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

IDPS • Honeypots • Honeynets • Padded Cells • Scanning Tools

Principles of Information Security
Whitman & Mattord — 6th Edition | Chapter 7

Topic Security Technology: IDPS and Other Security Tools **Edition** 6th (2018) **Chapter** 7 of 12

LEARNING OBJECTIVES	
Objective 1	Identify and describe the categories and models of intrusion detection and prevention systems (IDPSs)
Objective 2	Describe the detection approaches: signature-based detection, anomaly-based detection, and stateful protocol analysis
Objective 3	Define and describe honeypots, honeynets, and padded cell systems — use, advantages, disadvantages, and legal implications
Objective 4	List and define major categories of scanning and analysis tools, and describe specific tools within each category

7.1 Introduction

Building on Chapter 6 (firewalls, VPNs), this chapter covers advanced security technologies including IDPSs, honeypots, and scanning tools.

Intrusion	An adverse event in which an attacker attempts to gain entry into an information system or disrupt its normal operations, almost always with the intent to do harm.
IDS (Intrusion Detection System)	A system capable of automatically detecting an intrusion and notifying a designated authority. Works like a burglar alarm — detects violation and activates alarm. PASSIVE — detects and reports only.
IPS (Intrusion Prevention System)	Extends IDS with active prevention capability — can prevent an intrusion from succeeding by means of an active response. Typically deployed INLINE in the traffic path.
IDPS	The general term encompassing both detection AND prevention. An IDPS can detect and modify its environment to prevent intrusions. Per NIST SP 800-94, this is the current standard term.

KEY PRINCIPLE	While every INTRUSION is an incident, NOT every INCIDENT is an intrusion. Service outages and natural disasters are incidents — but they are not intrusions. Intrusions are almost always instigated by someone with intent to harm.

7.1.1 IDPS Response Techniques (NIST SP 800-94)

According to NIST SP 800-94, Rev. 1, IDPSs can respond in three ways:

- INTERDICTING the attack by itself — terminating the user session, blocking access from the attack source, or blocking all access to the targeted asset
- MODIFYING ITS ENVIRONMENT — changing firewall rules or reconfiguring network devices to disrupt the attack channel
- CHANGING ATTACK COMPONENTS — replacing malicious content with benign material or quarantining packet contents

7.2 IDPS Terminology

Understanding how an IDPS works requires familiarity with these key terms:

Term	Definition	Impact/Notes
False Positive	An alert or alarm that occurs in the ABSENCE of an actual attack	Makes users insensitive to alarms — reduces reaction to actual intrusions
False Negative	FAILURE of IDPS to react to an actual attack event	MOST GRIEVOUS IDPS failure — attack succeeds undetected
True Attack Stimulus	Event that triggers alarm during an actual attack or authorized drill	Desired outcome — IDPS working correctly
False Attack Stimulus	Event that triggers alarm but NO actual attack is in progress	Used in IDPS testing scenarios
Noise	Accurate alarms that do NOT pose significant threats	Unsuccessful attacks are most common noise source
Alarm Clustering	Grouping nearly identical alarms into a single higher-level alarm	Reduces admin overhead; identifies relationships between alarms
Alarm Filtering	Classifying IDPS alerts for more effective management	Admin configures after observing false positive patterns
Confidence Value	Measure of IDPS ability to correctly detect certain attack types	Based on fuzzy logic and past performance measurements
Evasion	Attacker changes format/timing of activities to avoid detection	IDPS must be tuned to detect evasion techniques
Tuning	Adjusting IDPS to maximize true positives, minimize false positives/negatives	Ongoing administrative responsibility

Site Policy Awareness	IDPS ability to dynamically modify its configuration (dynamic IDPS)	Smart IDPS knows when NOT to alert — known exploit from protected system

EXAM TIP	False Negative is MORE DANGEROUS than False Positive in security contexts. A false negative means an attack occurred and was NOT detected. A false positive is a nuisance (alert fatigue) but does not result in a successful attack.

7.3 Why Use an IDPS?

7.3.1 Intrusion Detection

The primary purpose of an IDPS is to identify and report intrusions early enough to contain the attack:

- Detect FOOTPRINTING — activities that gather information about the organization's network (passive reconnaissance)
- Detect FINGERPRINTING — activities that scan for active systems and services (active reconnaissance) — together called 'doorknob rattling'
- Protect assets even when known vulnerabilities CANNOT be immediately patched (when services cannot be disabled)
- Detect attacks even against ZERO DAY VULNERABILITIES by using anomaly-based detection

Zero Day Vulnerability	An unknown or undisclosed vulnerability that can't be predicted or prepared for. Called 'zero day' because owners have ZERO DAYS to mitigate once discovered. Most become known only when used in an actual attack.

7.3.2 Data Collection

IDPSs configured to log data contribute to:

- Forensic investigation — reveals WHO (IP address), WHAT (attack method), and HOW (tools and techniques) of an attack
- EVIDENTIARY PACKET DUMP — data hashed with cryptographic algorithm becomes admissible in civil or criminal court
- Detecting data theft — large file transfers or unauthorized access to protected files
- Management justification — documentation of threats supports security budget requests

7.3.3 Attack Deterrence & Quality Assurance

Additional reasons to deploy IDPSs:

- Attack Deterrence — known presence of IDPS increases fear of detection (like a burglar alarm on a house)
- Detect incomplete firewall configurations — traffic passing that should have been filtered
- Identify security policy violations by authorized internal users
- Kill Chain — success of an attack can be disrupted at ANY phase from reconnaissance to exfiltration

- Detect IDPS TERRORISTS — attackers who deliberately trip the IDPS to cause the organization to DoS itself via overreaction

7.4 Types of IDPS

7.4.1 Network-Based IDPS (NIDPS)

NIDPS	Resides on a computer or appliance connected to a network segment. Monitors traffic on that segment for indications of attacks. Consists of a management console plus AGENTS/SENSORS at remote locations.

Key NIDPS concepts:

- MONITORING PORT (SPAN port / Mirror port) — a specially configured switch port that can view ALL traffic through the device. Required because switches create dedicated point-to-point links that would otherwise hide traffic from the NIDPS.
- PROTOCOL STACK VERIFICATION — looks for invalid data packets (malformed under TCP/IP protocol rules). Detects DoS/DDoS attacks that use malformed packets.
- APPLICATION PROTOCOL VERIFICATION — examines higher-order protocols (HTTP, SMTP, FTP) for unexpected packet behavior. Detects DNS cache poisoning and similar protocol abuse attacks.

NIDPS Advantages	NIDPS Disadvantages
Good coverage — few devices monitor large network	Can be overwhelmed by network volume — fails to detect attacks
Passive — deployed with no disruption to operations	Cannot analyze ENCRYPTED traffic (SSL, SSH, VPN)
Typically not detectable by attackers	Cannot reliably confirm attack SUCCESS — requires log review
Detects DoS, port scans, protocol anomalies	Limited on fully switched networks — requires SPAN port capability
Centralizes security monitoring	Vulnerable to fragmented packet attacks

7.4.2 Wireless IDPS

Monitors and analyzes wireless network traffic at OSI Layers 2–3. Cannot evaluate higher-layer protocols like TCP/UDP. Wireless IDPS capability can be built into access points (APs).
Wireless IDPS deployment issues:

- Physical security — sensors often in public areas (conference rooms, hallways, outdoors)
- Sensor range — affected by atmospheric conditions and building construction; footprints should overlap
- Cost — wireless components cost more than wired counterparts

Wireless IDPSs can detect: unauthorized WLANs and devices, poorly secured WLAN devices, unusual usage patterns, DoS attacks, and man-in-the-middle attacks.

7.4.3 Network Behavior Analysis (NBA) IDPS

Identifies problems related to FLOW of network traffic. Uses anomaly detection to identify excessive packet flows from equipment malfunction, DoS, viruses, worms, and policy violations.
NBA sensors detect: DoS/DDoS attacks, scanning, worm activity, unexpected application services (tunneled protocols, backdoors), and policy violations.

7.4.4 Host-Based IDPS (HIDPS)

HIDPS	Resides on a particular HOST (computer/server). Monitors activity on that system only. Also known as a SYSTEM INTEGRITY VERIFIER — benchmarks and monitors status of key system files and detects when intruder creates, modifies, or deletes monitored files.

HIDPS characteristics:

- Monitors system configuration databases (Windows registry, .ini/.cfg/.dat files)
- Triggers alerts when file attributes change, new files created, or existing files deleted
- Maintains its own LOG FILE — audit trail available even if attacker modifies system files
- Color-coded file categories: RED (critical — OS kernel, registry, security apps), YELLOW (support — device drivers), GREEN (user data — modified frequently)
- False positives occur ONLY when authorized changes are made to monitored files — easily reviewed

HIDPS Advantages	HIDPS Disadvantages
Detects local events that may elude NIDPS	More management effort — configured per host
CAN access encrypted traffic (post-decryption)	Vulnerable to direct attacks on host OS
Not affected by switched network protocols	Cannot detect multi-host scanning
Detects Trojan programs via audit log comparison	Susceptible to some DoS attacks
Detects privilege escalation attempts	Performance overhead + disk space for audit logs

7.5 IDPS Detection Methods

7.5.1 Signature-Based Detection (Knowledge-Based / Misuse Detection)

Signature-Based Detection	Examines network traffic in search of patterns that match known SIGNATURES — preconfigured, predetermined attack patterns. Must continuously update signature database to detect new attacks.

Signatures work well against:

- Footprinting/fingerprinting activities using ICMP, DNS querying, and e-mail routing analysis
- Exploits using specific attack sequences targeting known vulnerabilities
- DoS/DDoS attacks overloading systems with requests

KEY LIMITATION	Signature-based detection CANNOT detect zero-day attacks — only attacks with known signatures in the database. New attack patterns must be continuously added. A slow, methodical multi-event attack may also escape detection.

7.5.2 Anomaly-Based Detection (Behavior-Based / Statistical Detection)

Anomaly-Based Detection	Collects statistical summaries by observing NORMAL TRAFFIC during a TRAINING PERIOD to establish a baseline. Alerts when activity EXCEEDS THE CLIPPING LEVEL — the predefined deviation from baseline.

Key concepts:

- CLIPPING LEVEL — the predefined assessment threshold that triggers a response when surpassed
- STATIC PROFILES — do not change until modified/recalibrated by admin
- DYNAMIC PROFILES — periodically update baseline from new observations. Vulnerability: slow attacks can corrupt dynamic baseline
- CAN detect zero-day attacks — looks for ANY abnormal activity
- Higher false positive rate — dramatic swings in legitimate activity generate false alarms

7.5.3 Stateful Protocol Analysis (SPA)

Stateful Protocol Analysis (SPA)	Comparison of vendor-supplied profiles of NORMAL PROTOCOL BEHAVIOR against observed traffic. IDPS knows how FTP/HTTP/SMTP is supposed to work — detects anomalous use. Also called DEEP PACKET INSPECTION.

SPA capabilities:

- Detects out-of-sequence commands, malformed commands, and commands outside expected length parameters
- Stores relevant session data to detect multi-session attacks
- Better at detecting specialized, multisession attacks than signature-based detection

SPA limitations:

- Heavy processing overhead — tracks multiple simultaneous connections
- Proprietary protocols not published in sufficient detail for comprehensive SPA
- May interfere with normal protocol operations it monitors

7.5.4 Log File Monitors (LFM) and SIEM

Log File Monitor (LFM)	Reviews log files generated by servers, network devices, and other IDPSs looking for patterns indicating an attack. Multiple log sources reveal subtle patterns invisible when one system is examined in isolation.

SIEM (Security Information and Event Management)	Software and procedures that COLLECT, ANALYZE, REPORT, and REACT to events determined by patterns in aggregated data. Coined 2005 by Gartner. Data sources: IDPS, IAM, network devices, host systems. May be required for compliance (HIPAA, PCI DSS, SOX).

7.6 IDPS Response Options

IDPS responses are classified as ACTIVE (automatically initiated on alert trigger) or PASSIVE (reports and waits for admin action):

Response Type	Description	Considerations
Audible/Visual Alarm	Sound, light, pop-up window with attack specifics and confidence level	Most common; pop-ups can include attack tools and addresses
SNMP Traps	Notify SNMP management console via trap function	Standard implementation in network devices
E-mail / SMS Message	Notify administrators via email or SMS text	Caution: attacks may disrupt or delay email delivery
Log Entry	Record event details in separate server logs	Store on separate servers to prevent attacker deletion
Evidentiary Packet Dump	Cryptographic hash-protected logs suitable for court	Resource-intensive; especially in DoS attacks
Reconfigure Firewall	Send command to block attacker IP, port, or protocol	Attacker may change IP/port to evade; temporary blocks are common
Terminate Session	TCP close packet terminates session	Simple but attacker can immediately open new session
Terminate Connection	Disconnect internal or external network links	LAST RESORT — may be attacker's goal (DoS)
Launch Program	Execute specialized tracking or response software	Multiple vendor solutions available for this purpose

LEGAL CAUTION	Taking action AGAINST the intruder (back-hacking, counterattacks) is NOT advisable. An organization only owns its network to its perimeter. Counterattacking may harm an innocent compromised intermediary — making the organization as criminally liable as the original attacker. Seek legal counsel before configuring any automated retaliation.

7.7 IDPS Control Strategies & Deployment

7.7.1 Control Strategies

Strategy	Description	Advantages	Disadvantages
Centralized	All control functions managed at ONE central IDS Console. Sensors report to central management system.	Cost-effective; one management system; enables holistic attack detection	Single point of failure; response time limited by communication to central console
Fully Distributed	All control functions applied at PHYSICAL LOCATION of each component. Each sensor	Fastest local response time; each sensor	Expensive; difficult to coordinate; no big-picture attack detection

	manages its own detection and response.	optimized for its environment	
Partially Distributed ★ RECOMMENDED	Local agents respond to local threats; report to hierarchical central facility for correlation.	Combines local response speed with centralized big-picture analysis; detects distributed attacks	More complex to implement than purely centralized

EXAM TIP	Partially Distributed control strategy is the RECOMMENDED approach. It combines the local response speed of fully distributed with the big-picture detection capability of centralized. Particularly effective for detecting intelligent attackers who probe multiple entry points simultaneously.

7.7.2 NIDPS Sensor Placement (NIST SP 800-94)

Location	Placement	Purpose
Location 1 (Recommended)	Behind external firewall, in DMZ	Sees attacks penetrating perimeter; identifies firewall policy problems; monitors Web/FTP servers
Location 2	Outside external firewall	Documents NUMBER and TYPES of attacks from the Internet targeting the network
Location 3	On major network backbones	Monitors large traffic volumes; detects unauthorized activity by authorized internal users
Location 4	On critical subnets	Detects attacks targeting critical systems; allows limited-budget organizations to protect highest-value assets

7.7.3 HIDPS Deployment

HIDPS deployment principles:

- Begin with most CRITICAL systems first — practice on test servers to develop expertise before production deployment
- Install until all systems are covered or the planned degree of coverage is reached
- Each HIDPS should interact with a CENTRAL MANAGEMENT CONSOLE for ease of management
- Use offline test systems to develop baseline of normal traffic before deploying on production
- Create training scenarios enabling users to recognize and respond to common attacks

7.8 Measuring IDPS Effectiveness

IDPSs are evaluated using several mechanisms:

- THRESHOLDS — values specifying maximum acceptable levels (e.g., x failed connections in 60 seconds). Most used for anomaly-based detection and SPA.
- BLACKLISTS — list of hosts, ports, applications, URLs associated with malicious activity. IDPSs block highly likely malicious activity from blacklisted entities.

- WHITELISTS — list of entities known to be benign. Used to reduce false positives for trusted hosts.
- ALERT SETTINGS — admins customize each alert type (toggle on/off, set priority, specify notification methods, specify prevention capabilities)

KEY POINT	Modern IDPS effectiveness is measured by: (1) percentage of attacks detected at a given traffic load, and (2) the network load level at which the IDPS fails (measured in Mbps). Example: 'At 100 Mb/s, the IDPS detected 97% of directed attacks.' The old 'more signatures = better' metric is outdated — some sophisticated systems use FEWER signatures but are more effective.

7.9 Honeypots, Honeynets, and Padded Cell Systems

Honeypot	An application that entices people illegally perusing internal network areas by providing simulated rich content while notifying the administrator. Also called decoys, lures, or flytraps. Any unauthorized access is SUSPICIOUS BY DEFINITION.
Honeynet	A monitored network or network segment containing MULTIPLE HONEYPOT SYSTEMS. Simulates a full production network environment. All traffic in/out is logged and analyzed.
Padded Cell System	A HARDENED HONEYPOT that cannot be easily compromised. Works with a traditional IDPS — when IDPS detects attacker, they are SEAMLESSLY TRANSFERRED to the padded cell where they can cause no harm.

Honeypots are designed to:
- Divert an attacker from critical systems
- Collect information about the attacker's activity, tools, and techniques
- Encourage the attacker to stay long enough for administrators to document the event and respond

Honeypot/Padded Cell Advantages	Honeypot/Padded Cell Disadvantages
Attackers diverted to targets they CANNOT damage	Legal implications are NOT WELL UNDERSTOOD
Administrators have TIME to decide how to respond	Not yet shown to be GENERALLY USEFUL security technologies
Attacker actions extensively monitored for threat modeling	Expert attackers may launch MORE AGGRESSIVE attacks when diverted
Effective at catching INSIDERS snooping the network	Require HIGH LEVEL OF EXPERTISE to operate safely

7.9.1 Trap-and-Trace Systems and Legal Framework

Trap-and-Trace	Combines honeypot/padded cell with capability to TRACE the attacker back through the network. While attacker is distracted, system notifies admin and initiates trace.

Enticement	LEGAL — attracting attention to a system by placing tantalizing information in key locations. Acceptable use of honeypots.
Entrapment	ILLEGAL — luring a person into committing a crime in order to get a conviction. NEVER acceptable.
Back Hack	The process of illegally attempting to determine source of intrusion by tracing it and gaining access to the originating system. Typically illegal and may harm innocent third parties.

LEGAL REQUIREMENT	Under Title 18, U.S. Code Chapter 206, §3121 — no person may install or use a pen register or trap-and-trace device without a COURT ORDER, unless: (1) used for maintenance/testing, (2) used to track connections, or (3) user consent is obtained. Organizations must consult legal counsel before deploying honeypots, honeynets, padded cells, or trap-and-trace systems.

7.9.2 Active Intrusion Prevention — LaBrea

LaBrea is a 'sticky' honeypot and IDPS that takes up UNUSED IP ADDRESS SPACE on a network. When LaBrea detects an ARP request for an unused IP address, it pretends to be a computer at that address, completes the TCP/IP three-way handshake with the attacker, then changes the TCP sliding window size to a very LOW NUMBER to hold the connection open for hours, days, or months — effectively slowing worms and other automated attacks.

7.10 Scanning and Analysis Tools

To truly assess the risks in a computing environment, defense in depth requires IDPSs, ACTIVE VULNERABILITY SCANNERS, PASSIVE VULNERABILITY SCANNERS, AUTOMATED LOG ANALYZERS, and PROTOCOL ANALYZERS (sniffers). Scanning tools enable administrators to 'see what the attacker sees.'

7.10.1 The Attack Protocol

Footprinting	The organized research and investigation of Internet addresses owned or controlled by a target organization. Uses public Internet data sources, company websites, and search engines. Example tool: Sam Spade, GNU Wget (mirrors entire websites).
Fingerprinting	The systematic survey of a targeted organization's Internet addresses to identify network services offered by hosts. Uses port scanners, OS detection tools, and vulnerability scanners to reveal internal structure.

KEY PRINCIPLE	A chain is only as strong as its weakest link. Attackers use footprinting to find B2B partners and subsidiaries — often less secure than the primary target — and use them as an entry point into the main network.

7.10.2 Port Scanners

Port Scanner	Tools used by both attackers and defenders to identify active computers on a network, active ports and services on those computers, functions and roles of machines, and other useful information. Most popular: Nmap (UNIX and Windows).

Key port scanning concepts:

- ATTACK SURFACE — the functions and features that a system exposes to unauthenticated users. Security design goal: MINIMIZE the attack surface.
- Ports 1–1023 = well-known ports (reserved for standard services). Ports >1023 = EPHEMERAL ports.
- Any port not absolutely necessary for business should be SECURED OR REMOVED FROM SERVICE.
- Nmap options: TCP SYN scan, TCP Connect scan, UDP scan, OS detection (-O), idle scan (-I for firewall analysis)

7.10.3 Firewall Analysis Tools

Tools that automate remote discovery and analysis of firewall rules:

- NMAP IDLE SCAN (-I switch) — bounces a scan through a DMZ host to discover internal network services behind a firewall without detection
- FIREWALK (Schiffman & Goldsmith) — uses incrementing TTL packets to determine network path and default firewall policy. Reveals where routers and firewalls filter traffic.
- HPING — modified ping client supporting multiple protocols. Can determine DMZ infrastructure using modified TTL values or bypass poorly configured ICMP-permissive firewalls.

7.10.4 OS Detection Tools

- XPROBE — uses ICMP to determine remote OS. Each OS has a unique way of responding to ICMP — XProbe matches responses against its internal database. DEFENSE: restrict ICMP through firewalls.

7.10.5 Vulnerability Scanners

Active Vulnerability Scanner	Initiates traffic on the network to determine security holes. Identifies hosts, services, OS, CVEs, misconfigurations, default credentials. Examples: Nessus (commercial), OpenVAS (open-source), Nexpose, MBSA, QualysGuard, SAINT.
Passive Vulnerability Scanner	Listens in on the network to identify vulnerable versions of both server AND client software. Does NOT require vulnerability analysts to obtain approval prior to testing. Examples: Tenable PVS, Watcher Web Security Scanner.
Fuzzer (Black-Box Scanner)	Looks for vulnerabilities by feeding RANDOM INPUT to a program or protocol. Used for new/custom applications where no known CVE database exists. Example: SPIKE (with SPIKE Proxy).

KEY DISTINCTION	Active vulnerability scanners INITIATE TRAFFIC — they can be detected and may disrupt systems. Passive scanners LISTEN ONLY — they can find client-side vulnerabilities that active scanners miss. Nessus in 'destructive mode' can crash systems — use ONLY in lab environments.

Top vulnerability scanners (from the book): Core Impact, GFI LanGuard, MBSA, Nessus, Nexpose, Nipper, OpenVAS, QualysGuard, Retina, Secunia PSI, SAINT.

Metasploit Framework	Collection of exploits plus an interface to automate exploitation of vulnerable systems. Allows creation of accounts, modification of web pages, or data viewing on compromised systems. The ONLY major exploit framework available without a license fee (unlike Core Impact and Immunity CANVAS). MOST RISKY — use only when absolutely necessary.

7.10.6 Packet Sniffers

Packet Sniffer (Network Protocol Analyzer)	A software program or hardware appliance that can intercept, copy, and interpret network traffic. Wireshark (formerly Ethereal) is the most popular open-source example.

LEGAL REQUIREMENTS for packet sniffer use — ALL three must be met:

- Be on a network that the ORGANIZATION OWNS
- Have DIRECT AUTHORIZATION from the network's owners
- Have KNOWLEDGE AND CONSENT of the content's creators (typically signed in user agreements)

IMPORTANT	These three conditions are the same requirements for EMPLOYEE MONITORING in general. Packet sniffing should be construed as a form of employee monitoring. Simply being on a switched network does NOT protect against sniffing — tools like Ettercap using ARP-spoofing can enable packet capture on switched networks. ENCRYPTION is the essential defense.

7.10.7 Wireless Security Tools

A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess confidentiality on the wireless network:

Tool	Type	Description
Aircrack	Cracking tool	Wireless network protocol cracking tool for testing WEP/WPA
Kismet	Passive sniffer/IDPS	Powerful wireless network protocol sniffer, network detector, and IDPS — works by passively sniffing
NetStumbler	Scanner	Freeware Windows tool for detecting WLANs
inSSIDer	Enhanced scanner	Enhanced scanner for Windows, OS X, and Android
KisMac	GUI stumbler	GUI passive wireless stumbler for Mac OS X (Kismet variant)

AirSnare	Alert tool	Monitors airwaves for new devices/access points; sounds alarm when new wireless apparatus is detected

7.11 Chapter Summary & Exam Review

Key Terms Summary

Term	Definition	Key Detail
IDS	Intrusion Detection System	Passive — detects and reports only. Out-of-band.
IPS	Intrusion Prevention System	Active + inline — detects and blocks in real time.
IDPS	Intrusion Detection & Prevention System	Combined term for both IDS and IPS capabilities.
False Negative	IDPS fails to detect actual attack	MOST GRIEVOUS failure — attack succeeds undetected.
False Positive	IDPS triggers alarm without actual attack	Alert fatigue — reduces reaction to real alarms.
NIDPS	Network-Based IDPS	Monitors network segment. CANNOT inspect encrypted traffic.
HIDPS	Host-Based IDPS	Monitors individual host. CAN inspect encrypted traffic.
SPAN Port	Switched Port Analysis (Mirror Port)	Required for NIDPS on switched networks — mirrors all traffic.
Signature-Based	Knowledge-Based/Misuse Detection	Effective against known attacks; cannot detect zero-days.
Anomaly-Based	Behavior-Based/Statistical Detection	Can detect zero-days; higher FP; requires training period.
SPA	Stateful Protocol Analysis	Compares normal protocol profiles against observed traffic.
Clipping Level	Threshold for anomaly detection	Exceeded level triggers alert in anomaly-based IDPS.
Honeypot	Decoy system	Any access is suspicious by definition; legal issues.
Honeynet	Network of honeypots	Multiple decoys simulating a production network.
Padded Cell	Hardened honeypot + IDPS integration	IDPS detects → seamlessly transfers attacker to padded cell.
Footprinting	Passive info gathering	Research of organization's public Internet addresses.
Fingerprinting	Active network scanning	Scanning to identify active services and OS.
Blacklist	Blocked entity list	Entities associated with malicious activity — blocked by IDPS.
Whitelist	Trusted entity list	Known benign entities — reduces false positives.

Review Questions (from Book)

#	Question	Answer
Q1	What common security system is an IDPS most like?	A BURGLAR ALARM — detects violations and activates an alarm. Similar in that it detects intrusion and notifies appropriate personnel.
Q2	How does a false positive differ from a false negative? Which is less desirable?	FP = alarm with no real attack. FN = missed real attack. False NEGATIVE is less desirable — attack succeeds undetected.
Q3	How does a network-based IDPS differ from a host-based IDPS?	NIDPS monitors network segment traffic. HIDPS monitors individual host activity. NIDPS cannot inspect encrypted traffic; HIDPS can (post-decryption).
Q4	How does a signature-based IDPS differ from a behavior-based IDPS?	Signature = known attack patterns, low FP, no zero-days. Behavior/anomaly = detects zero-days, higher FP, requires training period.
Q5	What is a monitoring (SPAN) port?	A specially configured switch port that can view ALL traffic through the device. Required for NIDPS on switched networks.
Q6	List and describe the three IDPS control strategies.	Centralized (one console), Fully Distributed (each sensor controls itself), Partially Distributed (local + hierarchical central) — RECOMMENDED.
Q7	What is a honeypot? How is it different from a honeynet?	Honeypot = single decoy system. Honeynet = MULTIPLE honeypots on a network segment simulating a full production environment.
Q8	How does a padded cell system differ from a honeypot?	Padded cell works WITH an IDPS — IDPS detects attacker and TRANSFERS them to the padded cell. A honeypot operates independently to attract attackers.
Q9	What is network footprinting?	The organized PASSIVE research of Internet addresses owned by a target — using public data sources, search engines, and company websites.
Q10	What is network fingerprinting?	The ACTIVE systematic survey of a target's Internet addresses to identify network services offered by hosts — uses port scanners and OS detection tools.
Q14	Why is it important to limit the number of open ports?	Each open port is a potential attack vector. The fewer open ports, the smaller the ATTACK SURFACE — minimizing latent defects and unintended consequences.
Q17	Difference between active and passive vulnerability scanners?	Active scanners INITIATE TRAFFIC to find holes. Passive scanners LISTEN ONLY to identify vulnerable software versions — no approval needed.
Q18	What is Metasploit and why is it riskier?	Metasploit is an exploitation framework that actually exploits vulnerable systems. Riskier because it demonstrates actual impact — may create accounts or modify systems.

★ FINAL EXAM TIPS — CHAPTER 7

- **False Negative is the MOST DANGEROUS — attack succeeds undetected. False Positive causes alert fatigue but no direct harm.**
- **IDS = passive (detect + alert, out-of-band). IPS = active inline (detect + block). IDPS = both combined.**

- **NIDPS CANNOT inspect encrypted traffic. HIDPS CAN inspect encrypted traffic (decrypted on the host first).**
- **Signature-based = known attacks, LOW false positive rate, CANNOT detect zero-days. Anomaly-based = CAN detect zero-days, HIGHER false positive rate.**
- **Honeypot any access = suspicious by definition. Enticement (legal) vs Entrapment (illegal). ISOLATION from production required. Legal counsel required.**
- **Footprinting = PASSIVE (public info). Fingerprinting = ACTIVE (port scans, OS detection). Both = pre-attack reconnaissance.**
- **Partially Distributed IDPS control strategy = RECOMMENDED. Combines local response with centralized detection of distributed attacks.**
- **All vulnerability scanning and penetration testing REQUIRE WRITTEN AUTHORIZATION. Unauthorized = may violate CFAA.**
- **SPAN/Mirror port = required for NIDPS on switched networks (copies all traffic to monitoring port).**
- **Clipping level = threshold that triggers anomaly-based detection. SIEM = aggregates/correlates logs from all devices.**