Free Questions for GSNA by dumpshq

Shared by Bowman on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He begins to perform a pre-attack test before conducting an attack on the We-are-secure server. Which of the following will John perform in the pre-attack phase?

Each correct answer represents a complete solution. Choose all that apply.

Options:

A- Determining network range

B- Identifying active machines

C- Enumeration

D- Finding open ports and applications

E- Information gathering

Answer:

A, B, D, E

Explanation:

In the pre-attack phase, there are seven steps, which have been defined by the EC-Council, as follows:

1.Information gathering

2.Determining network range

3.Identifying active machines

4.Finding open ports and applications

5.OS fingerprinting

6.Fingerprinting services

7.Mapping the network

Answer C is incorrect. In the enumeration phase, the attacker gathers information such as the network

user and group names, routing

tables, and Simple Network Management Protocol (SNMP) data. The techniques used in this phase are as follows:

1.Obtaining Active Directory information and identifying vulnerable user accounts

2.Discovering NetBIOS names

3.Employing Windows DNS queries

4.Establishing NULL sessions and queries

Question 2

Question Type: MultipleChoice

Sam works as a Network Administrator for SoftTech Inc. The computers in the company run Windows Vista operating system, and they are continuously connected to the Internet. This makes the network of the company susceptible to attacks from unauthorized users. Which of the following will Sam choose to protect the network of the company from such attacks?

Options:

A- Firewall

B- Windows Defender

C- Software Explorer

D- Quarantined items

Answer:

A

Explanation:

A firewall is a set of related programs configured to protect private networks connected to the Internet from intrusion. It is used to regulate the network traffic between different computer networks. It permits or denies the transmission of a network packet to its destination based on a set of rules. A firewall is often installed on a separate computer so that an incoming packet does not get into the network directly.

Answer B is incorrect. Windows Defender is a software product designed by Microsoft to provide continuous security against malware.

If it detects anything suspicious, an alert will appear on the screen. Windows Defender can also be used to scan a computer for suspicious

software. It can remove or quarantine any malware or spyware it finds.

Answer C is incorrect. Software Explorer is a tool of Windows Defender. It is used to remove, enable, or disable the programs running

on a computer.

Answer D is incorrect. Quarantined items is a tool of Windows Defender. It is used to remove or restore a program blocked by Windows

Defender.

Question 3

Question Type: MultipleChoice

You work as the Network Administrator of a Windows 2000 Active Directory network. Your company's offices are at Dallas and New York. Your company wants to configure a secure, direct Internet link. The company's management wants to accomplish the following tasks:

Keep the offices' internal resources secure from outsiders.

Keep communication secure between the two offices.

You install a firewall in each office. Which of the tasks does this action accomplish?

Options:

A- The action taken will fulfill the secure communication concern.

B- The action taken will accomplish neither of the goals.

C- The action taken will fulfill the internal resource security concern.

D- The action taken will accomplish both the goals.

Answer:

C

Explanation:

The action taken will fulfill the internal resource security concern. It has nothing to do with the secured communication.

Firewall is used to protect the network from external attacks by hackers. Firewall prevents direct communication between computers in the

network and the external computers, through the Internet. Instead, all communication is done through a proxy server, outside the

organization's network, which decides whether or not it is safe to let a file pass through.

To achieve the secured communication goal, you will have to configure a virtual private network (VPN) between the two offices.

Question 4

Question Type: MultipleChoice

Which of the following tools can be used to perform ICMP tunneling?

Each correct answer represents a complete solution. Choose two.

Options:

A- Itunnel

B- Ptunnel

C- WinTunnel

D- Ethereal

Answer:

A, B

Explanation:

Ptunnel and Itunnel are the tools that are used to perform ICMP tunneling. In ICMP tunneling, an attacker establishes a covert connection

between two remote computers (a client and proxy), using ICMP echo requests and reply packets. ICMP tunneling works by injecting arbitrary

data into an echo packet sent to a remote computer. The remote computer replies in the same manner, injecting an answer into another ICMP

packet and sending it back. The client performs all communication using ICMP echo request packets, while the proxy uses echo reply packets.

Normally, ICMP tunneling involves sending what appear to be ICMP commands but really they are the Trojan communications.

Answer C is incorrect. WinTunnel is used to perform TCP tunneling.

Answer D is incorrect. Ethereal is a network sniffer.

Question 5

Question Type: **MultipleChoice**

You work as a Network Administrator for ABC Inc. The company needs a secured wireless network. To provide network security to the company, you are required to configure a device that provides the best network perimeter security. Which of the following devices would you use to accomplish the task?

Options:

A- Proxy server

B- IDS

C- Packet filtering firewall

D- honeypot

Answer:

C

Explanation:

Packet filtering firewalls work on the first three layers of the OSI reference model, which means all the work is done between the network and

physical layers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of the packet

filtering rules that are configured in the firewall and drops or rejects the packet accordingly. In a software firewall, packet filtering is done by a

program called a packet filter. The packet filter examines the header of each packet based on a specific set of rules, and on that basis, decides

to prevent it from passing (called DROP) or allow it to pass (called ACCEPT). A packet filter passes or blocks packets at a network interface

based on source and destination addresses, ports, or protocols. The process is used in conjunction with packet mangling and Network

Address Translation (NAT). Packet filtering is often part of a firewall program for protecting a local network from unwanted intrusion. This type

of firewall can be best used for network perimeter security.

Answer B is incorrect. An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

Answer A is incorrect. A proxy server exists between a client's Web-browsing program and a real Internet server. The purpose of the proxy server is to enhance the performance of user requests and filter requests. A proxy server has a database called cache where the most frequently accessed Web pages are stored. The next time such pages are requested, the proxy server is able to suffice the request locally, thereby greatly reducing the access time. Only when a proxy server is unable to fulfill a request locally does it forward the request to a real Internet server. The proxy server can also be used for filtering user requests. This may be done in order to prevent the users from visiting non-genuine sites.

Answer D is incorrect. A honeypot is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner

counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to

be part of a network, but is actually isolated, and monitored, and which seems to contain information or a resource of value to attackers.

Question 6

Question Type: MultipleChoice

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack

tools?

Options:

A- Snort

B- IDS

C- Firewall

D- WIPS

Answer:

D

Explanation:

Wireless intrusion prevention system (WIPS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use

of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator

whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Rogue devices can spoof MAC address of an authorized network device as their own. WIPS uses fingerprinting approach to weed out devices

with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against

the known signatures of pre-authorized, known wireless devices.

Answer B is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can compromise the

security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access to sensitive

data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has

three main components: Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and

to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS

implementations, these three components are combined into a single device. Basically, following two types of IDS are used :

Network-based IDS

Host-based IDS

Answer A is incorrect. Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It

logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including

Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

The three main modes in which Snort can be configured are as follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console.

Packet logger mode: It logs the packets to the disk.

Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set.

Answer C is incorrect. A firewall is a tool to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports.