GCFW

GIAC

GIAC Certified Firewall Analyst

The GCFW practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The GCFW Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently.
The GCFW exam is very challenging, but with our GCFW questions and answers practice exam, you can feel confident in obtaining your success on the GCFW exam on your FIRST TRY!

GIAC GCFW Exam Features

- Detailed questions and answers for GCFW exam
- Try a demo before buying any GIAC exam
- GCFW questions and answers, updated regularly
- Verified GCFW answers by Experts and bear almost 100% accuracy
- GCFW tested and verified before publishing
- GCFW examcollection vce questions with exhibits
- GCFW same questions as real exam with multiple choice options

Acquiring GIAC certifications are becoming a huge task in the field of I.T. More over these exams like GCFW exam are now continuously updating and accepting this challenge is itself a task. This GCFW test is an important part of GIAC certifications. We have the resources to prepare you for this. The GCFW exam is essential and core part of GIAC certifications and once you clear the exam you will be able to solve the real life problems yourself.Want to take advantage of the Real GCFW Test and save time and money while developing your skills to pass your GIAC GCFW Exam? Let us help you climb that ladder of success and pass your GCFW now!

QUESTION: 1
Which of the following can be monitored by using the host intrusion detection system (HIDS)? Each correct answer represents a complete solution. Choose two.

A. Computer performance
B. File system integrity
C. Storage space on computers
D. System files

Answer: B, D

QUESTION: 2
Which of the following components are usually found in an Intrusion detection system (IDS)? Each correct answer represents a complete solution. Choose two.

A. Firewall
B. Console
C. Gateway
D. Modem
E. Sensor

Answer: B, E

QUESTION: 3
Which of the following are the countermeasures against a man-in-the-middle attack? Each correct answer represents a complete solution. Choose all that apply.

A. Using Secret keys for authentication.
B. Using public key infrastructure authentication.
C. Using Off-channel verification.
D. Using basic authentication.

Answer: A, B, C

QUESTION: 4
Which of the following ICMPv6 neighbor discovery messages is sent by hosts to request an immediate router advertisement, instead of waiting for the next scheduled advertisement?

A. Router Advertisement
B. Neighbor Advertisement
C. Router Solicitation
D. Neighbor Solicitation

Answer: C

QUESTION: 5
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 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.
C. It records the time taken for a round trip for each packet at each router.
D. It is an online tool that performs polymorphic shell code attacks.

Answer: B, C

QUESTION: 6
Which of the following intrusion detection systems (IDS) monitors network traffic and compares it against an established baseline?

A. Network-based
B. File-based
C. Signature-based
D. Anomaly-based

Answer: D

QUESTION: 7
You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP network. You have been assigned a task to configure security mechanisms for the network of the company. You have decided to configure a packet filtering firewall. Which of the following may be the reasons that made you choose a packet

filtering firewall as a security mechanism? Each correct answer represents a complete solution. Choose all that apply.

A. It makes security transparent to end-users which provide easy use of the client application s.
B. It prevents application-layer attacks.
C. It is easy to install packet filtering firewalls in comparison to the other network security sol utions.
D. It easily matches most of the fields in Layer 3 packets and Layer 4 segment headers, and thus, provides a lot of flexibility in implementing security policies.

Answer: A, C, D

QUESTION: 8
Which of the following types of Intrusion Detection Systems consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state?

A. HIDS
B. NIDS
C. APIDS
D. PIDS

Answer: A

QUESTION: 9
A packet filtering firewall inspects each packet passing through the network and accepts or rejects it based on user-defined rules. Based on which of the following information are these rules set to filter the packets? Each correct answer represents a complete solution. Choose all that apply.

A. Layer 4 protocol information
B. Actual data in the packet
C. Interface of sent or received traffic
D. Source and destination Layer 3 address

Answer: A, C, D

QUESTION: 10
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 the 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 the 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 ICMP type 3 messages
C. Block all outgoing traffic on port 21
D. Block all outgoing traffic on port 53

Answer: A

QUESTION: 11
You work as a Security Manger for Tech Perfect Inc. The company has a Windows-based network. You want to scroll real-time network traffic to a command console in a readable format. Which of the following command line utilities will you use to accomplish the task?

A. WinPcap
B. WinDump
C. iptables
D. libpcap

Answer: B

QUESTION: 12
Which of the following is the default port for POP3?

A. 25
B. 21
C. 80
D. 110