Version 1.0

October 2011

Issue No. 10

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to assist organisations in understanding Intrusion Detection and Prevention Systems (IDPS) and also to guide them in the implementation, configuration, security, and maintenance of IDPS.

1.2 Audience

The target audience for this document includes computer security staff, program managers, computer security incident response teams (CSIRTs), and system and network administrators who are responsible for managing or monitoring IDPS technologies.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on IDPS.

Section 3 describes four types of available IDPS available.

Section 4 details the planning, evaluation and implementation of an IDPS

Section 6 concludes the document.

Section 7 comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

2.1 What is Intrusion Detection and Prevention?

Intrusion Detection is the ability to detect actions that attempt to compromise the confidentiality, integrity or availability of a resource. Intrusion Detection however does not always include prevention of intrusions. Intrusion prevention is a defensive approach to network security used to identify potential threats and respond to them swiftly.

2.2 Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPSs) are composed of software that helps organisations to monitor and analyse events occurring in their information systems and networks, and to identify and stop potentially harmful incidents. With the growing dependence of organisations on information systems to carry out essential activities and with the increasingly frequent and intense attacks on systems, IDPSs have become an essential component of the security infrastructure of nearly every organisation.

2.3 Functions of Intrusion Detection and Prevention Systems

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorised access to systems from the Internet, and authorised users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorised. Although many incidents are malicious in nature, many others are not; for example, a user could enter an incorrect address of a system and accidentally attempt to connect to a different system without authorisation.

Intrusion detection and prevention systems identify possible incidents, log information about them, attempt to stop them, and produce reports for security administrators. The systems also assist organisations in identifying problems with security policies, documenting threats, and deterring individuals from violating security policies.

3.0 Types of Intrusion Detection and Prevention Systems

The following intrusion detection and prevention systems are based on the type of events that they monitor and the ways in which they are deployed.

3.1 Network-Based Systems

Network-based systems monitor network traffic for particular network segments or devices and analyse the network and application protocol activity to identify suspicious activity. This type of system can identify many different types of events of interest, and is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

3.2 Wireless Systems

Wireless systems monitor wireless network traffic and analyse it to identify suspicious activity involving the wireless networking protocols themselves. This type of system cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organisation's wireless network to monitor it, but it can also be deployed to locations where unauthorised wireless networking could be occurring.

3.3 Network Behaviour Analysis (NBA) Systems

Network Behaviour Analysis (NBA) systems examine network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware, and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organisation's internal networks, and are sometimes deployed where they can monitor flows between an organisation's networks and external networks.

3.4 Host-based Systems

Host-based systems monitor the characteristics of a single host and the events occurring within that host for suspicious activity. The types of characteristics that a host-based IDPS might monitor are network traffic for that host, system logs, running processes, application activity; file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

4.0 Planning, Evaluation and Implementation of an IDPS

An important part of the planning phase of an IDPS installation is determining where the critical assets of an organisation are located throughout the network and what traffic the organisation wants to monitor/detect. Some factors consider during the planning stage should include:

- Assets that you need to monitor
- Whether monitoring of traffic include both internal and external (traffic outside the boarder router) traffic
- Sensor placement could cause latency on high traffic networks - this becomes an issue of security versus productivity
- The number of sensors that will be required to adequately monitor all segments of your network
- Identification of high-risk servers and devices and inclusion of these locations in your placement of the sensors. Ideally a Vulnerability Assessment should be performed to assess and identify these assets on the network.
- Installation and location of sensors with Confidentiality, Integrity and Availability in mind
- Actions to be taken when an incident occurs
- Any interaction(s) the IDS/IPS have with your firewall and/or switches to facilitate blocking or denying malicious traffic. Is this traffic secured?
- Identification of who will be assigned to manage and respond to alerts generated by the IDS/IPS

In addition to the above, a strong Incident Handling Policy should be in place to respond to these intrusion attempts. A good Incident Handling policy should include the following: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

9.1 Evaluation - General Requirements

Prior to evaluating IDPS products, organisations should first define the general requirements that the IDPS solution and products should meet. The features provided by IDPS products and the methodologies that they use vary considerably, so a product that best meets one organisation's requirements might not necessarily be suitable for meeting another organisation's requirements. Also, a single IDPS product might not be able to meet all of an organisation's requirements for a particular type of IDPS technology (e.g., network-based),

necessitating the use of multiple IDPS products of the same technology type. This is most common for large environments and for environments in which IDPS technologies serve multiple operational purposes.

9.1.1 System and Network Environments

Evaluators first need to be familiar with the characteristics of the organisation's system and network environments, so that an IDPS can be chosen that will be compatible with them and able to monitor the events of interest on the systems and/or networks. This knowledge is also needed to design the IDPS solution and determine how many components (e.g., sensors, agents) will be needed and where they will be deployed (e.g., which systems will run IDPS agents, which network segments will be monitored). Characteristics to consider include the following:

- **Technical specifications of the IT environment**
  Examples:
  - Network diagrams and maps laying out the architecture (both logical and geographical) of the network, including all connections to other networks, and the number and locations of hosts
  - The operating systems (OS), network services, and applications run by each host that might need to be protected by the IDPS
  - The attributes of non-security systems with which the IDPS might need to be integrated, such as network management systems.

- **Technical specifications of the existing security protections.**
  Examples:
  - Existing IDPS implementations
  - Centralised logging servers and SIEM software
  - Anti-malware software, such as anti-virus and anti-spyware software
  - Content filtering software, including anti-spam software
  - Network firewalls, routers, proxies, and other packet filtering devices and software
  - Communication encryption services, including link encryptors, Virtual Private Networks (VPN), and Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

9.1.2 Goals and Objectives

Once the existing system and network environments have been thoroughly understood, evaluators should document and communicate the technical, operational, and business objectives and objectives they wish to attain by using an IDPS. The following questions should be considered in this area:

- **The types of threats for which the IDPS should provide protection**
  Evaluators should state, as specifically as possible, the concerns that the organisation has with regards to the types of threats that are instigated both outside the organisation and inside the organisation (insider threats). Insider threats should cover not only users who attack the system from within, but also authorised users who violate their privileges, thereby violating organisational security policy or laws.

- **Any needs to monitor system and network usage for acceptable use violations or non-security reasons**
  In some organisations, there are Acceptable Use Policies that target user behaviours that may be considered personnel management rather than system security issues. These might include accessing websites that provide content of questionable content or using the organisation's systems to send personal e-mails or other messages to pester individuals. Some IDPSs provide features for detecting such occurrences. Monitoring usage can also assist organisations in determining when systems and networks are reaching their capacity limits and therefore might need to be upgraded or replaced.

9.1.3 Security and Other IT Policies

Evaluators should review their existing security policies and other IT policies before selecting products. The policies act as a specification for many of the features that the IDPS products need to provide. Examples of policy elements that can contain useful information for IDPS product selection are as follows:

- **The goals of the policies**
  It is helpful to communicate the goals outlined in the policies in terms of the standard security goals (integrity, confidentiality, and availability) as well as more generic management goals (privacy, protection from liability, manageability).

- **Reasonable use policies or other management provisions**

  As mentioned above, many organisations have Acceptable Use Policies included as part of security policies and other IT policies.

- **Processes for dealing with specific policy violations**

  It is important to have a clear idea of what the organisation aims to do when an IDPS detects that a policy has been violated. If the organisation does not intend to react to such violations, it may not make sense to configure the IDPS to detect them. If the organisation wishes to respond to such violations, it may be necessary to select an IDPS product that can detect them, and perhaps also perform automated responses to halt them.

9.1.4 External Requirements

Evaluators should understand if the organisation is subject to oversight or review by another organisation, or if it is likely that the organisation will be subject to an additional form of oversight in the near future. If either is true, the evaluators should determine if that oversight authority requires IDPSs or other specific security resources. Examples of external requirements are as follows:

- **Security-specific requirements levied by law**

  For example, there may be legal requirements to protect personal information (such as salary information or medical records) stored on systems. There could also be legal requirements for investigation of security violations that divulge or jeopardise that information.

- **Audit requirements for security best practices**

  The audit requirements may specify functions that the IDPS must provide or support. Some IDPSs meet the special needs of certain industries or market niches, such as reports designed to meet legislative requirements for health care or financial institutions.

- **System accreditation requirements**

If the organisation's systems are subject to accreditation, the evaluators should identify and consider the accreditation authority's requirements for IDPS or other security protection.

- **Requirements for law enforcement investigation and resolution of security incidents**

  They may impose additional requirements on IDPS functions, in particular those dealing with collection and protection of IDPS logs as evidence.

- **Requirements to purchase products previously evaluated through an independent process**

  For example, an organisation might be required to or prefer to purchase products that have been rated by an evaluating body.

- **Cryptography requirements**

  For instance, some organisations are required to purchase products that use approved encryption algorithms to protect network communications and storage of sensitive data.

9.1.5 Resource Limitations

IDPSs can protect an organisation's systems, but not free of charge. It is obviously not profitable to invest in additional IDPS features if the organisation does not have sufficient systems or personnel to use them. Evaluators should consider the following:

- **The budget for acquisition and life cycle support of IDPS hardware, software, and infrastructure**

  The total cost of ownership of IDPSs is much more than acquisition costs. Other costs may be associated with acquiring systems on which to run software components, deploying additional networks, providing sufficient storage for IDPS data, obtaining specialised assistance in installing and configuring the system, and training personnel.

- **The staff needed to monitor and maintain an IDPS**

  Some IDPSs are designed, assuming that personnel will be available to monitor and maintain them around the clock. If evaluators do not expect having such personnel available, they may wish to go for systems that require less than full-time attendance

or are designed for unattended use, or they could consider the feasibility of outsourcing the monitoring process and possibly also the maintenance of the IDPS.

9.2 Security Requirements

Further to defining general requirements, evaluators also need to define more specialised sets of requirements. This section specifically addresses security requirements.

9.2.1 Information Gathering Capabilities

Organisations should identify the information gathering capabilities needed for their IDPS's detection methodologies and analysis functions, and evaluate each IDPS product under consideration for its ability to offer those capabilities.

9.2.2 Logging Capabilities

Organisations should closely examine the event and alert logging capabilities of each IDPS solution being evaluated. The quality of logging, both completeness and accuracy, affects an organisation's ability to perform analysis, confirm the precision of alerts, and correlate logged events with events recorded by other sources (e.g., other security controls, OS logs). IDPSs should log basic information at a minimum, such as a timestamp, the event type, the source of the event, and the sensor or agent that detected the event. Each IDPS should also log supporting data involving the details of the event; these data fields are specific to particular IDPS product types. IDPS products should also provide a mechanism that allows users to associate each log entry with corresponding external references, including Common Vulnerabilities and Exposures (CVE) numbers, which provide universal identifiers for vulnerabilities, and possibly other references such as vendor security advisories.

9.2.3 Detection Capabilities

Organisations should carefully evaluate the detection capabilities of each IDPS solution being evaluated. For many implementations, the detection capabilities are the most important function. Comparing detection capabilities is a complex undertaking because each product typically performs detection of a somewhat different set of events using different methodologies. The following are factors that organisations should consider in their IDPS evaluations:

- Which types of activities it currently analyses fully and analyses partially, as well as future plans for additional analysis capabilities. Examples:

    - For network-based IDPS, a listing of the network, transport, and application layer protocols analysed, and an explanation of the amount of analysis performed on each (e.g., signature-based detection, anomaly-based detection, stateful protocol analysis)

    - For host-based IDPS, a listing of the specific resources that can be monitored (e.g., log files, system files, network interfaces) and an explanation of how each is monitored (e.g., after-the-fact detection of changes, active handling of file access requests, TCP/IP stack monitoring)

- What types of incidents it can identify, such as denial of service (DoS) attacks, backdoors, policy violations, port scans, malware (e.g., worms, Trojan horses, rootkits, malicious mobile code), and unauthorised application/protocol use.

- How comprehensive its detection is for each type of incident it can identify (e.g., how many worms, how many types of DoS attacks).

- How effective its default configuration is. When an IDPS is first deployed, its default settings should be reasonable. For example, signatures or policies that tend to generate large numbers of false positives should be disabled, and signatures or policies that are reliable and identify important recent attacks should be enabled. Detection thresholds (e.g., x instances in y minutes) should be set to values that attempt to balance false positives and false negatives. Also, features that are particularly resource-intensive should be disabled.

- How effective it is at detecting known malicious events, such as attacks, scans, or malware. Signature-based detection techniques typically perform better than anomaly detection and stateful protocol analysis techniques in recognising known events. This should include the IDPS's ability to state precisely which exploit was performed and which vulnerability was targeted (e.g., CVE reference identifier).

- How effective it is at detecting previously unknown malicious events, such as new attacks or variants on existing attacks, without reconfiguring or updating the IDPS. Anomaly detection and stateful protocol analysis techniques typically perform better than signature-based detection techniques in recognising unknown events.

- How effective it is at detecting known and unknown malicious events that have been concealed through evasion techniques. Examples of such techniques include unusual IP packet fragmentation, non-standard application port use, and alternate character sets or other character encoding.

- How accurately it can determine the success or failure of attacks.

- What response mechanisms it offers, excluding prevention responses. Examples are logging events (both locally and to remote log servers), displaying console alerts, and sending Simple Network Management Protocol (SNMP) traps, e-mails, text messages, and pages. The standard also includes effective prioritisation of events, such as taking different actions when a certain type of event occurs or when an event involves a certain system or service.

- How administrators can customise detection capabilities by modifying signatures, policies, and other settings. Examples include altering whitelists, blacklists, and thresholds; customising code to reduce false positives or false negatives; and writing new signatures or policies from scratch or based on samples or frameworks. Evaluators should consider how easily the customisations can be performed (e.g., through a GUI/console, through editing text files). If the customisations require knowledge of a programming language, additional considerations include the following:

    - Is the language commonly used or is it a specialty/proprietary language that administrators would need to learn?
    - How complex and powerful is the language?
    - Does the product offer a development environment or other tools to assist in customisation, such as syntax checking or virtual machines for testing customisations before implementing them?

- When the product is updated or upgraded, how are code customisations maintained?

- How effectively the product can use data from other sources, such as vulnerability scan results and logs from other IDPSs, to link events and improve the prioritisation of alerts.

9.2.4 Prevention Capabilities

Organisations should determine whether or not the IDPS solution may need to perform prevention actions, including future needs, and evaluate the prevention capabilities of each product that have been selected. Most prevention capabilities are specific to a particular type of IDPS. When available, it is generally preferred to have a product that has multiple prevention capabilities instead of only one, because some methods are more effective than others in certain situations and ineffective in others. All IDPS products should offer considerable granularity in configuration options for prevention methods, such as enabling or disabling them only for particular alerts, suppressing prevention methods for hosts on whitelists, and allowing administrators to specify which prevention method should be used for each alert if multiple methods are available. Some products offer additional granularity that may be beneficial, such as performing prevention actions only if a certain system is being attacked.

9.3 Performance Requirements

Comparing the performance of IDPS products is challenging for the following reasons:

- Performance is highly dependent on the configuration and tuning of each product. Although testing can be performed using the default settings of each product, some products are designed under the assumption that they will need extensive customisation and tuning.

- Performance and detection are often in conflict; having more complex and robust detection capabilities often causes poorer performance because they require more processing power and memory capacity.

- Many IDPSs are appliance-based and have many hardware models and configurations available, each with its own performance characteristics. Other IDPS components are not appliance-based, so their hardware, OSs, and OS configurations may vary widely, which can all affect performance.

- There are no open standards for performance testing, nor are there publicly available, comprehensive, up-to-date test suites.

Evaluators should thus focus on the general performance characteristics of IDPS products and avoid differentiating products by slight differences in reported performance capabilities. Vendors typically rate their products by maximum capacity, such as the volume of network traffic or number of packets per second monitored for network-based IDPS, the number of events monitored per second for host-based IDPS, or the flows monitored per second or the number of hosts that can be profiled for NBA systems. When evaluating maximum capacity claims, evaluators should consider the following questions:

- Does the maximum capacity reflect activity that is being analysed or activity that is being monitored but not necessarily analysed? For example, a network-based IDPS might perform little or no analysis on the use of certain application protocols.

- What was the nature of the activity used to measure capacity? This information can help evaluators to determine if the testing used an environment similar to their own or had significant differences that could affect performance results. Aspects of this to consider include the following:

    - How was the activity used for testing generated?
    - What types of malicious activity were included in the testing? What percentage of the events monitored by the IDPS was malicious? What percentage of the malicious events was detected by the IDPS under maximum load?
    - For network traffic, what protocols were used and in roughly what percentages? For host-based activity, what applications were run, and what other sources of events were used?

    - How closely did the activity used for testing reflect the actual conditions of the production environment?

- How was the IDPS configured? Was the default configuration used? If not, what detection capabilities, logging capabilities, and other features were enabled or disabled from the default?

- For any non-appliance components, what hardware, OSs, and applications or services were in use?

- Who performed the testing?

- When was the testing performed?

Evaluators should also consider the performance features that each IDPS under consideration offers. Possible considerations for performance features include the following:

- Does the IDPS offer any performance tuning features, either manually configured or automatically implemented? For example, if an IDPS is being overwhelmed by high volumes of activity, can it alter its detection capabilities so that it temporarily performs less extensive analysis on all the traffic or stops analysing low-risk traffic?

- For products that track state (e.g., stateful protocol analysis of network connections), how many activities (e.g., connections) can they track state for simultaneously? How long is state information maintained normally and under maximum load?

- For products that process the actual events, not copies of the events (e.g., inline network-based IDPS sensors), how much latency does the processing cause? For example, there might be a delay of 50 microseconds between when a network-based IDPS sensor receives a packet and when the IDPS retransmits that packet to continue to its destination. A host-based IDPS might delay the execution of system calls for a similarly short time. Under high loads, IDPS products might experience significantly higher latency, so it is important to consider latency under both typical and extreme loads.

- For products that process copies of events, not the actual events (e.g., passive network-based IDPS sensors, NBA software analysing network flow logs sent by routers), how long does it take from the occurrence of an event to the event's detection and reporting by the IDPS?

9.4 Management Requirements

Evaluating the management capabilities of each IDPS product is very important because if a product is difficult to manage or does not offer the necessary management functionality, then it is likely that the product will not be used as effectively as initially intended. This section presents IDPS management capability considerations in three categories:

- Design and implementation
- Operation and maintenance
- Training, documentation, and technical support.

9.4.1 Design and Implementation

Most aspects of IDPS design and implementation are specific to each IDPS technology type. Organisations should consider general criteria related to reliability, interoperability, scalability, and security.

9.4.1.1 Reliability

Organisations should ensure that the IDPS products they select will be sufficiently reliable to meet their requirements. Possible considerations for reliability are:

- What types of redundant hardware are included or available separately for appliances, such as duplicate power supplies, network interface cards, storage devices (e.g., hard drives, flash ROMs), and CPUs?

- What software redundancy features are incorporated into the products, especially for agents and sensors, such as the product automatically restarting itself and/or supporting services when they fail?

- Can the product use multiple management servers so that if one fails, sensors or agents automatically fail over to another one? How disruptive is the failover process?

- Can multiple sensors be deployed to monitor the same activity so that if one fails, another automatically assumes its responsibilities? How disruptive is the failover process (e.g., loss of state tracking, loss of event counts for thresholds)?

- If a sensor fails to operate, how easily can its configuration be transferred to another sensor (e.g., transferring a sensor CD and configuration floppy from the first sensor to the second sensor, then rebooting the second sensor)?

9.4.1.2 Interoperability

Organisations should ensure that the IDPS products they select will interoperate effectively with the desired systems. These systems could include the following:

- Data input sources, such as other IDPS products, log files, and vulnerability scanning results
- Log analysis and management software, such as syslog and other logging servers, SIEM software, and network management software
- Systems to be reconfigured by prevention actions, such as firewalls and routers.

9.4.1.3 Scalability

When evaluating IDPS products, organisations should consider not only their current needs, but also possible future needs, so that they choose products that are sufficiently scalable. Possible considerations for scalability include the following:

- The number of sensors or agents, management servers, consoles, and other IDPS components that can be part of a single logical implementation

- The number of sensors or agents that a single management server can support
- The range of appliances available for appliance-based IDPS components (e.g., appliance devices with varying capacities), and the ability to expand appliances (e.g., add more memory, network interface cards (NIC), or storage devices)

- How multiple sensors or agents can share monitoring functions for a network or system, including how load balancing can be performed with or without the use of separate load balancing devices

- How many networks a network-based, wireless, or NBA sensor can monitor simultaneously; how many network interfaces a host-based agent can monitor simultaneously

- How the IDPS's storage capabilities can be expanded and enhanced (e.g., automated archival of older data, use of separate storage devices)

- What levels of activity (e.g., network traffic, system calls, log entries) each of the IDPS components can support

- How well the IDPS solution integrates the management and monitoring of multiple sensors or agents, management servers, and other components

- The cost of and resources needed for each scalability option.

9.4.1.4 Security

When evaluating IDPS products, organisations should consider the security requirements for the IDPS solution itself. Examples of security considerations include the following:

- How stored data (including logs) and communications among all the IDPS components are protected, such as using alternate data channels or approved encryption and digital signature algorithms to support data confidentiality and integrity when needed

- The authentication, access control, and auditing features performed for IDPS usage and administration

- The IDPS's resistance to attacks against it, such as blinding and DoS attacks.

9.4.2 Operation and Maintenance

This criterion focuses on requirements for the user and administrator interfaces for ongoing management of the IDPS. This includes the ease of performing daily monitoring, analysis, and reporting activities; managing and maintaining the IDPS; and applying updates. Possible specific criteria for each of these areas are provided below. In addition, evaluators should consult with vendors, analysts, and/or trusted peers to determine the level of technical and security expertise needed to use and maintain each product. Evaluators should ask vendors what their assumptions are regarding the users and administrators of their products.

9.4.2.1 Daily Use

Organisations should consider how the IDPS solution needs to be used on a daily basis for monitoring security events, performing analysis of events of interest, and generating reports. Because these three activities are often intertwined, it is often easiest to assess them together. Daily use considerations for IDPSs should include the following:

- How it displays events and alerts to users, what features it provides to ease analysis (e.g., drill-down capability, links to supporting information, correlation of events from multiple sensors or agents, colour-coding alerts to indicate their severity/priority), and how users can customise the views and filters to alter the display of events and alerts

- How it displays its status information to users and administrators (e.g., how a sensor failure is communicated)

- How it notifies users and administrators of both serious security events and IDPS failures and other operational problems

- How much supporting information it records for events (e.g., is enough information recorded to allow analysts to determine what happened?)

- How many interfaces/programs are needed for the daily use functions (e.g., can a single GUI provide all the functions that the IDPS users need?)

- How many concurrent interfaces are supported

- What default report formats are offered (e.g., text, comma-separated values (CSV), HTML, Extensible Markup Language (XML), PDF, Microsoft Word, Microsoft Excel) and what data storage formats are supported for IDPS data, log, and report retention

- How reports can be customised (both altering existing reports and creating new reports)

- Whether or not reports can be generated automatically (e.g., on a schedule, when certain events occur), how the reports can be distributed (e.g., e-mailed to administrators), and how the distributed reports are protected (e.g., file encryption)

- Whether or not it offers any workflow tracking capabilities, such as incident tracking.

9.4.2.2 Maintenance

Organisations should consider how the IDPS solution and its components should be maintained, and then evaluate products based on those maintenance requirements. Maintenance considerations should include the following:

- Whether or not sensors or agents can be managed both independently and through a management server, and whether such accesses are logged

- What local and remote maintenance mechanisms are available (e.g., locally installed GUI, Web-based console, command-line interface, third-party tools), and what differences there are (if any) in their functionality

- Which components can be maintained locally and remotely with each maintenance mechanism

- What security protections are provided for each maintenance mechanism (e.g., strong encryption for network traffic)

- How component configuration settings can be backed up and restored, and how they can be transferred from a component to a replacement component (e.g., swapping sensor appliances because of hardware failure)

- How robust the product is at logging component status information (e.g., low disk space, high CPU utilisation), operational failures, and other events that may necessitate maintenance actions

- Whether or not the IDPS provides sufficiently robust log management tools, and if not, how administrators could compensate (e.g., write scripts, acquire third-party tools).

9.4.2.3 Updates

Organisations should carefully consider how the vendor of each evaluated IDPS product releases updates for it. Aspects of this to consider include the following:

- How often regular major and minor updates to each component are released (e.g., sensors, management servers, consoles)

- How often updates to detection capabilities are released in response to major new threats, and how soon after the identification of a new threat the corresponding update is typically available

- Which types of updates usually or sometimes require that IDPS components be rebooted or restarted

- How the organisation receives each type of update from the vendor (e.g., sensor upgrade distributed on CD, signature updates available for download through the console or from the vendor's technical support website)

- How the authenticity and integrity of updates can be confirmed (e.g., through cryptographic checksums)

- How updates can be distributed to IDPS components such as sensors and consoles (e.g., automated process, manual installation)

- How the installation of updates can affect existing IDPS settings or customisations.

9.4.3 Training, Documentation, and Technical Support

Organisations should consider the resources available to the IDPS administrators and users for learning about the IDPS's functionality and characteristics and for receiving assistance when problems occur. These resources - training, documentation, and technical support should take into account both administrator and user needs, as well as different experience levels.

- **Training**

  Most IDPS vendors offer training courses for their products. Some offer a single course per product, while others offer separate courses for users and administrators. Separate courses may also be available for particular IDPS components, such as consoles or management servers, or for specialised tasks such as code customisation or report creation. Some vendors also offer general IDPS courses that are intended to give users a better understanding of IDPS principles. Third parties also offer general IDPS courses and courses for some specific IDPS products. Organisations should consider which training courses are available that meet their needs, what format the courses are in (e.g., instructor-led, online, computer-based training (CBT)), and where the classes are held (e.g., the IDPS vendor's headquarters, regional locations, the customer's site). For instructor-led classes, organisations should determine if they include lab work or other hands-on exercises that allow users to use the actual IDPS equipment.

- **Documentation**

  IDPS products usually include documentation in paper or electronic forms. Examples include installation, user, administrator, and signature/policy development mnu. Electronic guides are often fully searchable; some products also offer context-sensitive help through the console, allowing a user to easily access the relevant documentation for a particular console feature or security event type. If guides are

provided on paper only, organisations should determine if the guides can be copies, and if not, what the availability of additional copies is.

- **Technical Support**

  Most IDPS vendors offer multiple technical support contracts. For example, one contract might provide basic phone, e-mail, and Web-based support during business hours with a one-hour response time, while another contract might provide 24-hour access to senior support staff with a 15-minute response time and include annual onsite visits and consulting services. Organisations should take care to determine what activities are and are not covered by a contract; for example, tuning and customisation, such as writing signatures or customising reports, might not be included. Vendors typically provide multiple support contract options so that each customer can select one that is cost-effective for them. Free technical support is also available for some products through user groups, mailing lists, forums, and other methods.

9.5 Life Cycle Costs

Organisations should compare the funding they have available for IDPS solutions to the estimated life cycle costs for each of the evaluated solutions. Quantifying the life cycle costs for IDPS solutions can be difficult because there are many environment-specific factors that impact cost, and because it is usually challenging to capture the cost benefits provided by IDPSs. The criteria presented below focus on the basic costs of the IDPS solution itself and do not take into account any cost savings achieved by IDPS use.

- **Initial Costs**

  The initial costs of acquiring and deploying a solution typically include the following:

  - Hardware, including appliances, additional network equipment (e.g., management network, network taps, IDS load balancers), and hosts for non-appliance components (e.g., consoles)
  - Software and software licensing fees for IDPS components and supporting software (e.g., reporting tools, database software)
  - Installation and initial configuration costs, which could include external assistance as well as internal labour

- Customisation costs, such as having programmers develop custom scripts or reports
- Training costs, if the necessary training is not included as part of the initial hardware and software purchase.

- **Maintenance Costs**

  Expected maintenance costs for IDPS solutions typically include the following:
  - Labour. This includes the cost of staff performing IDPS administration and analysis.
  - Software licensing fees, subscription fees, or maintenance contracts. These costs, typically incurred on an annual basis, usually provide the purchaser with IDPS software and signature updates.
  - Technical support fees. Many organisations purchase technical support contracts for their IDPS products; these contracts are typically annual. Some organisations pay a fee per technical support call instead of an annual contract.
  - Training costs. Training might be needed periodically in preparation for deploying new versions of an IDPS product, as well as for new IDPS users and administrators. Organisations might want to have customised training classes that focus on the elements of the IDPS product that are most important to the organisation, and also take into account certain aspects of the organisation's environment and needs.
  - Customisation costs. During the use of an IDPS product, users and administrators might need the product to be further customised, such as having programmers develop additional custom reports or modify existing reports, and having programmers or administrators create custom analysers and signatures.
  - Professional services or technical support that falls outside the technical support contract. Examples include designing IDPS implementations, performing product installations, tuning sensors or agents, creating and customising reports, and assisting with incident response efforts. Organisations can perform these services themselves, or they can purchase services from IDPS vendors and third parties.

9.6 Evaluating Products

After collecting requirements and selecting criteria, evaluators need to find sources of information about the products to be evaluated. Common product data sources include the following:

Test lab or real-world environment testing of selected IDPS products

- Previous real-world experience with IDPSs from individuals within the organisation and trusted individuals at other organisations
- Vendor-provided information, such as product manuals and datasheets, whitepapers, product demonstrations, and discussions with vendor employees
- Third-party product reviews, including reviews of individual products and comparisons of multiple products.

9.6.1 IDPS Testing Challenges

An organisation performing its own in-depth hands-on testing of IDPS products ideally could generate comprehensive data on the products that would accurately reflect how tailored each product is to meeting the organisation's needs. However, this is normally not feasible to achieve because of how difficult and resource-intensive it is to perform IDPS testing well. The following are some of the major reasons for these problems:

- **Test Methodology**

  There is no standard methodology for performing IDPS testing. Also, details are not available for most of the methodologies used for commercial evaluation of IDPS products. Organisations performing IDPS testing have to create their own methodologies or perform a survey of existing methodologies, determine which would be best for their needs and then design and implement testing processes using the selected methodology. Besides, a different methodology, including test environments and test suites, is required for each type of IDPS technology.

- **Multiple Environments**

  Organisations performing IDPS testing should conduct it in both real-world and lab environments. The real-world testing helps evaluators to understand how well the product will likely function in their environment. The lab testing allows evaluators to better assess the detection and prevention capabilities of the product. Detection results

can be difficult to understand when real-world activity is being monitored because the real-world activity is likely to contain different types of malicious activity, and it is sometimes unclear whether or not the detected activity was in reality malicious. Prevention capabilities are generally not tested in real-world environments because they can easily cause disruptions to harmless activity. It is very difficult to duplicate real-world environments in lab environments, so organisations performing IDPS testing generally need to do their testing separately in each environment.

- **Test Availability**

  There are no standard IDPS test suites available. Organisations performing IDPS testing need to find ways to generate both malicious activity (to see how well the products identify them) and harmless activity (to put the product under normal or heavy loads). The malicious activity should accurately reflect the composition of recent threats against the organisation's systems and networks; accordingly, it can take considerable time to identify those threats and acquire tests for them. The tests also need to take into account all detection methodologies used by the IDPSs, because usually different types of tests are needed to properly evaluate the effectiveness of each methodology. Typically it takes a combination of carefully selected tools and custom-written attack scripts to build a reasonable test suite. Each tool and script should be reviewed and tested to ensure that it performs the tests properly.

- **Lab Environment Resources**

  Organisations performing IDPS testing in lab environments typically need to expend considerable resources in setting up the lab environments. Attacker and victim systems need to be set up and configured. The victim systems need to run the OSs, services, and applications targeted by the attacks. Depending on the methodologies used by the IDPSs, the victim systems may need to have all the vulnerabilities exploited by the attacks. Some IDPSs might alert only on attacks that they think will be successful; also, some attacks will stop executing if they do not detect exploitable vulnerabilities. Evaluators also need to be aware of the capabilities of the IDPSs; for example, an IDPS might see a few attacks from a single attacker system and automatically perform prevention actions to stop all future attacks from that system.

- **Product Equivalence**

Most IDPS products need to be tuned and customised to meet the requirements of the organisation. Each product is configured rather differently by default, so organisations performing IDPS testing should attempt to tune and customise the products so that they are as similar as possible. For example, thresholds such as the number of failed login attempts permitted in a certain time period should be set to the same values. Also, each detection feature should be enabled or disabled consistently on all the IDPSs. This is often very difficult to accomplish. For example, a product performing signature-based detection tends to have settings based on specific exploits being performed, while a product performing stateful protocol analysis detection often has settings based on specific vulnerabilities being exploited. Evaluators would need to map the exploits and vulnerabilities to determine the equivalent settings on different IDPSs.

9.6.2 Recommendations for Performing IDPS Evaluations

The challenges in performing in-depth hands-on IDPS testing often make it infeasible; however, performing some amount of IDPS testing is generally quite helpful in evaluating how well IDPSs meet an organisation's requirements for security capabilities, performance, and operation and maintenance. IDPS testing is also helpful in setting realistic expectations for the capabilities of the products and the amount of labour required to maintain and monitor them in the organisation's environment. Accordingly, organisations should consider using a combination of several data sources, such as limited product testing, vendor-provided information, third-party product reviews, and individuals' previous IDPS experience, when performing IDPS product evaluations. For example, organisations could use data sources other than product testing to narrow the product selection to only a few choices, and then perform limited testing of those choices only. In some cases, omitting product testing and performing a paper-only evaluation of a product is necessary because of time and resource constraints, but generally an evaluation will produce better results if it incorporates at least some product testing.

When using data from other parties, organisations should consider the integrity of the data. Data is often presented without a detailed explanation of how it was created, such as maximum capacities or detection accuracy rates. Because there are no standard methodologies for compiling such data, organisations should be cautious when comparing

data from different sources, because the measurements may have been performed using fundamentally different methods.

When performing hands-on IDPS testing, organisations should focus on those testing methods that are most likely to be valuable. Testers should also avoid disrupting the organisation's operations. The following provides guidance on performing testing for each class of IDPS product. After testing has been completed, testers should ensure that any hardware on loan from IDPS vendors has its writable media sanitised appropriately to remove the organisation's data.

9.6.2.1 Network-Based IDPSs

Valuable insights into network-based IDPS security capabilities (especially detection accuracy and tuning), performance with the organisation's network traffic, and the operation and maintenance of the IDPS can be gained by performing real-world testing of the IDPS. However, it is generally prudent to keep the IDPS somewhat separate from the production environment during this testing so that the IDPS does not adversely affect it (e.g., increase latency) and so that any vulnerabilities in the IDPS cannot be exploited by attackers. An IDS load balancer is ideal for giving multiple sensors identical copies of the network traffic simultaneously, allowing for side-by-side comparisons of the products, while isolating the sensors and preventing them from inadvertently disrupting production (traffic passes through a load balancer in only one direction). Depending on the network architecture, it may be possible to test sensors in inline deployments by duplicating traffic at the network locations where each of an inline sensor's network interfaces would be and feeding that traffic to the inline sensors' interfaces. Otherwise, most inline sensors can be placed into a passive mode and tested as passive; the benefit of testing them with production traffic in inline mode is to study their performance.

Lab testing of network-based IDPSs is most advantageous for the evaluation of the following:

- **The prevention capabilities of products**
  Testers can set up test systems (targets and attacking systems), generate attacks, and monitor the effectiveness of each IDPS's prevention actions.

- **The performance of inline sensor deployments**

If this cannot be done as part of real-world testing, testers could use network traffic generation tools or replay previously recorded traffic to generate activity to pass through the sensor.

- **Design and implementation-related characteristics**

  Product reliability could be tested by deploying multiple sensors or management servers, configuring them for failover conditions, generating traffic for them to process, and then intentionally causing a failure of one component and monitoring the resulting product behaviour. Interoperability could be tested by configuring test systems representing the products with which the IDPS must interoperate, and then generating activity that should cause the products to work together. The security of the IDPS itself can also be tested through vulnerability scanning, penetration testing, and other methods.

9.6.2.2 Wireless IDPSs

The methods to be used for testing wireless IDPSs should be selected primarily by the format of the wireless IDPS sensors to be tested:

- **Mobile sensors, fixed sensors, and sensors packaged with Access Points**

  Testing of security capabilities, performance, and some components of operation and maintenance can typically be performed by using the sensors in production environments, with the caveat that prevention capabilities should be disabled. Prevention capabilities could be evaluated in an isolated test environment that is out of range of all other wireless local area networks. This test environment would contain test access points and test wireless clients using the access points; testers might need to set up test systems that the wireless clients can access to generate wireless network communications. Attacks can be issued from one or more wireless clients, and rogue access points can be deployed in the test environment. If the sensors will be integrated with an IDPS infrastructure, any testing of this should also be performed in the test environment to evaluate performance, operation and maintenance, and design and implementation characteristics without jeopardising the production infrastructure (e.g., an IDPS sensor could have vulnerabilities that could be exploited by attackers within range of the sensor).

- **Sensors bundled with wireless switches**

  Generally, this testing should be performed by setting up a test switch with sensor software in a test environment like the one described above for other types of wireless sensors. The same type of testing described above should be performed.

9.6.2.3 Network-Behaviour Analysis IDPSs

If the NBA IDPSs will be directly monitoring network traffic, then real-world and lab testing of that capability should be performed based on the guidance given for testing network-based products. If the NBA products will be monitoring network flow logs from other devices, the preferred method for real-world testing of that capability is to set up a separate network and forward the logs from the devices over that network to the NBA sensors. This protects the NBA solution and allows the bandwidth used by the solution to be measured easily. If the production networks will be used instead of a separate network, testers need to be very cautious not to overload the production networks with the volume of logs, particularly if multiple NBA products are being tested simultaneously. Testing can also be performed in a lab environment by providing copies of production logs to the NBA products. NBA product lab testing is also beneficial for the same reasons mentioned for network-based IDPS lab testing - evaluating prevention capabilities, inline sensor performance, and product design and implementation-related characteristics.

9.6.2.4 Host-Based IDPSs

Host-based IDPSs are typically more challenging to perform real-world testing for than any other type of IDPS. Agents alter the hosts that they monitor and can negatively affect their performance and functionality (e.g., IDPS compatibility applications interfering with other applications); appliance-based IDPSs are deployed inline in front of production systems. The methods to be used for testing host-based IDPSs should be selected primarily by the roles of the hosts to be protected.

- **A server (including a single application service on a server)**

  Testing should be performed in a test environment only. For example, a test server could be created that mimics a production server or even uses one of its backups. Typical activity directed at the server, both benign and malicious, should be generated by test systems (e.g., scripts or tools to create HTTP requests) and monitored by the host-based IDPS. Testers can perform attacks against the server and monitor the prevention actions performed without endangering any production systems. Testers

can also measure the impact of the host-based IDPS on the performance of the server and evaluate the reliability and security of the host-based IDPS by attempting to disrupt it.

- **A client host (desktop or laptop)**

  Initial testing should be performed in a test environment to identify major performance and functionality problems that host-based IDPSs might introduce. The reliability and security of the IDPS can also be evaluated in a test environment. Testing of agents' security capabilities, prevention actions, and other characteristics can be conducted in both a test environment and a production environment because the risk posed by IDPS failure to the production environment is very low. Attacks should only be issued against the hosts in a test environment, while the agents' behaviour against benign activity can be tested most easily in a real-world environment. For example, a few of the testers might volunteer to have IDPS agents installed on their production desktops and document the agents' behaviour and any problems they cause for a week or two. This provides true real-world testing of the agents. For agents that require user interaction, such as responding to queries about permitting or denying activity, conducting end user testing in a test or production environment is also prudent.

  When testing host-based IDPSs, organisations should test the most commonly used and important OSs and applications that need to be protected. The architecture of each OS and each application is different, so a single product might exhibit significantly different behaviour when used on different platforms.

6.0 Conclusion

IDPS are suitable for monitoring and analysing traffic in information systems and networks and are prospective tools that help identify and prevent disruptive incidents. However, before evaluating IDPS products, organisations should first define the general requirements that the products should meet. Then, evaluators should communicate the goals and objectives they wish to achieve by using an IDPS. Evaluators should also review their existing security and other IT policies before selecting products. Finally they should test the products either in test labs or real-world environments in order to rate their efficiency.

7.0 References

- Dean De Beer | Zero(day)solutions, Implementation Standards for Intrusion Detection/Prevention Systems,
- State of Vermont , Intrusion Detection and Prevention Policy
- Wikipedia: http://en.wikipedia.org
- Information Technology Labouratory Bulletin, Advising users on Information Technology, Intrusion Detection And Prevention Systems
- National Institute of Standard and Technology: Guide to Intrusion Detection and Prevention Systems (IDPS)

Appendix A

List of Acronyms

CBT	Computer Based Training
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposure
CSV	Comma-Separated Values
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IPS	Intrusion Prevention System
NBA	Network-Behaviour Analysis
NIC	Network Interface Card
OS	Operating System
SIEM	Security Information and Event Management
TLS	Transport Layer Security
VPN	Virtual Private Network
XML	Extensible Markup Language