Computer Hacking Forensics Investigator

ECCouncil 312-50 Dumps Available Here at:

https://www.certification-questions.com/eccouncil-exam/312-50-dumps.html

Enrolling now you will get access to 502 questions in a unique set of 312-50 dumps

Question 1

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

Options:

A. Fast processor to help with network traffic analysis

B. They must be dual-homed

C. Similar RAM requirements

D. Fast network interface cards

Answer: B

Explanation:
Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.
References: https://en.wikipedia.org/wiki/Dual-homed

Question 2

Which of the following is an application that requires a host application for replication?

Options:

A. Micro

B. Worm

C. Trojan

D. Virus

Answer: D

Explanation:
Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing it self or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".
References: https://en.wikipedia.org/wiki/Computer_virus

Question 3

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

Options:

A. Paros Proxy

B. BBProxy

C. BBCrack

D. Blooover

Answer: B

Explanation:
Blackberry users warned of hacking tool threat.
Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.
References: http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

Question 4

Which statement is TRUE regarding network firewalls preventing Web Application attacks?

Options:

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.

C. Network firewalls can prevent attacks if they are properly configured.

D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Explanation:
Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.
References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

Question 5

Which of the following programs is usually targeted at Microsoft Office products?

Options:

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

Answer: C

Explanation:
A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.
References: https://en.wikipedia.org/wiki/Macro_virus

Question 6

Bluetooth uses which digital modulation technique to exchange information between paired devices?

Options:

A. PSK (phase-shift keying)

B. FSK (frequency-shift keying)

C. ASK (amplitude-shift keying)

D. QAM (quadrature amplitude modulation)

Answer: A

Explanation:
Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: Ï€/4 DQPSK, and 8DPSK.
References: http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php

Question 7

In order to show improvement of security over time, what must be developed?

Options:

A. Reports

B. Testing tools

C. Metrics

D. Taxonomy of vulnerabilities

Answer: C

Explanation:
Today, management demands metrics to get a clearer view of security.
Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.
References: http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html

Question 8

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

Options:

A. Restore a random file.

B. Perform a full restore.

C. Read the first 512 bytes of the tape.

D. Read the last 512 bytes of the tape.

Answer: B

Explanation:
A full restore is required.

Question 9

Passive reconnaissance involves collecting information through which of the following?

Options:

A. Social engineering

B. Network traffic sniffing

C. Man in the middle attacks

D. Publicly accessible sources

Answer: D

Question 10

How can rainbow tables be defeated?

Options:

A. Password salting

B. Use of non-dictionary words

C. All uppercase character passwords

D. Lockout accounts under brute force password cracking attempts

Answer: A