Free Questions for GCIH by dumpshq

Shared by Calderon on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is used to determine the range of IP addresses that are mapped to a live hosts?

Options:

A- Port sweep

B- Ping sweep

C- IP sweep

D- Telnet sweep

Answer:

B

Question 2

Question Type: MultipleChoice

Which of the following is a process of searching unauthorized modems?

Options:

A- Espionage

B- Wardialing

C- System auditing

D- Scavenging

Answer:

B

Question 3

Question Type: **MultipleChoice**

Which of the following applications is NOT used for passive OS fingerprinting?

Options:

A- Networkminer

B- Satori

C- p0f

D- Nmap

Answer:

D

Question 4

Question Type: **MultipleChoice**

Which of the following are used to identify who is responsible for responding to an incident?

Options:

A- Disaster management policies

B- Incident response manuals

C- Disaster management manuals

D- Incident response policies

Answer:

D

Question 5

Question Type: MultipleChoice

Which of the following ensures that the investigation process of incident response team does not break any laws during the response to an incident?

Options:

A- Information Security representative

B- Lead Investigator

C- Legal representative

D- Human Resource

Answer:

C

Question 6

Question Type: MultipleChoice

Which of the following statements about threats are true?

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

Options:

A- A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.

B- A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

C- A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.

D- A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

Answer:

B, C, D

Question 7

Question Type: MultipleChoice

Which of the following steps can be taken as countermeasures against sniffer attacks?

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

Options:

A- Use encrypted protocols for all communications.

B- Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.

C- Use tools such as StackGuard and Immunix System to avoid attacks.

D- Reduce the range of the network to avoid attacks into wireless networks.

Answer:

A, B, D

Question 8

Question Type: MultipleChoice

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux. The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

Options:

A- Code red

B- Ramen

C- LoveLetter

D- Nimda

Answer:

B

Question 9

Question Type: **MultipleChoice**

Which of the following tools is used for port scanning?

Options:

A- NSLOOKUP

B- NETSH

C- Nmap

D- L0phtcrack

Answer:

C

Question 10

Question Type: MultipleChoice

Which of the following statements about smurf is true?

Options:

A- It is a UDP attack that involves spoofing and flooding.

B- It is an ICMP attack that involves spoofing and flooding.

C- It is an attack with IP fragments that cannot be reassembled.

D- It is a denial of service (DoS) attack that leaves TCP ports open.

Answer:

B

Question 11

Question Type: MultipleChoice

Which of the following is the method of hiding data within another media type such as graphic or document?

Options:

A- Spoofing

B- Steganography

C- Packet sniffing

D- Cryptanalysis

Answer:

B