EC-Council Network Security Administrator (ENSA)

ECCouncil 312-38

Version Demo

Total Demo Questions: 20

Total Premium Questions: 563

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

QUESTION NO: 1

Network security is the specialist area, which consists of the provisions and policies adopted by the Network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. For which of the following reasons is network security needed? Each correct answer represents a complete solution. Choose all that apply.

A. To protect information from loss and deliver it to its destination properly

B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users

C. To protect private information on the Internet

D. To prevent a user from sending a message to another user with the name of a third person

ANSWER: A B C D

Explanation:

Network security is needed for the following reasons:

To protect private information on the Internet

To protect information from unwanted editing, accidentally or intentionally by unauthorized users

To protect information from loss and deliver it to its destination properly

To prevent a user from sending a message to another user with the name of a third person

QUESTION NO: 2

Which of the following statements are true about IPv6 network? Each correct answer represents a complete solution. Choose all that apply.

A. It uses a longer subnet masks as those used for IPv4.

B. The interoperability, the IPv4 addresses using the last 32 bits of the IPv6 address.

C. It provides enhanced authentication and security.

D. It uses 128-bit addresses.

E. It's more of available IP addresses.

ANSWER: B C D E

QUESTION NO: 3

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

„It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.“

Which of the following tools is John using to crack the wireless encryption keys?

A. Cain

B. PsPasswd

C. Kismet

D. AirSnort

ANSWER: D

Explanation:

AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.

Answer option C is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets

To detect standard named networks

To detect masked networks

To collect the presence of non-beaconing networks via data traffic Answer option A is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:

Dictionary attack

Brute force attack

Rainbow attack

Hybrid attack

Answer option B is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:

pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

QUESTION NO: 4

Which type of firewall consists of three interfaces and allows further subdivision of the systems based on specific security objectives of the organization?

A. Screened subnet

B. Bastion host

C. Unscreened subnet

D. Multi-homed firewall

ANSWER: D

QUESTION NO: 5

Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

A. They need to use Nessus.

B. Snort is the best tool for their situation.

C. They could use Tripwire.

D. They can implement Wireshark.

ANSWER: C

QUESTION NO: 6

Which of the following protocols is used for E-mail?

A. TELNET

B. MIME

C. SSH

D. SMTP

ANSWER: D

QUESTION NO: 7

Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.

A. Message replay

B. Identity theft

C. Message modification

D. Message digest

E. Message repudiation

F. Eavesdropping

G. False message

ANSWER: A B C E F G

Explanation:

Following are the common security problems involved in communications and email:

Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.

Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages. These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.

Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.

False message: It the act of constructing messages that appear to be sent by someone else.

Message replay: In a message replay, messages are modified, saved, and re-sent later.

Message repudiation: In message repudiation, normal email messages can be forged. There is no way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.

Answer option D is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.

QUESTION NO: 8

Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.

A. Read-Only Memory (ROM) is an example of volatile memory.

B. The content is stored permanently, and even the power supply is switched off.

C. The volatile storage device is faster in reading and writing data.

D. It is computer memory that requires power to maintain the stored information.

ANSWER: C D

Explanation:

Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

QUESTION NO: 9

Which of the following is a Cisco product that performs VPN and firewall functions?

A. Circuit-Level Gateway

B. PIX Firewall

C. IP Packet Filtering Firewall

D. Application Level Firewall

ANSWER: B

QUESTION NO: 10

Which of the following things need to be identified during attack surface visualization?

A. Attacker's tools, techniques, and procedures

B. Authentication, authorization, and auditing in networks

C. Regulatory frameworks, standards and, procedures for organizations

D. Assets, topologies, and policies of the organization

ANSWER: A

QUESTION NO: 11

You just set up a wireless network to customers in the cafe. Which of the following are good security measures implemented? Each correct answer represents a complete solution. Choose all that apply.

A. WEP encryption

B. WPA encryption

C. Not broadcasting the SSID

D. The MAC-filtering router

ANSWER: A B

QUESTION NO: 12

Which of the following statements are true about security risks? Each correct answer represents a complete solution. (Choose three.)

A. They are considered an indicator of threats coupled with vulnerability.

B. They can be removed completely by taking proper actions.

C. They can be analyzed and measured by the risk analysis process.

D. They can be mitigated by reviewing and taking responsible actions based on possible risks.

ANSWER: A C D

Explanation:

In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the

organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process.

Answer option B is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

QUESTION NO: 13

Fargo, head of network defense at Globadyne Tech, has discovered an undesirable process in several Linux systems, which causes machines to hang every 1 hour. Fargo would like to eliminate it; what command should he execute?

A. # update-rc.d -f [service name] remove

B. # service [service name] stop

C. # ps ax | grep [Target Process]

D. # kill -9 [PID]

ANSWER: D

QUESTION NO: 14

Which of the Windows security component is responsible for controlling access of a user to Windows resources?

A. Network Logon Service (Netlogon)

B. Security Accounts Manager (SAM)

C. Security Reference Monitor (SRM)

D. Local Security Authority Subsystem (LSASS)

ANSWER: D

QUESTION NO: 15

Which of the following is NOT a WEP authentication method?

A. Kerberos authentication

B. Media access authentication

C. Open system authentication

D. Shared key authentication

ANSWER: A

QUESTION NO: 16

Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile? Each correct answer represents a complete solution. Choose all that apply.

A. Business Continuity Planning

B. Benefit-Cost Analysis

C. Disaster recovery

D. Cost-benefit analysis

ANSWER: B D

Explanation:

Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to: helping to appraise, or assess, the case for a project, program, or policy proposal;

an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis).

Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.

Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

QUESTION NO: 17

Which of the following IP addresses is not reserved for the hosts? Each correct answer represents a complete solution. Choose all that apply.

A. E-Class

B. class D

C. class A

D. B-

ANSWER: A B

QUESTION NO: 18

Assume that you are a network administrator and the company has asked you to draft an Acceptable Use Policy (AUP) for employees. Under which category of an information security policy does AUP fall into?

A. Incident Response Policy (IRP)

B. Issue Specific Security Policy (ISSP)

C. Enterprise Information Security Policy (EISP)

D. System Specific Security Policy (SSSP)

ANSWER: D

QUESTION NO: 19

Management asked their network administrator to suggest an appropriate backup medium for their backup plan that best suits their organization's need. Which of the following factors will the administrator consider when deciding on the appropriate backup medium? (Choose all that apply.)

A. Reliability

B. Capability

C. Accountability

D. Extensibility

ANSWER: A B D

QUESTION NO: 20 - (DRAG DROP)

DRAG DROP

Drag and drop the terms to match with their descriptions.

Select and Place:

	Terms	Description
ASLR	Place Here	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
Hypervisor	Place Here	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
DEP	Place Here	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

ANSWER:

	Terms	Description
ASLR	DEP	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
Hypervisor	ASLR	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
DEP	Hypervisor	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.

Explanation:

Following are the terms with their descriptions:

Terms	Description
DEP	It is a Windows Vista and Windows XP Service Pack 2 (SP2) feature that prevents attackers from using buffer overflow to execute malware.
ASLR	It makes it harder for an attacker to guess where the operating system functionality resides in memory.
Hypervisor	It is a software technology used in virtualization that allows multiple operating systems to share a single hardware host.