1.
intrusion

2.
Alarm filtering

3.
intrusion detection systems (IDS)

4.
intrusion detection and prevention system (IDPS)

5.
Alarm clustering and compaction

6.
Alert or alarm

7.
Confidence value

8.
Evasion

9.
False negative

10.
False positive

2.

The process of classifying IDPS alerts so they can be more effectively managed. An IDPS administrator can set up alarm filtering by running the system for a while to track the types of false positives it generates and then adjusting the alarm classifications. For example, the administrator may set the IDPS to discard

1.

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.

4.

The general term for a system that can both detect and modify its configuration and environment to prevent intrusions. An IDPS encompasses the functions of both intrusion detection systems and intrusion prevention technology.

3.

A system capable of automatically detecting an intrusion into an organization’s networks or host systems and notifying a designated authority.

6.

An indication or notification that a system has just been attacked or is under attack. IDPS alerts and alarms take the form of audible signals, e-mail messages, pager notifications, or pop-up windows.

5.

A process of grouping almost identical alarms that occur nearly at the same time into a single higher-level alarm. This consolidation reduces the number of alarms, which reduces administrative overhead and identifies a relationship among multiple alarms. Clustering may be based on combinations of frequency,

8.

The process by which attackers change the format and/or timing of their activities to avoid being detected by an IDPS.

7.

The measure of an IDPS’s ability to correctly detect and identify certain types of attacks. The confidence value an organization places in the IDPS is based on experience and past performance measurements. The confidence value, which is based on *fuzzy logic*, helps an administrator determine the likelihood that an

10.

An alert or alarm that occurs in the absence of an actual attack. A false positive can sometimes be produced when an IDPS mistakes normal system activity for an attack. False positives tend to make users insensitive to alarms and thus reduce their reactions to actual intrusion events.

9.

The failure of an IDPS to react to an actual attack event. This is the most grievous IDPS failure, given that its purpose is to detect and respond to attacks.

11.
False attack stimulus

12.
Noise

13.
Site policy

14.
Site policy awareness

15.
Tuning

16.
True attack stimulus

17.
known vulnerabilities

18.
Zero day vulnerabilities

19.
sensors

20.
agents

11.

An event that triggers an alarm when no actual attack is in progress. Scenarios that test the configuration of IDPSs may use false attack stimuli to determine if the IDPSs can distinguish between these stimuli and real attacks.

12.

The presence of additional and disruptive signals in network communications or electrical power delivery. Also, noise can be alarm events that are accurate and noteworthy but do not pose significant threats to information security. Unsuccessful attacks are the most common source of IDPS noise, although some noise

13.

The rules and configuration guidelines governing the implementation and operation of IDPSs within the organization.

14.

An IDPS's ability to dynamically modify its configuration in response to environmental activity. A so-called dynamic IDPS can adapt its reactions in response to administrator guidance over time and the local environment. A dynamic IDPS logs events that fit a specific profile instead of minor events, such as file

15.

The process of adjusting an IDPS to maximize its efficiency in detecting true positives while minimizing false positives and false negatives.

16.

An event that triggers an alarm and causes an IDPS to react as if a real attack is in progress. The event may be an actual attack, in which an attacker is attempting a system compromise, or it may be a drill, in which security personnel are using hacker tools to test a network segment.

17.

A published weakness or fault in an information asset or its protective systems that may be exploited and result in loss.

18.

An unknown or undisclosed vulnerability in an information asset or its protection systems that may be exploited and result in loss. This vulnerability is also referred to as *zero day* (or *zero hour*) because once it is discovered, the technology owners have zero days to identify, mitigate, and resolve the vulnerability.

19.

A hardware and/or software component deployed on a remote computer or network segment and designed to monitor network or system traffic for suspicious activities and report back to the host application. For example, IDPS sensors report to an IDPS application.

20.

See *sensor*.

21.
network-based IDPS (NIDPS)

22.
monitoring port

23.
switched port analysis (SPAN) port

24.
protocol stack verification

25.
mirror port

26.
Inline sensors

27.
passive mode

28.
host-based IDPS (HIDPS)

29.
application protocol verification

30.
misuse detection

22.
Also known as a switched port analysis (SPAN) port or mirror port, a specially configured connection on a network device that can view all the traffic that moves through the device.

21.
An IDPS that resides on a computer or appliance connected to a segment of an organization's network and monitors traffic on that segment, looking for indications of ongoing or successful attacks.

24.
The process of examining and verifying network traffic for invalid data packets—that is, packets that are malformed under the rules of the TCP/IP protocol.

23.
See *monitoring port*.

26.
An IDPS sensor intended for network perimeter use and deployed in close proximity to a perimeter firewall to detect incoming attacks that could overwhelm the firewall.

25.
See *monitoring port*.

28.
An IDPS that resides on a particular computer or server, known as the host, and monitors activity only on that system. Also known as a system integrity verifier.

27.
An IDPS sensor setting in which the device simply monitors and analyzes observed network or system traffic.

30.
See *signature-based detection*.

29.
The process of examining and verifying the higher-order protocols (HTTP, FTP, and Telnet) in network traffic for unexpected packet behavior or improper use.

31.
signature-based detection

32.
knowledge-based detection

33.
behavior-based detection

34.
Anomaly-based detection

35.
signatures

36.
clipping level

37.
security information and event management (SIEM)

38.
log file monitor (LFM)

39.
stateful protocol analysis (SPA)

40.
partially distributed IDPS control strategy

32.
See *signature-based detection*.

31.
Also known as *knowledge-based detection* or *misuse detection*, the examination of system or network data in search of patterns that match known attack signatures.

34.
Also known as *behavior-based detection*, an IDPS detection method that compares current data and traffic patterns to an established baseline of normalcy.

33.
See *anomaly-based detection*.

36.
A predefined assessment level that triggers a predetermined response when surpassed. Typically, the response is to write the event to a log file and/or notify an administrator.

35.
Patterns that correspond to a known attack.

38.
An attack detection method that reviews the log files generated by computer systems, looking for patterns and signatures that may indicate an attack or intrusion is in process or has already occurred.

37.
A software-enabled approach to aggregating, filtering, and managing the reaction to events, many of which are collected by logging activities of IDPSs and network management devices.

40.
An IDPS implementation approach that combines the best aspects of the centralized and fully distributed strategies.

39.
The comparison of vendor-supplied profiles of protocol use and behavior against observed data and network patterns in an effort to detect misuse and attacks.

41.
fully distributed IDPS control strategy

42.
threshold

43.
centralized IDPS control strategy

44.
blacklist

45.
Honeypots

46.
whitelist

47.
pen registers

48.
honeynet

49.
padded cell system

50.
Trap-and-trace

42.

A value that sets the limit between normal and abnormal behavior. See also *clipping level*.

41.

An IDPS implementation approach in which all control functions are applied at the physical location of each IDPS component.

44.

A list of systems, users, files, or addresses that have been associated with malicious activity; it is commonly used to block those entities from systems or network access.

43.

An IDPS implementation approach in which all control functions are implemented and managed in a central location.

46.

A list of systems, users, files, or addresses that are known to be benign; it is commonly used to expedite those entities’ access to systems or networks.

45.

An application that entices people who are illegally perusing the internal areas of a network by providing simulated rich content while the software notifies the administrator of the intrusion.

48.

A monitored network or network segment that contains multiple honeypot systems.

47.

An application that records information about outbound communications.

50.

An application that combines the function of honeypots or honeynets with the capability to track the attacker back through the network.

49.

A protected honeypot that cannot be easily compromised.

51.
back hack

52.
entrapment

53.
enticement

54.
footprinting

55.
fingerprinting

56.
attack protocol

57.
port scanners

58.
Active vulnerability scanners

59.
attack surface

60.
passive vulnerability scanner

52.
The act of luring a person into committing a crime in order to get a conviction.

51.
The process of illegally attempting to determine the source of an intrusion by tracing it and trying to gain access to the originating system.

54.
The organized research and investigation of Internet addresses owned or controlled by a target organization.

53.
The act of attracting attention to a system by placing tantalizing information in key locations.

56.
A logical sequence of steps or processes used by an attacker to launch an attack against a target system or network.

55.
The systematic survey of a targeted organization’s Internet addresses collected during the footprinting phase to identify the network services offered by the hosts in that range.

58.
An application that scans networks to identify exposed usernames and groups, open network shares, configuration problems, and other vulnerabilities in servers.

57.
Tools used both by attackers and defenders to identify or fingerprint active computers on a network, the active ports and services on those computers, the functions and roles of the machines, and other useful information.

60.
A scanner that listens in on a network and identifies vulnerable versions of both server and client software.

59.
The functions and features that a system exposes to unauthenticated users.

1.
project plan

2.
project management

3.
projectitis

4.
work breakdown structure (WBS)

5.
deliverables

6.
resources

7.
milestones

8.
request for proposal (RFP)

9.
project scope

10.
predecessors

2.

The process of identifying and controlling the resources applied to a project as well as measuring progress and adjusting the process as progress is made toward the goal.

1.

The documented instructions for participants and stakeholders of a project that provide details on goals, objectives, tasks, scheduling, and resource management.

4.

A list of the tasks to be accomplished in the project, the skill sets or individual employees needed to perform the tasks, the start and end dates for tasks, the estimated resources required, and the dependencies among tasks.

3.

A situation in project planning in which the project manager spends more time documenting project tasks, collecting performance measurements, recording project task information, and updating project completion forecasts in the project management software than accomplishing meaningful project work.

6.

Components required for the completion of a project, which could include skills, personnel, time, money, and material.

5.

A completed document or program module that can either serve as the beginning point for a later task or become an element in the finished project.

8.

A document specifying the requirements of a project, provided to solicit bids from internal or external contractors.

7.

A specific point in the project plan when a task that has a noticeable impact on the plan's progress is complete.

10.

Tasks or action steps that come before the specific task at hand.

9.

A description of a project's features, capabilities, functions, and quality level, used as the basis of a project plan.

11.
successors

12.
gap analysis

13.
Project wrap-up

14.
direct changeover

15.
phased implementation

16.
pilot implementation

17.
parallel operations

18.
bull’s-eye model

19.
Technology governance

20.
change control

12.

The process of comparing measured results against expected results, then using the resulting “gap” as a measure of project success and as feedback for project management.

11.

Tasks or action steps that come after the specific task at hand.

14.

The conversion strategy that involves stopping the old system and starting the new one without any overlap.

13.

A process of bringing a project to a conclusion, addressing any pending issues and the overall project effort, and identifying ways to improve the process in the future.

16.

The conversion strategy that involves implementing the entire system into a single office, department, or division, and dealing with issues that arise before expanding to the rest of the organization.

15.

The conversion strategy that involves a measured rollout of the planned system; only part of the system is brought out and disseminated across an organization before the next piece is implemented.

18.

A method for prioritizing a program of complex change; it requires that issues be addressed from the general to the specific and focuses on systematic solutions instead of individual problems.

17.

The conversion strategy that involves running the new system concurrently with the old system.

20.

A method of regulating the modification of systems within the organization by requiring formal review and approval for each change.

19.

A process organizations use to manage the effects and costs of technology implementation, innovation, and obsolescence.

21. accreditation	**22.** certification

22.

In information security, the comprehensive evaluation of an IT system’s technical and nontechnical security controls that establishes the extent to which a particular design and implementation meets a set of predefined security requirements, usually in support of an accreditation process.

21.

The process that authorizes an IT system to process, store, or transmit information.