

**Exam : SCP SC0-451**

**Title : Tactical Perimeter Defense**

**Version : Demo**

## Important Note, Please Read Carefully

### Other VisualExams products

[All visual exams IT Exam Products](#)

### Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[visual exams Testing Engine](#)

### Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at VisualExams and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.visual exams.com/>
2. Log in the **User Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

### Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com). You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

### Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com).

### Features

- Comprehensive questions with complete details
- Instant Downloadable in PDF form.
- Verified Answers Researched by Industry Experts
- Questions accompanied by exhibits.
- Drag and Drop questions as experienced in the Actual Exams.
- These questions and answers are backed by our GUARANTEE.
- Questions updated on regular basis.
- Like actual certification exams our product is in multiple-choice questions (MCQs)

**Commitment to Your Success: At VisualTestExam.com, we are committed to you ongoing success. Our exams and questions are constantly being updated and compared to industry standards.**

Want to earn a Microsoft certification like MCSE, MCSE 2003, CCNA, CCNP? Thinking about getting an A+ or CCSP?

A, CCSP or Network+ Certification with less effort and time. You will be astonished at the theoretical and practical knowledge you will acquire in such a short period of time using our Certification Training Products. Our Study material will enable you to pass your Microsoft, Your Cisco and any other certification on the very first attempt.

## **Guarantee**

Visualexams provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if somehow you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

1. The exhibit represents a simple routed network. Node 7 is a Windows 2000 Professional machine that establishes a TCP communication with Node 10, a Windows 2003 Server. The routers are Cisco 2500 series running IOS 11.2.

While working at Node 10, you run a packet capture. Packets received by Node 10, and sent from Node 7 will reveal which of the following combination of source IP and source Physical addresses:

<Missing>

- A. Source IP address 10.0.10.115, Source Physical address for Node 7
- B. Source IP address 50.0.50.1, Source Physical address for Node 7
- C. Source IP address for Router D's Int E0, Source Physical address for Node 7
- D. Source IP address 10.0.10.115, Source Physical address Router D's Int E0
- E. Source IP addresses for both Nodes 7 and Router D's Int E0, Source Physical address for both Nodes 7 and Router D's Int E0.

**Answer: D**

2. You have implemented an IPSec policy, using only AH. You are analyzing your network traffic in Network Monitor, which of the following statements are true about your network traffic?

- A. You will not be able to view the data in the packets, as it is encrypted.
- B. You will not be able to identify the upper layer protocol.
- C. You will be able to view the unencrypted data in the packets.
- D. You will be able to identify the encryption algorithm in use.
- E. You will not be able to view the packet header.

**Answer: C**

3. In order to perform promiscuous mode captures using the Wireshark capture tool on a Windows Server 2003 machine, what must first be installed?

- A. IPv4 stack
- B. IPv6 stack
- C. WinPcap
- D. Nothing, it will capture by default
- E. At least two network adapters

**Answer: C**

4. You are configuring the rules on your firewall, and need to take into consideration that some clients in the network are using automatic addressing. What is the IP address range reserved for internal use for APIPA in Microsoft networks?

- A. 169.254.0.0 /4
- B. 169.254.0.0 /16
- C. 169.254.0.0 /8
- D. 169.254.0.0 /0
- E. 168.255.0.0 /16

**Answer: B**

5. If you capture an 802.11 frame, and the ToDS bit is set to zero and the FromDS bit is set to zero, what type of WLAN is this frame a part of?

- A. Mesh
- B. Broadcast
- C. Infrastructure
- D. Hierarchical
- E. Ad Hoc

**Answer: E**

6. There are several options available to you for your new wireless networking technologies, and you are examining how different systems function. What transmission system uses short bursts combined together as a channel?

- A. Frequency Hopping Spread Spectrum (FHSS)
- B. Direct Sequence Spread Spectrum (DSSS)
- C. Lamar Anthell Transmission (LAT)
- D. Digital Band Hopping (DBH)
- E. Digital Channel Hopping (DCH)

**Answer: A**

7. You have just installed a new Intrusion Detection System in your network. You are concerned that there are functions this system will not be able to perform. What is a reason an IDS cannot manage hardware failures?

- A. The IDS can only manage RAID 5 failures.
- B. The IDS cannot be programmed to receive SNMP alert messages.
- C. The IDS cannot be programmed to receive SNMP trap messages.
- D. The IDS cannot be programmed to respond to hardware failures.
- E. The IDS can only inform you that an event happened.

**Answer: E**

8. For the new Snort rules you are building, it will be required to have Snort examine inside the content of the packet. Which keyword is used to tell Snort to ignore a defined number of bytes before looking inside the packet for a content match?

- A. Depth
- B. Offset
- C. Nocase
- D. Flow\_Control
- E. Classtype

**Answer: B**

9. You have recently taken over the security of a mid-sized network. You are reviewing the current configuration of the IPTables firewall, and notice the following rule:

```
ipchains -A input -p TCP -d 0.0.0.0/0 12345 -j DENY
```

What is the function of this rule?

- A. This rule for the output chain states that all incoming packets from any host to port 12345 are to be denied.
- B. This rule for the input chain states that all incoming packets from any host to port 12345 are to be denied.
- C. This rule for the input chain states that any TCP traffic from any address destined for any IP address and to port 12345 is to be denied.
- D. This rule for the output chain states that any TCP traffic from any address destined for any IP address

and to port 12345 is to be denied.

E. This rule for the input chain states that all TCP packets inbound from any network destined to any network is to be denied for ports 1, 2, 3, 4, and 5.

**Answer: C**

10. At a policy meeting you have been given the task of creating the firewall policy. What are the two basic positions you can take when creating the policy?

- A. To deny all traffic and permit only that which is required.
- B. To permit only IP traffic and filter TCP traffic
- C. To permit only TCP traffic and filter IP traffic
- D. To permit all traffic and deny that which is required.
- E. To include your internal IP address as blocked from incoming to prevent spoofing.

**Answer: AD**

11. You are planning on implementing a token-based authentication system in your network. The network currently is spread out over four floors of your building. There are plans to add three branch offices. During your research you are analyzing the different types of systems. Which of the following are the two common systems token-based authentication uses?

- A. Challenge/Response
- B. Random-code
- C. Time-based
- D. Challenge/Handshake
- E. Password-Synch

**Answer: AC**

12. During your review of the logs of your Cisco router, you see the following line. What is the meaning of this line?

%SYS-5-CONFIG\_I: Configured from console by vty1 (172.16.10.1)

- A. A normal, but noteworthy event
- B. An informative message

- C. A warning condition has occurred
- D. A debugging message
- E. An error condition has occurred

**Answer: A**

13. You have implemented an IPSec policy, using only AH. You are analyzing your network traffic in Network Monitor, which of the following statements are true about your network traffic?

- A. You will not be able to view the data in the packets, as it is encrypted.
- B. You will not be able to identify the upper layer protocol.
- C. You will be able to view the unencrypted data in the packets.
- D. You will be able to identify the encryption algorithm in use.
- E. You will not be able to view the packet header.

**Answer: C**

14. You are monitoring the network traffic on your Frame-Relay Internet connection. You notice a large amount of unauthorized traffic on port 21. You examine the packets, and notice there are no files being transferred. Traffic on what other port must be examined to view any file contents?

- A. 20
- B. 119
- C. 23
- D. 80
- E. 2021

**Answer: A**

15. You are introducing a co-worker to the security systems in place in your organization. During the discussion you begin talking about the network, and how it is implemented. You mention something in RFC 791, and are asked what that is. What does RFC 791 specify the standards for?

- A. IP
- B. TCP
- C. UDP

- D. ICMP
- E. Ethernet

**Answer: A**

16. You have been given the task of building the new wireless networks for your office, and you need to verify that your equipment will not interfere with other wireless equipment frequencies. What wireless standard allows for up to 11 Mbps transmission rates and operates in the 2.4GHz range?

- A. 802.11b
- B. 802.11e
- C. 802.11a
- D. 802.11i
- E. 802.11g

**Answer: A**

17. When performing wireless network traffic analysis, what is the type and subtype for an 802.11 authentication packet?

- A. Type AA Subtype AAAA
- B. Type 00 Subtype 1011
- C. Type 0A Subtype 0A0A
- D. Type 11 Subtype 0000
- E. Type A0 Subtype A1A0

**Answer: B**

18. You are configuring your new IDS machine, where you have recently installed Snort. While you are working with this machine, you wish to create some basic rules to test the ability to log traffic as you desire. Which of the following Snort rules will log any tcp traffic from any host other than 172.16.40.50 using any port, to any host in the 10.0.10.0/24 network using any port?

- A. log udp ! 172.16.40.50/32 any -> 10.0.10.0/24 any
- B. log tcp ! 172.16.40.50/32 any -> 10.0.10.0/24 any
- C. log udp ! 172.16.40.50/32 any <> 10.0.10.0/24 any

- D. log tcp ! 172.16.40.50/32 any <> 10.0.10.0/24 any
- E. log tcp ! 172.16.40.50/32 any <- 10.0.10.0/24 any

**Answer: B**

19. You are configuring a new IDS, running Snort, in your network. To better configure Snort, you are studying the configuration file. Which four of the following are the primary parts of the Snort configuration file?

- A. Postprocessors
- B. Variables
- C. Preprocessors
- D. Output Plug-ins
- E. Rulesets

**Answer: BCDE**

20. If you wish to create a new rule in ISA Server 2006 so that all file attachments with an .exe extension that come through the firewall are dropped, what would you select in the Toolbox to create this rule?

- A. Content Type
- B. User Group
- C. Destination Set
- D. Protocol Set
- E. Extension Type

**Answer: A**

Visualexams.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, HuaWei, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

Web site: <http://www.visualexams.com>

You can reach us at any of the email addresses listed below.

E-Mail: [visualexams \(at\) hotmail.Com](mailto:visualexams@hotmail.com)