QUESTION 464

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished:

- A. through access control mechanisms that require identification and authentication and through the audit function.
- B. through logical or technical controls involving the restriction of access to systems and the protection of information.
- C. through logical or technical controls but not involving the restriction of access to systems and the protection of information.
- D. through access control mechanisms that do not require identification and authentication and do not operate through the audit function.

Correct Answer: A

Explanation:

Controls provide accountability for individuals who are accessing sensitive information. This accountability is accomplished through access control mechanisms that require identification and authentication and through the audit function. These controls must be in accordance with and accurately represent the organization's security policy. Assurance procedures ensure that the control mechanisms correctly implement the security policy for the entire life cycle of an information system.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

QUESTION 465

Which of the following is NOT a valid reason to use external penetration service firms rather than corporate resources?

- A. They are more cost-effective
- B. They offer a lack of corporate bias
- C. They use highly talented ex-hackers
- D. They ensure a more complete reporting

Correct Answer: C

Explanation:

Two points are important to consider when it comes to ethical hacking:

integrity and independence.

By not using an ethical hacking firm that hires or subcontracts to ex-hackers of others who have criminal records, an entire subset of risks can be avoided by an organization. Also, it is not cost-effective for a single firm to fund the effort of the ongoing research and development, systems development, and maintenance that is needed to operate state-of- the-art proprietary and open source testing tools and techniques.

External penetration firms are more effective than internal penetration testers because they are not influenced by any previous system security decisions, knowledge of the current system environment, or future system security plans. Moreover, an employee performing penetration testing might be reluctant to fully report security gaps.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Appendix F: The Case for Ethical

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html Hacking (page 517).

QUESTION 466

Which of the following monitors network traffic in real time?

- A. network-based IDS
- B. host-based IDS
- C. application-based IDS
- D. firewall-based IDS

Correct Answer: A

Explanation:

This type of IDS is called a network-based IDS because monitors network traffic in real time. 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 467

Which of the following would assist the most in Host Based intrusion detection?

- A. audit trails.
- B. access control lists.
- C. security clearances
- D. host-based authentication

Correct Answer: A

Explanation:

To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

QUESTION 468

Which of the following statements pertaining to ethical hacking is incorrect?

- A. An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services.
- B. Testing should be done remotely to simulate external threats.
- C. Ethical hacking should not involve writing to or modifying the target systems negatively.
- D. Ethical hackers never use tools that have the potential of affecting servers or services.

Correct Answer: D

Explanation:

This means that many of the tools used for ethical hacking have the potential of exploiting vulnerabilities and causing disruption to IT system. It is up to the individuals performing the tests to be familiar with their use and to make sure that no such disruption can happen or at least should be avoided.

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As https://www.ensurepass.com/SSCP.html

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

The first step before sending even one single packet to the target would be to have a signed agreement with clear rules of engagement and a signed contract. The signed contract explains to the client the associated risks and the client must agree to them before you even send one packet to the target range. This way the client understand that some of the test could lead to interruption of service or even crash a server. The client signs that he is aware of such risks and willing to accept them.

The following are incorrect answers:

An organization should use ethical hackers who do not sell auditing, hardware, software, firewall, hosting, and/or networking services. An ethical hacking firm's independence can be questioned if they sell security solutions at the same time as doing testing for the same client. There has to be independence between the judge (the tester) and the accuse (the client).

Testing should be done remotely to simulate external threats Testing simulating a cracker from the Internet is often time one of the first test being done, this is to validate perimeter security. By performing tests remotely, the ethical hacking firm emulates the hacker's approach more realistically.

Ethical hacking should not involve writing to or modifying the target systems negatively. Even though ethical hacking should not involve negligence in writing to or modifying the target systems or reducing its response time, comprehensive penetration testing has to be performed using the most complete tools available just like a real cracker would.

Reference(s) used for this question:

KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Appendix F: The Case for Ethical Hacking (page 520).

QUESTION 469

Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered. There are two basic IDS analysis methods that exists. Which of the basic method is more prone to false positive?

- A. Pattern Matching (also called signature analysis)
- B. Anomaly Detection
- C. Host-based intrusion detection
- D. Network-based intrusion detection

Correct Answer: B

Explanation:

Several analysis methods can be employed by an IDS, each with its own strengths and weaknesses, and their applicability to any given situation should be carefully considered.

There are two basic IDS analysis methods:

- 1. Pattern Matching (also called signature analysis), and
- 2. Anomaly detection

PATTERN MATCHING

Some of the first IDS products used signature analysis as their detection method and simply looked for known characteristics of an attack (such as specific packet sequences or text in the data stream) to produce an alert if that pattern was detected. If a new or different attack vector is used, it will not match a known signature and, thus, slip past the IDS.

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As

https://www.ensurepass.com/SSCP.html

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

ANOMALY DETECTION

Alternately, anomaly detection uses behavioral characteristics of a system's operation or network traffic to draw conclusions on whether the traffic represents a risk to the network or host. Anomalies may include but are not limited to:

Multiple failed log-on attempts Users logging in at strange hours Unexplained changes to system clocks Unusual error messages Unexplained system shutdowns or restarts Attempts to access restricted files

An anomaly-based IDS tends to produce more data because anything outside of the expected behavior is reported. Thus, they tend to report more false positives as expected behavior patterns change. An advantage to anomaly-based IDS is that, because they are based on behavior identification and not specific patterns of traffic, they are often able to detect new attacks that may be overlooked by a signature-based system. Often information from an anomaly-based IDS may be used to create a pattern for a signature-based IDS.

Host Based Intrusion Detection (HIDS)

HIDS is the implementation of IDS capabilities at the host level. Its most significant difference from NIDS is that related processes are limited to the boundaries of a single-host system. However, this presents advantages in effectively detecting objectionable activities because the IDS process is running directly on the host system, not just observing it from the network. This offers unfettered access to system logs, processes, system information, and device information, and virtually eliminates limits associated with encryption. The level of integration represented by HIDS increases the level of visibility and control at the disposal of the HIDS application.

Network Based Intrustion Detection (NIDS)

NIDS are usually incorporated into the network in a passive architecture, taking advantage of promiscuous mode access to the network. This means that it has visibility into every packet traversing the network segment. This allows the system to inspect packets and monitor sessions without impacting the network or the systems and applications utilizing the network.

Below you have other ways that instrusion detection can be performed:

Stateful Matching Intrusion Detection

Stateful matching takes pattern matching to the next level. It scans for attack signatures in the context of a stream of traffic or overall system behavior rather than the individual packets or discrete system activities. For example, an attacker may use a tool that sends a volley of valid packets to a targeted system. Because all the packets are valid, pattern matching is nearly useless. However, the fact that a large volume of the packets was seen may, itself, represent a known or potential attack pattern. To evade attack, then, the attacker may send the packets from multiple locations with long wait periods between each transmission to either confuse the signature detection system or exhaust its session timing window. If the IDS service is tuned to record and analyze traffic over a long period of time it may detect such an attack. Because stateful matching also uses signatures, it too must be updated regularly and, thus, has some of the same limitations as pattern matching.

Statistical Anomaly-Based Intrusion Detection

The statistical anomaly-based IDS analyzes event data by comparing it to typical, known, or predicted traffic profiles in an effort to find potential security breaches. It attempts to identify suspicious behavior by analyzing event data and identifying patterns of entries that deviate from a predicted norm. This type of detection method can be very effective and, at a very high level,

SSCP Exam Dumps SSCP PDF Dumps SSCP VCE Dumps SSCP Q&As

https://www.ensurepass.com/SSCP.html

Download Full Version SSCP Exam Dumps(Updated in Feb/2023)

begins to take on characteristics seen in IPS by establishing an expected baseline of behavior and acting on divergence from that baseline. However, there are some potential issues that may surface with a statistical IDS. Tuning the IDS can be challenging and, if not performed regularly, the system will be prone to false positives. Also, the definition of normal traffic can be open to interpretation and does not preclude an attacker from using normal activities to penetrate systems. Additionally, in a large, complex, dynamic corporate environment, it can be difficult, if not impossible, to clearly define "normal" traffic. The value of statistical analysis is that the system has the potential to detect previously unknown attacks. This is a huge departure from the limitation of matching previously known signatures. Therefore, when combined with signature matching technology, the statistical anomaly-based IDS can be very effective.

Protocol Anomaly-Based Intrusion Detection

A protocol anomaly-based IDS identifies any unacceptable deviation from expected behavior based on known network protocols. For example, if the IDS is monitoring an HTTP session and the traffic contains attributes that deviate from established HTTP session protocol standards, the IDS may view that as a malicious attempt to manipulate the protocol, penetrate a firewall, or exploit a vulnerability. The value of this method is directly related to the use of well-known or well-defined protocols within an environment. If an organization primarily uses well-known protocols (such as HTTP, FTP, or telnet) this can be an effective method of performing intrusion detection. In the face of custom or nonstandard protocols, however, the system will have more difficulty or be completely unable to determine the proper packet format. Interestingly, this type of method is prone to the same challenges faced by signature-based IDSs. For example, specific protocol analysis modules may have to be added or customized to deal with unique or new protocols or unusual use of standard protocols. Nevertheless, having an IDS that is intimately aware of valid protocol use can be very powerful when an organization employs standard implementations of common protocols.

Traffic Anomaly-Based Intrusion

Detection A traffic anomaly-based IDS identifies any unacceptable deviation from expected behavior based on actual traffic structure. When a session is established between systems, there is typically an expected pattern and behavior to the traffic transmitted in that session. That traffic can be compared to expected traffic conduct based on the understandings of traditional system interaction for that type of connection. Like the other types of anomaly-based IDS, traffic anomaly-based IDS relies on the ability to establish "normal" patterns of traffic and expected modes of behavior in systems, networks, and applications. In a highly dynamic environment it may be difficult, if not impossible, to clearly define these parameters.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3664-3686). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3711-3734). Auerbach Publications. Kindle Edition. Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 3694-3711). Auerbach Publications. Kindle Edition.

QUESTION 470

Which of the following would NOT violate the Due Diligence concept?

- A. Security policy being outdated
- B. Data owners not laying out the foundation of data protection
- C. Network administrator not taking mandatory two-week vacation as planned
- D. Latest security patches for servers being installed as per the Patch Management process

https://www.ensurepass.com/SSCP.html