COURSE TECHNOLOGY
CENGAGE Learning™

Principles of Information Security, Fifth Edition

Chapter 7
Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools

Do not wait; the time will never be just right. Start where you stand and work with whatever tools you may have at your command, and better tools will be found as you go along.

NAPOLEON HILL (1883–1970) FOUNDER OF THE SCIENCE of SUCCESS

Learning Objectives

- Upon completion of this material, you should be able to:
  - Identify and describe the categories and models of intrusion detection and prevention systems
  - Describe the detection approaches employed by modern intrusion detection and prevention systems
  - Define and describe honeypots, honeynets, and padded cell systems
  - List and define the major categories of scanning and analysis tools, and describe the specific tools used within each category

Introduction

- Protection of organizations assets relies as much on managerial controls as on technical safeguards.
- Properly implemented technical solutions guided by policy are essential to an information security program.
- Advanced technologies can be used to enhance the security of information assets.

Intrusion Detection and Prevention Systems

- An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an organization's information systems.
- Intrusion prevention consists of activities that deter an intrusion.
- Intrusion detection consists of procedures and systems that identify system intrusions.
- Intrusion reaction encompasses actions an organization undertakes when intrusion event is detected.

Intrusion Detection and Prevention Systems (cont'd)

- Intrusion correction activities: complete restoration of operations to a normal state and seek to identify source and method of intrusion
- Intrusion detection systems detect a violation of its configuration and activate alarm.
- Many IDPSs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers.
- Systems can also be configured to notify an external security service organization of a "break-in."

IDPS Terminology

- Alarm clustering and compaction
- Alarm filtering
- Alert or alarm
- Confidence value
- Evasion
- False attack stimulus
- False negative and false positive
- Noise
- Site policy
- Site policy awareness
- True attack stimulus
- Tuning

Why Use an IDPS?

- Intrusion detection:
  - Primary purpose to identify and report an intrusion
  - Can quickly contain attack and prevent/mitigate loss or damage
  - Detect and deal with preambles to attacks
- Data collection allows the organization to examine what happened after an intrusion and why.
- Serves as a deterrent by increasing the fear of detection
- Can help management with quality assurance and continuous improvement

Types of IDPSs

- IDPSs operate as network-based or host-based systems.
- Network-based IDPS is focused on protecting network information assets.
  - Wireless IDPS: focuses on wireless networks
  - Network behavior analysis IDPS: examines traffic flow on a network in an attempt to recognize abnormal patterns

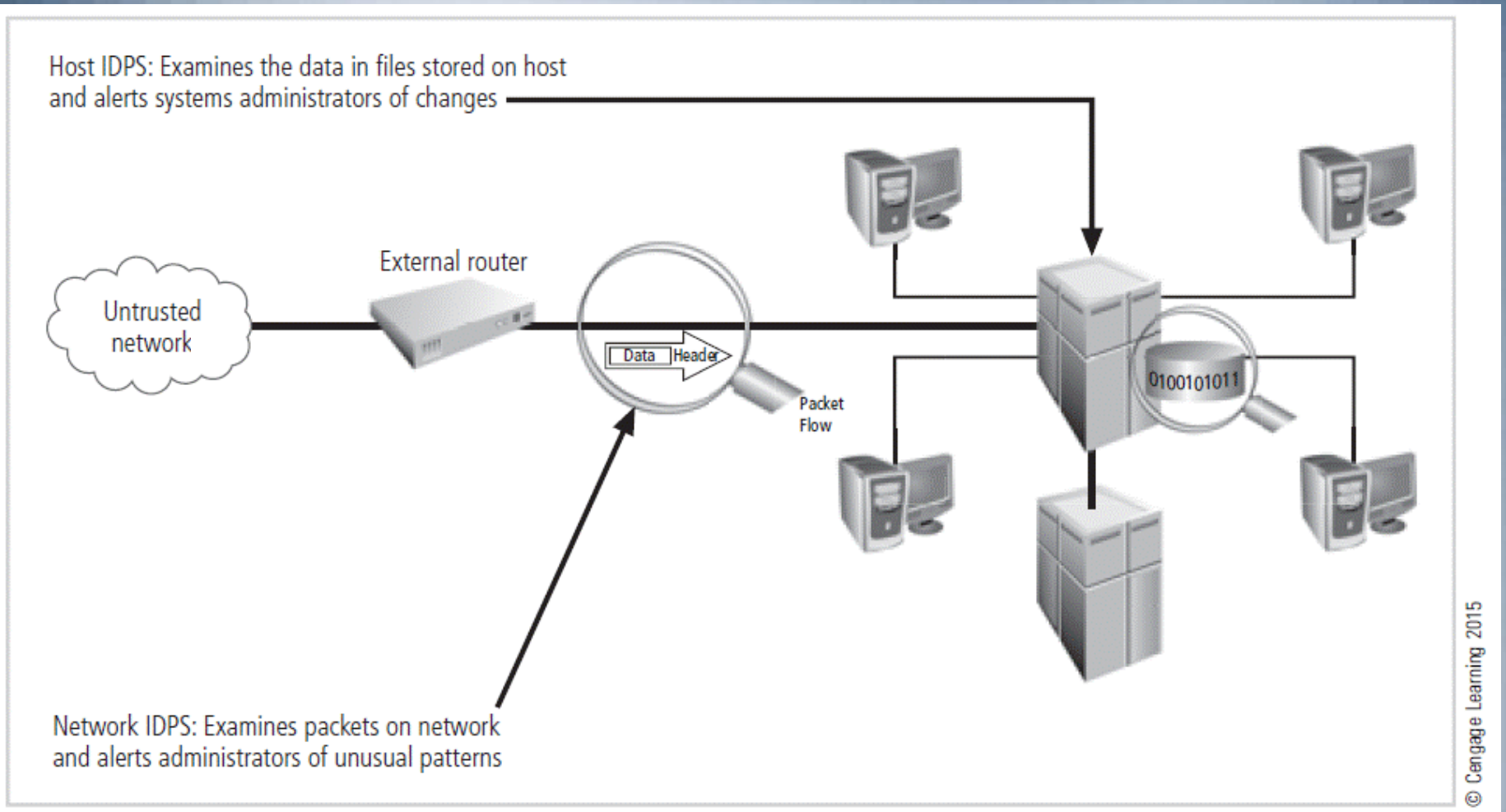

Figure 7-1 Intrusion detection and prevention systems

Types of IDPSs (cont'd)

- Network-based IDPS (NIDPS)
  - Resides on a computer or an appliance connected to a segment of an organization's network; looks for indications of attacks
  - When examining packets, a NIDPS looks for attack patterns within network traffic
  - Installed at specific place in the network where it can monitor traffic going into and out of a particular network segment

Types of IDPSs (cont'd)

- Network-based IDPS (NIDPS) (cont'd)
  - To determine whether attack has occurred/is under way, compare measured activity to known signatures in knowledge base
  - Done by using special implementation of TCP/IP stack:
    - In the process of protocol stack verification, NIDPSs look for invalid data packets.
    - In the application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use.

Types of IDPSs (cont'd)

- Advantages of NIDPSs
  - Good network design and placement of NIDPS can enable an organization to monitor a large network with few devices.
  - NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations.
  - NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers.

Types of IDPSs (cont'd)

- Disadvantages of NIDPSs
  - Can become overwhelmed by network volume and fail to recognize attacks
  - Require access to all traffic to be monitored
  - Cannot analyze encrypted packets
  - Cannot reliably ascertain if attack was successful or not
  - Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets.

Types of IDPSs (cont'd)

- Wireless NIDPS
  - Monitors and analyzes wireless network traffic
  - Issues associated with it include physical security, sensor range, access point and wireless switch locations, wired network connections, cost, AP and wireless switch locations.
- Network behavior analysis systems
  - Identify problems related to the flow of traffic
  - Types of events commonly detected include denial-of-service (DoS) attacks, scanning, worms, unexpected application services, and policy violations.
  - Offer intrusion prevention capabilities that are passive, inline, and both passive and inline

Types of IDPSs (cont'd)

- Host-based IDPS (HIDPS)
  - Resides on a particular computer or server (host) and monitors activity only on that system
  - Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files
  - Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks
  - Most HIDPSs work on the principle of configuration or change management.

Types of IDPSs (cont'd)

- Advantages of HIDPSs
  - Can detect local events on host systems and detect attacks that may elude a network-based IDPS
  - Functions on host system, where encrypted traffic will have been decrypted and is available for processing
  - Not affected by use of switched network protocols
  - Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Types of IDPSs (cont'd)

- Disadvantages of HIDPSs
  - Pose more management issues
  - Vulnerable both to direct attacks and attacks against host operating system
  - Does not detect multihost scanning, nor scanning of non-host network devices
  - Susceptible to some DoS attacks
  - Can use large amounts of disk space
  - Can inflict a performance overhead on its host systems

IDPS Detection Methods

- Signature-based detection
  - Examines network traffic in search of patterns that match known signatures
  - Widely used because many attacks have clear and distinct signatures
  - Problem with this approach is that new attack patterns must continually be added to IDPS's database of signatures.
    - Slow, methodical attack involving multiple events might escape detection.

IDPS Detection Methods (cont'd)

- Anomaly-based detection
  - Anomaly-based detection (or behavior-based detection) collects statistical summaries by observing traffic known to be normal.
  - When measured activity is outside baseline parameters or clipping level, IDPS sends alert to administrator.
  - IDPS can detect new types of attacks.
  - Requires much more overhead and processing capacity than signature-based detection
  - May generate many false positives

IDPS Detection Methods (cont'd)

- Stateful protocol analysis
  - SPA: process of comparing known normal/benign protocol profiles against observed traffic
  - Stores and uses relevant data detected in a session to identify intrusions involving multiple requests /responses; allows IDPS to better detect specialized, multisession attacks (also called deep packet inspection)
  - Drawbacks: analytical complexity; heavy processing overhead; may fail to detect intrusion unless protocol violates fundamental behavior; may interfere with normal operations of protocol

IDPS Detection Methods (cont'd)

- Log file monitors
  - Log file monitor (LFM) similar to NIDPS
  - Reviews log files generated by servers, network devices, and even other IDPSs for patterns and signatures
  - Patterns that signify attack may be much easier to identify when entire network and its systems are viewed as a whole
  - Requires considerable resources since it involves the collection, movement, storage, and analysis of large quantities of log data

IDPS Response Behavior

- IDPS response to external stimulation depends on the configuration and function; many response options are available.
- IDPS responses can be classified as active or passive.
  - Active response: collecting additional information about the intrusion, modifying the network environment, taking action against the intrusion
  - Passive response: setting off alarms or notifications, collecting passive data through SNMP traps
- Many IDPSs can generate routine reports and other detailed documents.
- Failsafe features protect IDPS from being circumvented.

Selecting IDPS Approaches and Products

- Technical and policy considerations
  - What is your systems environment?
  - What are your security goals and objectives?
  - What is your existing security policy?
- Organizational requirements and constraints
  - What requirements are levied from outside the organization?
  - What are your organization's resource constraints?

Selecting IDPS Approaches and Products (cont'd)

- IDPSs product features and quality
  - Is the product sufficiently scalable for your environment?
  - How has the product been tested?
  - What user level of expertise is targeted by the product?
  - Is the product designed to evolve as the organization grows?
  - What are the support provisions for the product?

Strengths and Limitations of IDPSs

- IDPSs perform the following functions well:
  - Monitoring and analysis of system events and user behaviors
  - Testing security states of system configurations
  - Baselining security state of system and tracking changes
  - Recognizing patterns of system events corresponding to known attacks
  - Recognizing activity patterns that vary from normal activity

Strengths and Limitations of IDPSs (cont'd)

- IDPSs perform the following functions well: (cont'd)
  - Managing OS audit and logging mechanisms and data they generate
  - Alerting appropriate staff when attacks are detected
  - Measuring enforcement of security policies encoded in analysis engine
  - Providing default information on security policies
  - Allowing non-security experts to perform important security monitoring functions

Strengths and Limitations of IDPSs (cont'd)

- IDPSs cannot perform the following functions:
  - Compensating for weak/missing security mechanisms in protection infrastructure
  - Instantaneously detecting, reporting, responding to attack when there is heavy network or processing load
  - Detecting new attacks or variants of existing attacks
  - Effectively responding to attacks by sophisticated attackers
  - Automatically investigating attacks without human intervention

Strengths and Limitations of IDPSs (cont'd)

- IDPSs cannot perform the following functions (cont'd):
  - Resisting attacks intended to defeat or circumvent them
  - Compensating for problems with fidelity of information sources
  - Dealing effectively with switched networks

Deployment and Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies:
  - Centralized: All IDPS control functions are implemented and managed in a central location.
  - Fully distributed: All control functions are applied at the physical location of each IDPS component.
  - Partially distributed: Combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks.

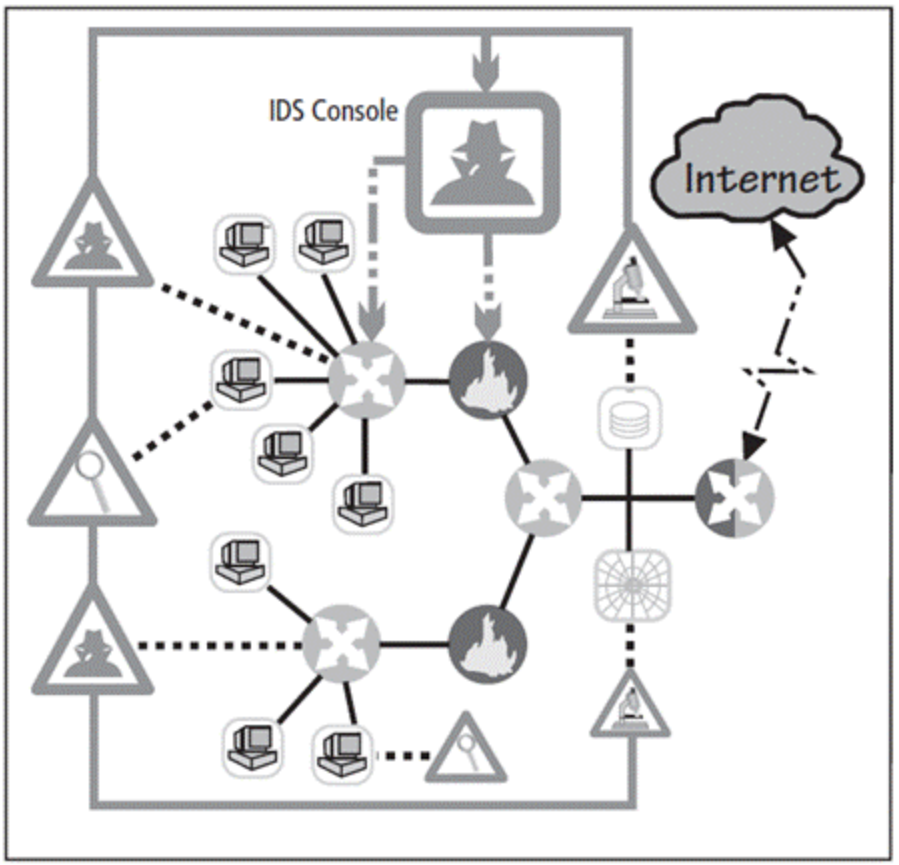

Figure 7-4 Centralized IDPS control[20]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

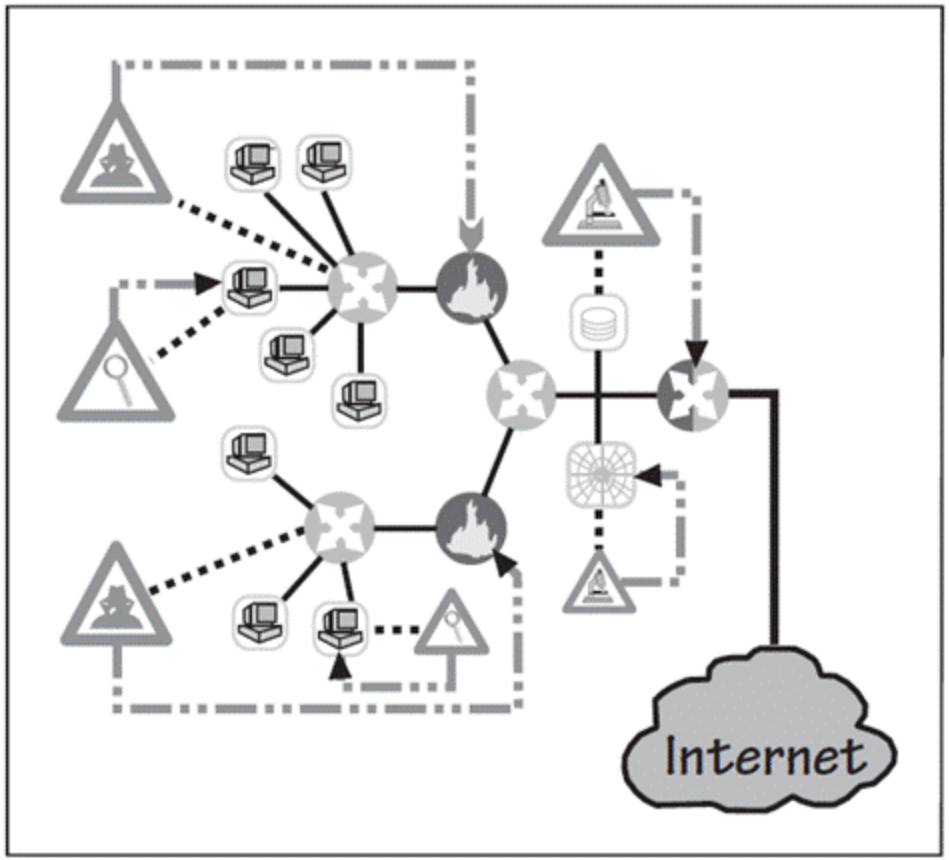

Figure 7-5 Fully distributed IDPS control[21]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

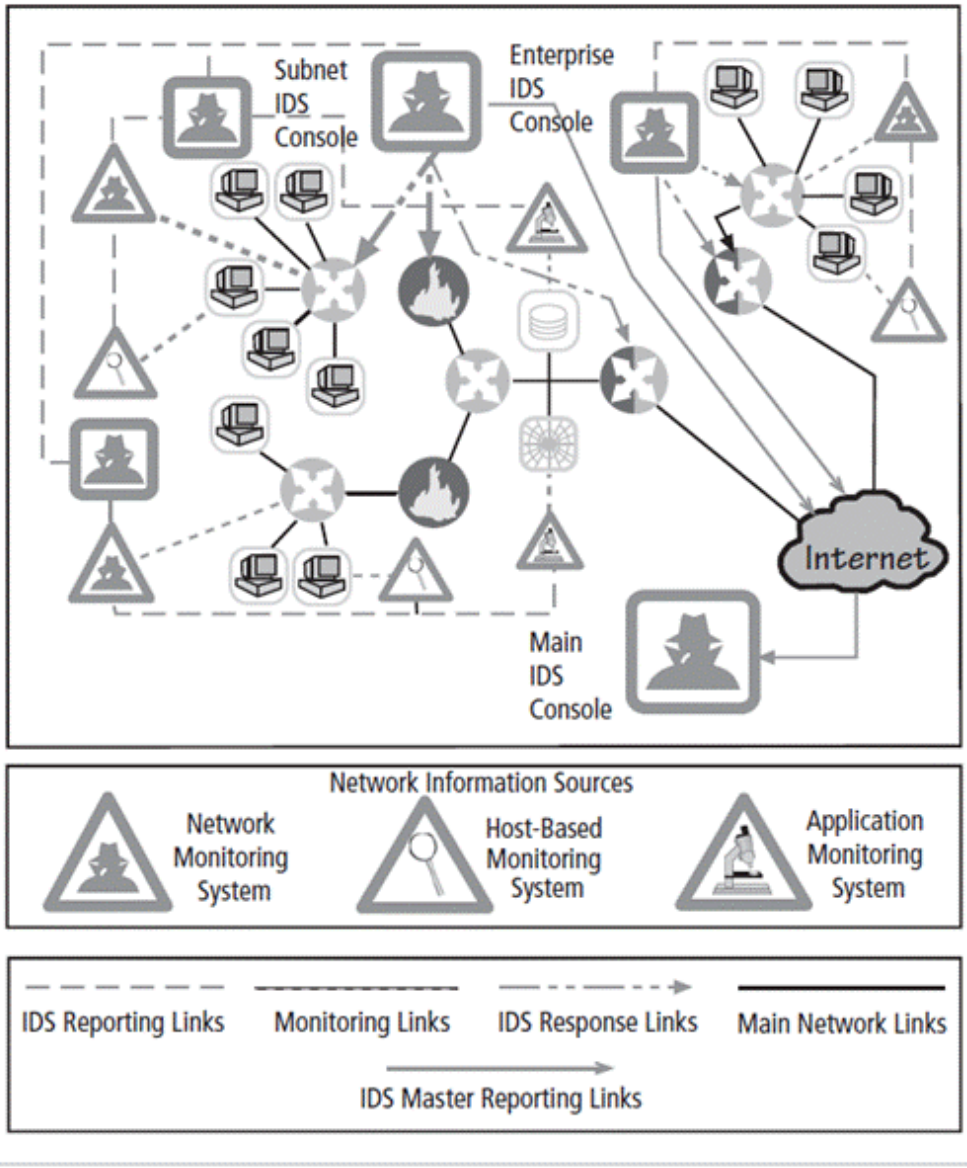

Figure 7-6 Partially distributed IDPS control[22]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Deployment and Implementation of an IDPS (cont'd)

- IDPS deployment
  - Great care must be taken when deciding where to locate components.
  - Planners must select deployment strategy that is based on careful analysis of organization's information security requirements and causes minimal impact.
  - NIDPS and HIDPS can be used in tandem to cover individual systems that connect to an organization's network and networks themselves.

Deployment and Implementation of an IDPS (cont'd)

- Deploying network-based IDPSs
  - NIST recommends four locations for NIDPS sensors
    - Location 1: Behind each external firewall, in the network DMZ
    - Location 2: Outside an external firewall
    - Location 3: On major network backbones
    - Location 4: On critical subnets

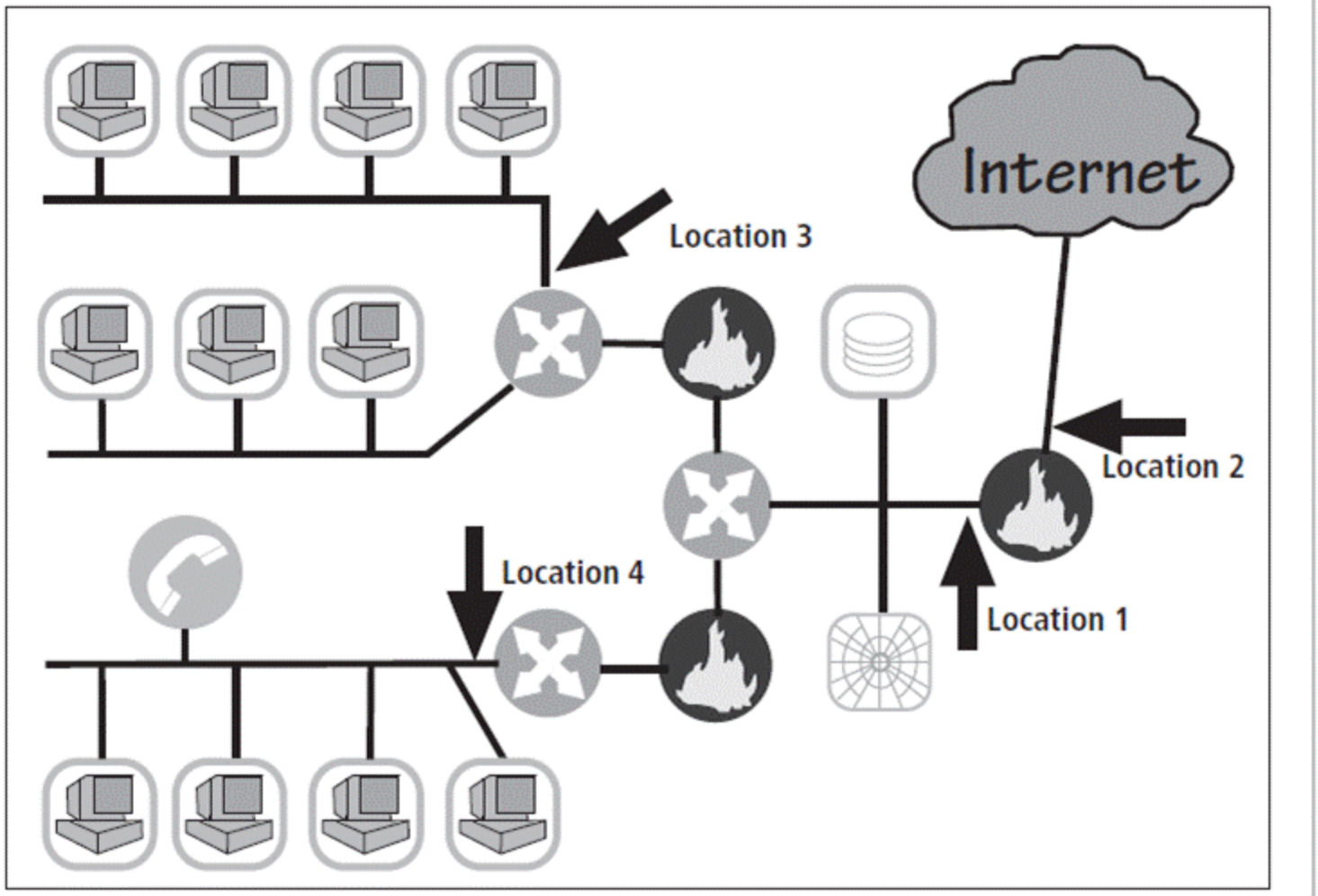

Figure 7-7 Network IDPS sensor locations[23]

Source: Adapted from Scarfone and Mell, NIST SP 800-94.

Deployment and Implementation of an IDPS (cont'd)

- Deploying host-based IDPSs
  - Proper implementation of HIDPSs can be a painstaking and time-consuming task.
  - Deployment begins with implementing most critical systems first.
  - Installation continues until either all systems are installed or the organization reaches planned degree of coverage it will accept.

Measuring the Effectiveness of IDPSs

- IDPSs are evaluated using four dominant metrics: thresholds, blacklists and whitelists, alert settings, and code viewing and editing.
- Evaluation of IDPS might read: At 100 Mb/s, IDPS was able to detect 97 percent of directed attacks.
- Because developing this collection can be tedious, most IDPS vendors provide testing mechanisms to verify systems are performing as expected.

Measuring the Effectiveness of IDPSs (cont'd)

- Some of these testing processes will enable the administrator to:
  - Record and retransmit packets from real virus or worm scan
  - Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
  - Conduct a real virus or worm scan against a hardened or sacrificial system
- Testing process should be as realistic as possible.

Honeypots, Honeynets, and Padded Cell Systems

- Honeypots: decoy systems designed to lure potential attackers away from critical systems
- Honeynets: several honeypots connected together on a network segment
- Honeypots are designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on a system long enough for administrators to document the event and perhaps respond

Honeypots, Honeynets, and Padded Cell Systems (cont'd)

- Padded cell system: protected honeypot that cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS.
- When the IDPS detects attackers, padded cell system seamlessly transfers them to a special simulated environment where they can cause no harm—hence the name *padded cell.*

Honeypots, Honeynets, and Padded Cell Systems (cont'd)

- Advantages
  - Attackers can be diverted to targets they cannot damage.
  - Administrators have time to decide how to respond to an attacker.
  - Attackers' actions can be easily and more extensively monitored, and records can be used to refine threat models and improve system protections.
  - Honeypots may be effective at catching insiders who are snooping around a network.

Honeypots, Honeynets, and Padded Cell Systems (cont'd)

- Disadvantages
  - Legal implications of using such devices are not well understood.
  - Honeypots and padded cells have not yet been shown to be generally useful security technologies.
  - An expert attacker, once diverted into a decoy system, may become angry and launch a more aggressive attack against an organization's systems.
  - Administrators and security managers need a high level of expertise to use these systems.

Trap-and-Trace Systems

- Use a combination of techniques to detect an intrusion and trace it back to its source
- Trap usually consists of a honeypot or a padded cell and alarm.
- Legal drawbacks to trap and trace
  - Enticement: act of attracting attention to system by placing tantalizing information in key locations
  - Entrapment: act of luring an individual into committing a crime to get a conviction
  - Enticement is legal and ethical, entrapment is not.

Active Intrusion Prevention

- Some organizations implement active countermeasures.
- One tool (LaBrea) takes up unused IP address space to pretend to be a computer and allow attackers to complete a connection request, but then holds connection open.

Scanning and Analysis Tools

- Scanning tools typically are used to collect information that an attacker needs to launch a successful attack.
- Attack protocol is a logical sequence of steps or processes used by an attacker to launch an attack against a target system or network.
- Footprinting: process of collecting publicly available information about a potential target

Scanning and Analysis Tools (cont'd)

- Fingerprinting: systematic survey of target organization's Internet addresses collected during the footprinting phase to identify network services offered by hosts in that range
- Fingerprinting reveals useful information about the internal structure and nature of the target system or network to be attacked.
- These tools are valuable to the network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close vulnerabilities.

Port Scanners

- Tools used by both attackers and defenders to identify/fingerprint computers active on a network and other useful information
- Can either perform generic scans or those for specific types of computers, protocols, or resources
- The more specific the scanner is, the more useful its information is to attackers and defenders.

Port number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

Table 7-1 Commonly Used Port Numbers

Firewall Analysis Tools

- Several tools automate remote discovery of firewall rules and assist the administrator/attacker in analyzing them.
- Administrators who feel wary of using the same tools that attackers use should remember:
  - User intent dictates how gathered information will be used.
  - To defend a computer or network well, administrators must understand ways it can be attacked.
- A tool that can help close an open or poorly configured firewall will help the network defender minimize risk from attack.

Operating System Detection Tools

- Ability to detect a target computer's operating system (OS) is very valuable to an attacker.
  - Once OS is known, the attacker can easily determine the vulnerabilities to which it is susceptible.
- Many tools use networking protocols to determine a remote computer's OS.

Vulnerability Scanners

- Active vulnerability scanners examine networks for highly detailed information and initiate traffic to determine security holes.
- Passive vulnerability scanners listen in on network and identify the vulnerable versions of both server and client software.
- Passive vulnerability scanners have the ability to find client-side vulnerabilities typically not found in active scanners.

Packet Sniffers

- Network tool that captures copies of packets from network and analyzes them
- Can provide network administrator with valuable information for diagnosing and resolving networking issues
- In the wrong hands, a sniffer can be used to eavesdrop on network traffic.
- To use packet sniffers legally, an administrator must be on a network that the organization owns, be under direct authorization of owners of the network, and have knowledge and consent of the content's creators.

Wireless Security Tools

- An organization that spends its time securing a wired network while ignoring wireless networks is exposing itself to a security breach.
- Security professionals must assess the risk of wireless networks.
- A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess the level of privacy or confidentiality afforded on the wireless network.

Summary

- Intrusion detection system (IDPS) detects violation of its configuration and activates alarm.
- Network-based IDPS (NIDPS) versus host-based IDPS (HIDPS)
- Selecting IDPS products that best fit an organization's needs is challenging and complex.
- Honeypots are decoy systems; two variations are known as honeynets and padded cell systems.

Summary (cont'd)

- Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of a network.