GCIA Q&As

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gcia.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

Which of the following IP packet elements is responsible for authentication while using IPSec?

A. Internet Key Exchange (IKE)

B. Authentication Header (AH)

C. Layer 2 Tunneling Protocol (L2TP)

D. Encapsulating Security Payload (ESP)

Correct Answer: B

QUESTION 2

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft\\'s Windows XP operating system?

A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

B. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe

C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

D. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe

Correct Answer: D

QUESTION 3

Which of the following tools is described below?

It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses

the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Libnids

C. Cain

D. LIDS

Correct Answer: A

QUESTION 4

A firewall is a combination of hardware and software, used 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. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. Stunnel

B. IPTables

C. IPChains

D. OpenSSH

Correct Answer: B

QUESTION 5

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

A. It is the core routing protocol of the Internet.

B. It allows data to be exchanged using a secure channel between two networked devices.

C. It was designed as a replacement for TELNET and other insecure shells.

D. It is a network protocol used primarily on Linux and Unix based systems.

Correct Answer: BCD

QUESTION 6

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. On the basis of above information, which of the following types of attack is Adam attempting to perform?

A. Fraggle attack

B. SYN Flood attack

C. Land attack

D. Ping of death attack

Correct Answer: D

QUESTION 7

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Risk analysis

B. Cryptography

C. Firewall security

D. OODA loop

Correct Answer: B

QUESTION 8

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

A. It generates a buffer overflow exploit by transforming an attack shell code so that the new attack shell code cannot be recognized by any Intrusion Detection Systems.

B. It records the time taken for a round trip for each packet at each router.

C. It uses ICMP echo packets to display the Fully Qualified Domain Name (FQDN) and the IP address of each gateway along the route to the remote host.

D. It is an online tool that performs polymorphic shell code attacks.

Correct Answer: BC

QUESTION 9

Which of the following log files are used to collect evidences before taking the bit-stream image of the BlackBerry? Each correct answer represents a complete solution. Choose all that apply.

A. user history

B. Transmit/Receive

C. Radio status

D. Roam and Radio

Correct Answer: BCD

QUESTION 10

What are the benefits of creating a new view using role-based CLI?

A. Scalability

B. Operational efficiency

C. Security

D. Availability

Correct Answer: BCD

QUESTION 11

Which of the following UDP ports are used by the Simple Network Management Protocol (SNMP)? Each correct answer represents a complete solution. Choose two.

A. UDP port 69

B. UDP port 161

C. UDP port 137

D. UDP port 162

Correct Answer: BD

QUESTION 12

Which of the following snort keywords is used to match a defined payload value?

A. content

B. ttl

C. id

D. msg

Correct Answer: A

QUESTION 13

Which of the following firewalls inspects the actual contents of packets?

A. Application-level firewall

B. Stateful inspection firewall

C. Packet filtering firewall

D. Circuit-level firewall

Correct Answer: A

QUESTION 14

Which of the following algorithms is used as a default algorithm for ESP extension header in IPv6?

A. Propagating Cipher Block Chaining (PCBC) Mode

B. Cipher Block Chaining (CBC) Mode

C. Electronic Codebook (ECB) Mode

D. Cipher Feedback (CFB) Mode

Correct Answer: B

QUESTION 15

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect\\'s computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, interne t traces

B. Volatile data, file slack, file system, registry, memory dumps, system state backup, interne t traces

C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

Correct Answer: B