



## **Cisco 642-564**

**Security Solutions for Systems Engineers**

Q&A

DEMO Version

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$10.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1**

**Which protocol is used for transporting the event data from Cisco IPS 5.0 and later devices to the Cisco Security MARS appliance?**

- A. RDEP over SSL**
- B. SDEE over SSL**
- C. SSH**
- D. syslog**

**Answer: B**

**QUESTION NO: 2 DRAG DROP**

**You work as a network technician at TestKing.com. Your boss, Mrs Tess King, is curious about attack methodologies. Match the technology with the appropriate description.**

**Use each technology once and only once.**

Methodology, select from these

Access attacks

Denios of service attacks

Reconnaissance attacks

Worms, viruses, and Trojan horses

Description

Methodology, place here

Learn information about a target network

Place here

Make a network service unavailable for normal use.

Place here

Escalate privileges

Place here

Exploit weaknesses that are intrinsic to an application

Place here

Target vulnerabilities of end-user workstations

Place here

Answer:

Explanation:

Description	Methodology, place here
Learn information about a target network	Reconnaissance attacks
Make a network service unavailable for normal use.	Denial of service attacks
Escalate privileges	Access attacks
Exploit weaknesses that are intrinsic to an application	<i>Place here</i>
Target vulnerabilities of end-user workstations	Worms, viruses, and Trojan horses

### Reconnaissance Attacks

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities. It is also called information gathering. In most cases, it precedes an actual access or DoS attack. The malicious intruder typically ping-sweeps the target network first to determine what IP addresses are alive. After this is accomplished, the intruder determines what services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the application type and version as well as the type and version of the operating system running on the target host.

Reconnaissance is somewhat analogous to a thief scoping out a neighborhood for vulnerable homes he can break into, such as an unoccupied residence, an easy-to-open door or window, and so on. In many cases, an intruder goes as far as "rattling the door handle"-not to go in immediately if it is open, but to discover vulnerable services he can exploit later when there is less likelihood that anyone is looking.

### Access Attacks

Access is an all-encompassing term that refers to unauthorized data manipulation, system access, or privilege escalation. Unauthorized data retrieval is simply reading, writing, copying, or moving files that are not intended to be accessible to the intruder. Sometimes this is as easy as finding shared folders in Windows 9x or NT, or NFS exported directories in UNIX systems with read or read-write access to everyone. The intruder has no problem getting to the files. More often than not, the easily accessible information is highly confidential and completely unprotected from prying eyes, especially if the attacker is already an internal user.

System access is an intruder's ability to gain access to a machine that he is not allowed access to (such as when the intruder does not have an account or password). Entering or accessing systems that you don't have access to usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Another form of access attacks involves privilege escalation. This is done by legitimate users who have a lower level of access privileges or intruders who have gained lower-privileged access. The intent is to get information or execute procedures that are unauthorized at the user's current level of access. In many cases this involves gaining root access in a UNIX system to install a sniffer to record network traffic, such as usernames and passwords, that can be used to access another target.

In some cases, intruders only want to gain access, not steal information-especially when the motive is intellectual challenge, curiosity, or ignorance.

### **DoS Attacks**

DoS is when an attacker disables or corrupts networks, systems, or services with the intent to deny the service to intended users. It usually involves either crashing the system or slowing it down to the point where it is unusable. But DoS can also be as simple as wiping out or corrupting information necessary for business. In most cases, performing the attack simply involves running a hack, script, or tool. The attacker does not need prior access to the target, because usually all that is required is a way to get to it. For these reasons and because of the great damaging potential, DoS attacks are the most feared-especially by e-commerce website operators.

### **QUESTION NO: 3**

**Which Cisco management product provides a Security Audit wizard?**

- A. Cisco Security Auditor**
- B. CiscoWorks VPN/Security Management Solution**
- C. Cisco Adaptive Security Device Manager**
- D. Cisco Router and Security Device Manager**

**Answer: D**

**QUESTION NO: 4**

**Which three features of Cisco Security MARS provide for identity and mitigation of threats? (Choose three.)**

- A. determines security incidents based on device messages, events, and sessions**
- B. provides incident analysis that is topologically aware for visualization and replay**
- C. integrates with Trend Micro to clean infected hosts**
- D. performs mitigation on Layer 2 ports and at Layer 3 choke points**
- E. provides a security solution for preventing DDoS attacks**
- F. pushes signatures to Cisco IPS to keep viruses from entering the network**

**Answer: A,B,D**

**QUESTION NO: 5**

**How is Cisco IOS Control Plane Policing achieved?**

- A. by adding a service-policy to virtual terminal lines and the console port**
- B. by applying a QoS policy in control plane configuration mode**
- C. by disabling unused services**
- D. by rate-limiting the exchange of routing protocol updates**
- E. by using AutoQoS to rate-limit the control plane traffic**

**Answer: B**

**QUESTION NO: 6**

**Which component of the Cisco NAC framework is responsible for compliance evaluation and policy enforcement?**

- A. Cisco Secure ACS server**
- B. Cisco Trust Agent**
- C. network access devices**
- D. posture validation server**

**Answer: A**

**QUESTION NO: 7 DRAG DROP**

You work as a network technician at TestKing.com. Your trainee Sandra is curious about Network Security Lifecycles. Match each action with the appropriate task.

**Activities, select from these**

Perform impact analysis of new software and features	Perform analysis and create documentation
Develop sample configurations	Specify hardware and software requirements
Conduct a Security Posture Assessment	Monitor and inspect security logs
Develop an implementation plan	

**Activities, place here**

<b>Plan</b>	
Place here	Place here
<b>Design</b>	
Place here	Place here
<b>Optimize</b>	
Place here	Place here

**Answer:**

**Explanation:**

Activities, select from these

# TestKing.com

Develop an implementation plan

Activities, place here

**Plan**

Perform impact analysis of new software and features

Perform analysis and create documentation

**Design**

Develop sample configurations

Specify hardware and software requirements

**Optimize**

Conduct a Security Posture Assessment

Monitor and inspect security logs

**QUESTION NO: 8**

**What is a benefit of the Cisco Integrated Services Routers?**

**A. Intel Xeon CPUs**

- B. built-in event correlation engine**
- C. built-in encryption acceleration**
- D. customer programmable ASIC**

**Answer: C**

**QUESTION NO: 9**

**What are three functions of CSA in helping to secure customer environments?  
(Choose three.)**

- A. application control**
- B. control of executable content**
- C. identification of vulnerabilities**
- D. probing of systems for compliance**
- E. real-time analysis of network traffic**
- F. system hardening**

**Answer: A,B,F**

**QUESTION NO: 10**

**Which two features can the USB eToken for Cisco Integrated Services Router be used for? (Choose two.)**

- A. distribution and storage of VPN credentials**
- B. command authorization**
- C. one-time passwords**
- D. secure deployment of configurations**
- E. troubleshooting**

**Answer: A,D**