potential vulnerabilities and attacks in progress. One major limitation of current intrusion detection system (IDS) technologies is the requirement to filter false alarms lest the operator (system or security administrator) be overwhelmed with data. IDSes are classified in many different ways, including active and passive, network-based and host- based, and knowledge-based and behavior-based:
Active and passive IDS

An active IDS (now more commonly known as an intrusion prevention system -- IPS) is a system that's configured to automatically block suspected attacks in progress without any intervention required by an operator. IPS has the advantage of providing real-time corrective action in response to an attack but has many disadvantages as well. An IPS must be placed in-line along a network boundary; thus, the IPS itself is susceptible to attack. Also, if false alarms and legitimate traffic haven't been properly identified and filtered, authorized users and applications may be improperly denied access. Finally, the IPS itself may be used to effect a Denial of Service (DoS) attack by intentionally flooding the system with alarms that cause it to block connections until no connections or bandwidth are available.

A passive IDS is a system that's configured only to monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. It isn't capable of performing any protective or corrective functions on its own. The major advantages of passive IDSes are that these systems can be easily and rapidly deployed and are not normally susceptible to attack themselves.
Network-based and host-based IDS

A network-based IDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment.

A host-based IDS requires small programs (or agents) to be installed on individual systems to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. A host-based IDS can only monitor the individual host systems on which the agents are installed; it doesn't monitor the entire network.
Knowledge-based and behavior-based IDS

A knowledge-based (or signature-based) IDS references a database of previous attack profiles and known system vulnerabilities to identify active intrusion attempts. Knowledge- based IDS is currently more common than behavior-based IDS.

Advantages of knowledge-based systems include the following:

It has lower false alarm rates than behavior-based IDS.

Alarms are more standardized and more easily understood than behavior-based IDS.
Disadvantages of knowledge-based systems include these:
Signature database must be continually updated and maintained. New, unique, or original attacks may not be detected or may be improperly classified.

A behavior-based (or statistical anomaly-based) IDS references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered.

Advantages of behavior-based systems include that they Dynamically adapt to new, unique, or original attacks. Are less dependent on identifying specific operating system vulnerabilities.

Disadvantages of behavior-based systems include

Higher false alarm rates than knowledge-based IDSes. Usage patterns that may change often and may not be static enough to implement an effective behavior-based IDS.

QUESTION 435
What is the primary goal of setting up a honeypot?

A. To lure hackers into attacking unused systems
B. To entrap and track down possible hackers
C. To set up a sacrificial lamb on the network
D. To know when certain types of attacks are in progress and to learn about attack techniques so the network can be fortified.

Correct Answer: D
Explanation:
The primary purpose of a honeypot is to study the attack methods of an attacker for the purposes of understanding their methods and improving defenses.

"To lure hackers into attacking unused systems" is incorrect. Honeypots can serve as decoys but their primary purpose is to study the behaviors of attackers.

"To entrap and track down possible hackers" is incorrect. There are a host of legal issues around enticement vs entrapment but a good general rule is that entrapment is generally prohibited and evidence gathered in a scenario that could be considered as "entrapping" an attacker would not be admissible in a court of law.

"To set up a sacrificial lamb on the network" is incorrect. While a honeypot is a sort of sacrificial lamb and may attract attacks that might have been directed against production systems, its real purpose is to study the methods of attackers with the goals of better understanding and improving network defenses.

References
AIO3, p. 213

QUESTION 436
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?

A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System (IMS)
D. Compliance Monitoring System

Correct Answer: A
Explanation:
An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's system security policy have taken place.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 437
What setup should an administrator use for regularly testing the strength of user passwords?

A. A networked workstation so that the live password database can easily be accessed by the cracking program.
B. A networked workstation so the password database can easily be copied locally and processed by the cracking program.
C. A standalone workstation on which the password database is copied and processed by the cracking program.
D. A password-cracking program is unethical; therefore it should not be used.

Correct Answer: C
Explanation:
Poor password selection is frequently a major security problem for any system's security. Administrators should obtain and use password-guessing programs frequently to identify those users having easily guessed passwords.

Because password-cracking programs are very CPU intensive and can slow the system on which it is running, it is a good idea to transfer the encrypted passwords to a standalone (not networked) workstation. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system.

Out of the four choice presented above this is the best choice. However, in real life you would have strong password policies that enforce complexity requirements and does not let the user choose a simple or short password that can be easily cracked or guessed. That would be the best choice if it was one of the choice presented.

Another issue with password cracking is one of privacy. Many password cracking tools can avoid this by only showing the password was cracked and not showing what the password actually is. It is masking the password being used from the person doing the cracking.

Source: National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 8.

QUESTION 438
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance
B. deterrence
C. prevention
D. detection

Correct Answer: D
Explanation:
By reviewing system logs you can detect events that have occured.

The following answers are incorrect:

avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything.
deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred.
prevention. This is incorrect because system logs are a history of past events. You cannot

prevent something that has already occurred.

QUESTION 439
Which of the following tools is less likely to be used by a hacker?

A. l0phtcrack
B. Tripwire
C. OphCrack
D. John the Ripper

Correct Answer: B
Explanation:
Tripwire is an integrity checking product, triggering alarms when important files (e.g. system or configuration files) are modified.

This is a tool that is not likely to be used by hackers, other than for studying its workings in order to circumvent it.

Other programs are password-cracking programs and are likely to be used by security administrators as well as by hackers. More info regarding Tripwire available on the Tripwire, Inc. Web Site.

NOTE:
The biggest competitor to the commercial version of Tripwire is the freeware version of Tripwire. You can get the Open Source version of Tripwire at the following URL:
http://sourceforge.net/projects/tripwire/

QUESTION 440
Which of the following is required in order to provide accountability?

A. Authentication
B. Integrity
C. Confidentiality
D. Audit trails

Correct Answer: D
Explanation:
Accountability can actually be seen in two different ways:

1) Although audit trails are also needed for accountability, no user can be accountable for their actions unless properly authenticated.

2) Accountability is another facet of access control. Individuals on a system are responsible for their actions. This accountability property enables system activities to be traced to the proper individuals. Accountability is supported by audit trails that record events on the system and network. Audit trails can be used for intrusion detection and for the reconstruction of past events. Monitoring individual activities, such as keystroke monitoring, should be accomplished in accordance with the company policy and appropriate laws. Banners at the log-on time should notify the user of any monitoring that is being conducted.

The point is that unless you employ an appropriate auditing mechanism, you don't have accountability. Authorization only gives a user certain permissions on the network. Accountability is far more complex because it also includes intrusion detection, unauthorized actions by both unauthorized users and authorized users, and system faults. The audit trail provides the proof that unauthorized modifications by both authorized and unauthorized users took place. No proof, No accountability.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 50.

The Shon Harris AIO book, 4th Edition, on Page 243 also states:

Auditing Capabilities ensures users are accountable for their actions, verify that the secutiy policies are enforced,
and can be used as investigation tools. Accountability is tracked by recording user, system, and application activities.
This recording is done through auditing functions and mechanisms within an operating sytem or application.
Audit trail contain information about operating System activities, application events, and user actions.

QUESTION 441
Which protocol is NOT implemented in the Network layer of the OSI Protocol Stack?

A. hyper text transport protocol
B. Open Shortest Path First
C. Internet Protocol
D. Routing Information Protocol

Correct Answer: A
Explanation:
Open Shortest Path First, Internet Protocol, and Routing Information Protocol are all protocols implemented in the Network Layer.
Domain: Telecommunications and Network Security

References:
AIO 3rd edition. Page 429
Official Guide to the CISSP CBK. Page 411

QUESTION 442
Which of the following is not a preventive operational control?

A. Protecting laptops, personal computers and workstations.
B. Controlling software viruses.
C. Controlling data media access and disposal.
D. Conducting security awareness and technical training.

Correct Answer: D
Explanation:
Conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behaviour and their responsibilities in protecting the organization's mission is an example of a preventive management control, therefore not an operational control.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 37).