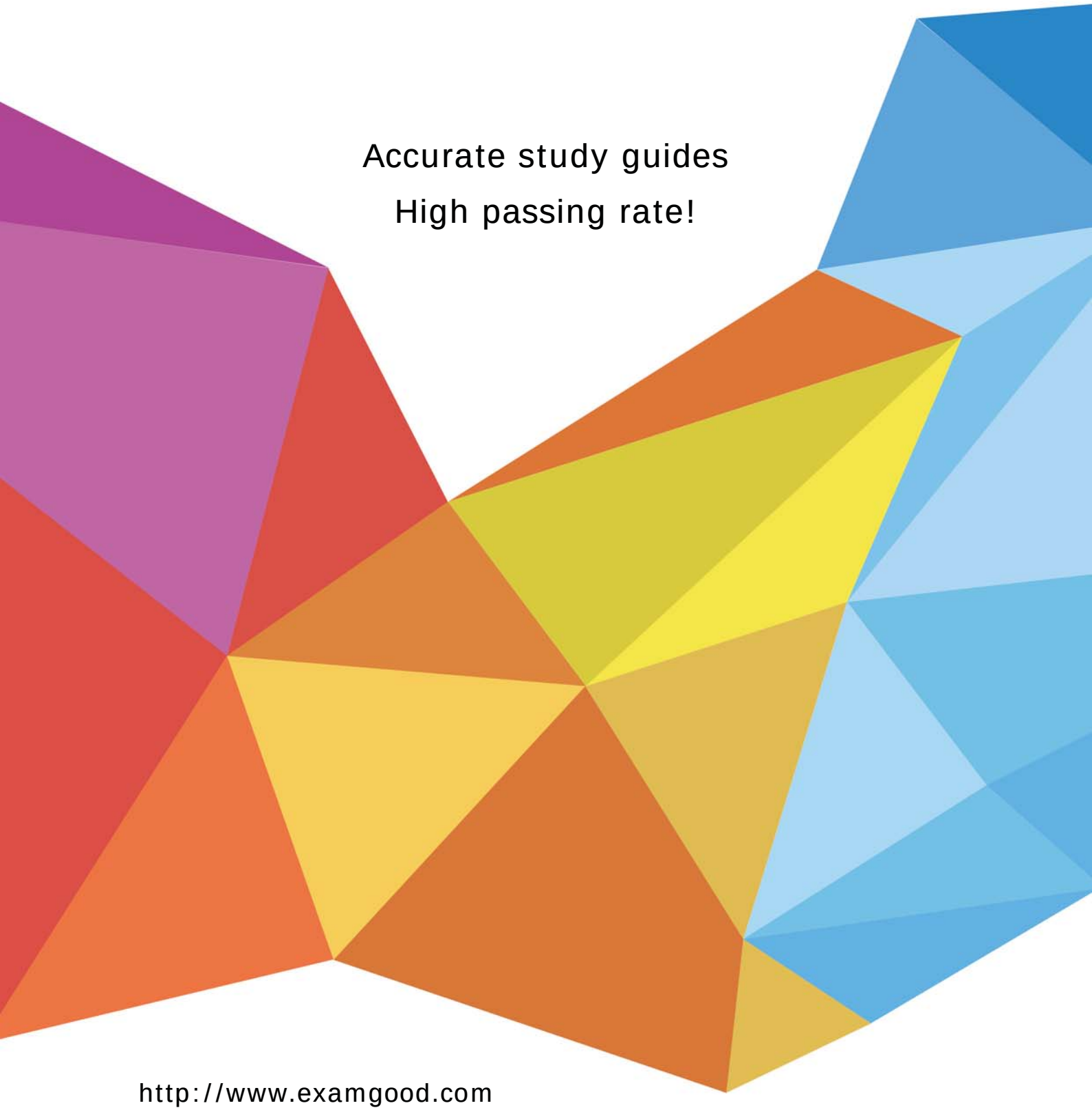
EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!



Accurate study guides

High passing rate!

Exam : **GCIA**

Title : GIAC Certified Intrusion Analyst

Version : Demo

1.Andrew works as a System Administrator for NetPerfect Inc. All client computers on the network run on Mac OS X. The Sales Manager of the company complains that his MacBook is not able to boot. Andrew wants to check the booting process. He suspects that an error persists in the bootloader of Mac OS X. Which of the following is the default bootloader on Mac OS X that he should use to resolve the issue?
A. LILO
B. BootX
C. NT Loader
D. GRUB
Answer: B

2.Sasha wants to add an entry to your DNS database for your mail server. Which of the following types of resource records will she use to accomplish this.?
A. ANAME
B. SOA
C. MX
D. CNAME
Answer: C

3.John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Dictionary attack
B. Hybrid attack
C. Brute Force attack
D. Rule based attack
Answer: A,B,C

4.Which of the following proxy servers is also referred to as transparent proxies or forced proxies?
A. Tunneling proxy server
B. Reverse proxy server
C. Anonymous proxy server
D. Intercepting proxy server
Answer: D

5.Which of the following statements about a host-based intrusion prevention system (HIPS) are true?
Each correct answer represents a complete solution. Choose two.
A. It can detect events scattered over the network.
B. It can handle encrypted and unencrypted traffic equally.
C. It cannot detect events scattered over the network.
D. It is a technique that allows multiple computers to share one or more IP addresses.
Answer: B,C

6.Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet.

Which of the following security threats may occur if DMZ protocol attacks are performed?
Each correct answer represents a complete solution. Choose all that apply.
A. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.
B. Attacker can gain access to the Web server in a DMZ and exploit the database.
C. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.
D. Attacker can exploit any protocol used to go into the internal network or intranet of the com pany
Answer: A,B,D

7.Which of the following is known as a message digest?
A. Hash function
B. Hashing algorithm
C. Spider
D. Message authentication code
Answer: A

8.Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc.
Which of the following types of Cross-Site Scripting attack Ryan intends to do?
A. Document Object Model (DOM)
B. Non persistent
C. SAX
D. Persistent
Answer: D

9.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
Answer: B

10.You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?
A. Enable verbose logging on the firewall
B. Install a network-based IDS

C. Install a DMZ firewall
D. Install a host-based IDS
Answer: B

11.Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server. Which of the following files will he review to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.
A. Checkpoint files
B. EDB and STM database files
C. Temporary files
D. cookie files
Answer: A,B,C

12.This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows: -It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc. -It is commonly used for the following purposes:
A. War driving
B. Detecting unauthorized access points
C. Detecting causes of interference on a WLAN
D. WEP ICV error tracking
E. Making Graphs and Alarms on 802.11 Data, including Signal Strength
Answer: D

13.SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?
Each correct answer represents a complete solution. Choose all that apply.
A. Blowfish
B. IDEA
C. DES
D. RC4
Answer: A,B,C

14.Adam works as a Security Analyst for Umbrella Inc. He is performing real-time traffic analysis on IP networks using Snort. Adam is facing problems in analyzing intrusion data. Which of the following software combined with Snort can Adam use to get a visual representation of intrusion data?
Each correct answer represents a complete solution. Choose all that apply.
A. Basic Analysis and Security Engine (BASE)
B. sguil
C. KFSensor
D. OSSIM
Answer: A,B,D

15.Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past. Which of the following statements are true about external threats?
Each correct answer represents a complete solution. Choose three.
A. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.
B. These are the threats that originate from within the organization.
C. These are the threats intended to flood a network with large volumes of access requests.
D. These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.
Answer: A,C,D

16.Which of the following file systems is designed by Sun Microsystems?
A. NTFS
B. CIFS
C. ZFS
D. ext2
Answer: C

17.You work as a Network Administrator for Tech Perfect Inc. The office network is configured as an IPv6 network. You have to configure a computer with the IPv6 address, which is equivalent to an IPv4 publicly routable address. Which of the following types of addresses will you choose?
A. Site-local
B. Global unicast
C. Local-link
D. Loopback
Answer: B

18.Which of the following is the default port for Simple Network Management Protocol (SNMP)?
A. TCP port 110
B. TCP port 25
C. TCP port 80
D. UDP port 161
Answer: D

19.Which of the following statements are true about snort?
Each correct answer represents a complete solution. Choose all that apply.
A. It develops a new signature to find vulnerabilities.
B. It detects and alerts a computer user when it finds threats such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, well-known backdoors and system vulnerabilities, and DDoS clients.
C. It encrypts the log file using the 256 bit AES encryption scheme algorithm.
D. It is used as a passive trap to record the presence of traffic that should not be found on a network, such

as NFS or Napster connections.
Answer: A,B,D

20.Allen works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a computer, which is used by the suspect to sexually harass the victim using instant messenger program. Suspect's computer runs on Windows operating system. Allen wants to recover password from instant messenger program, which suspect is using, to collect the evidence of the crime. Allen is using Helix Live for this purpose. Which of the following utilities of Helix will he use to accomplish the task?
A. Asterisk Logger
B. Access PassView
C. Mail Pass View
D. MessenPass
Answer: D

21.Which of the following tools are used to determine the hop counts of an IP packet?
Each correct answer represents a complete solution. Choose two.
A. TRACERT
B. Ping
C. IPCONFIG
D. Netstat
Answer: A,B

22.Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?
Each correct answer represents a complete solution. Choose all that apply.
A. All ideas present in the investigative report should flow logically from facts to conclusions.
B. Opinion of a lay witness should be included in the investigative report.
C. The investigative report should be understandable by any reader.
D. There should not be any assumptions made about any facts while writing the investigative report.
Answer: A,C,D

23.Which of the following can be applied as countermeasures against DDoS attacks?
Each correct answer represents a complete solution. Choose all that apply.
A. Limiting the amount of network bandwidth.
B. Blocking IP address.
C. Using LM hashes for passwords.
D. Using Intrusion detection systems.
E. Using the network-ingress filtering.
Answer: A,B,D,E

24.Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?
A. FAU
B. FTK Imager
C. Galleta
D. Device Seizure
Answer: D

25.Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except ports that must be used.
He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about programs like Hping2 that can get into a network through covert channels.
Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?
A. Block ICMP type 13 messages
B. Block all outgoing traffic on port 21
C. Block all outgoing traffic on port 53
D. Block ICMP type 3 messages
Answer: A

26.Which of the following tools performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs?
A. Dsniff
B. Snort
C. Nikto
D. Sniffer
Answer: C

27.Which of the following methods is a behavior-based IDS detection method?
A. Knowledge-based detection
B. Protocol detection
C. Statistical anomaly detection
D. Pattern matching detection
Answer: C

28.You work as a Network Administrator for McNeil Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) Server 2000. You want to configure intrusion detection on the server. You find that the different types of attacks on the Intrusion Detection tab page of the IP Packet Filters Properties dialog box are disabled. What is the most likely cause?

A. The PPTP through ISA firewall check box on the PPTP tab page of the IP Packet Filters Properties dialog box is not enabled.
B. The Enable IP routing check box on the General tab page of the IP Packet Filters Properties dialog box is not selected.
C. The Log packets from Allow filters check box on the Packet Filters tab page of the IP Packet Filters Properties dialog box is not enabled.
D. The Enable Intrusion detection check box on the General tab page of the IP Packet Filters Properties dialog box is not selected.
Answer: D

29.Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?
A. Command injection attack
B. Code injection attack
C. Cross-Site Request Forgery
D. Cross-Site Scripting attack
Answer: B

30.You work as a Network Administrator for Tech Perfect Inc. Your company has a Windows 2000based network. You want to verify the connectivity of a host in the network. Which of the following utilities will you use?
A. PING
B. TELNET
C. NETSTAT
D. TRACERT
Answer: A