



Security Best Practices for Mac OS X v10.4 Sample Test

To Register

You are required to have an Apple Tech ID number before registering for an exam. You can apply for a Tech ID by following the instructions at certifications.apple.com. Then, to register for an exam, call Prometric toll-free at 888-APL-EXAM (888-275-3926) or register online at 2test.com.

To register for an Apple Training course, please visit www.apple.com/training or call 800-848-6398. To schedule an onsite course at your organization's location, please call 800-848-6398 or email abouttraining@apple.com.

The Security Best Practices for Mac OS X v10.4 Exam (Prometric exam no. 9L0-612) is a computer-based test offered at Authorized Prometric Testing Centers. The exam is an elective specialization within the Apple Certified System Administrator (ACSA) certification track.

This Sample Test presents ten test questions similar in style and content to those presented in the Security Best Practices for Mac OS X v10.4 Exam. Reviewing these questions can familiarize you with the type of questions posed in the certification exam. Questions on the official exam will vary in content and may be more or less difficult than these.

Please visit the Apple Certified System Administrator page (train.apple.com/certification/acsa) and download the Security Best Practices for Mac OS X v10.4 Exam Skills Assessment Guide for a detailed description of the exam, including objectives, number of questions, time limit, and required score.

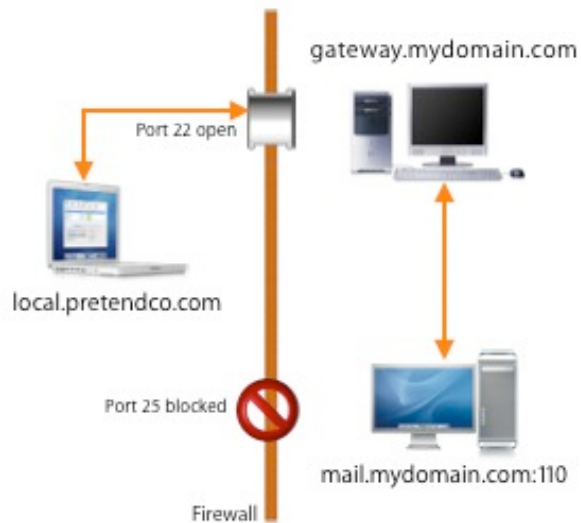
To use this Sample Test, answer the questions below, then refer to the answer key at the end of this document. Please note that UNIX commands and processes are shown in `monospace` in this Sample Test and in the actual exam.

Sample Questions

- 1. You have implemented Open Firmware passwords as a security measure in your office. Still, you find that an attacker has reformatted your boot drive. How could this attack happen?**
 - A. The attacker removed a memory module, then reset PRAM.
 - B. The attacker disconnected the computer's power cable, then reset PRAM multiple times.
 - C. The attacker held down the power button for 10 seconds, then reset PRAM multiple times.
 - D. The attacker reset PRAM multiple times, then typed "password" at the Open Firmware prompt.

- 2. What is the role of the 802.1x in WPA?**
 - A. 802.1x generates a unique encryption key for each packet.
 - B. 802.1x authenticates a user as an authorized user of the network.
 - C. 802.1x bridges the 802.11 network with an 802.3 Ethernet network.

- D. 802.1x encrypts each packet with the encryption key provided by the supplicant.
3. A malicious attacker has gained the shared key to your WEP network. What security risk does this breach entail?
- A. All traffic on the network is compromised until new keys are derived with TKIP.
 - B. All traffic on the network is compromised until the administrator changes the key.
 - C. Traffic for the specific user who was using the shared key is compromised until the user changes her key.
 - D. Traffic for the specific session that was using the shared key is compromised; starting a new session will end the breach.
4. Review the image below, then answer the question that follows.



You need a mail client to communicate with a mail server that resides on the far side of a firewall that is blocking the mail server's SMTP port (port 25). A gateway server with port 22 open has been set up to allow communication across the firewall. Which command will create an SSH tunnel through which the mail client and mail server can communicate?

- A. `ssh -L local.pretendco.com:2525 user@mail.pretendco.com`
- B. `ssh -T local.pretendco.com:2525 gateway.pretendco.com:25`
- C. `ssh -T 2525:mail.pretendco.com user@gateway.pretendco.com:25`
- D. `ssh -L 2525:mail.pretendco.com:25 user@gateway.pretendco.com`

5. **How can you force SSH to connect to only SSH version 2 servers?**
 - A. Add the line `version2 only` to the file `~/.ssh/config`
 - B. Add the line `disallow version1` to the file `~/.ssh/config`
 - C. Type the command `ssh -2 <username>@<remotehost>`
 - D. Type the command `ssh --version=2 <username>@<remotehost>`

6. **Which statement about keychains in Mac OS X v10.4 is true?**
 - A. Keychain entries can be moved between unlocked keychains.
 - B. Cleartext passwords cannot be recovered from a keychain file.
 - C. By default, an admin user has permission to view and edit keychains for all user accounts on a computer.
 - D. The default name of a new user's keychain is "login" or "auto-login" according to the login option selected in System Preferences.

7. **You want to set up a VPN server for your network, 10.0.0.0/8. How can you ensure that clients send only traffic that is addressed to the 10.0.0.0/8 network to your VPN server?**
 - A. Use Server Admin to enable "Private traffic only" in the VPN configuration.
 - B. Modify the `ipfw` rules on the server to divert traffic to the proper destination.
 - C. Use Server Admin to add a Private address of 10.0.0.0, with a subnet mask of 255.0.0.0, to the VPN service.
 - D. Use Internet Connect to configure the VPN client to route only private traffic to the VPN.

8. **You are working with colleagues from another company that uses self-signed certificates. How can you send them encrypted mail?**
 - A. Add your colleagues' public keys to your computer's X509Anchors keychain.
 - B. Have your colleagues send you their Certificate Authority's .cer file, and add it to your computer's X509Anchors keychain.
 - C. Self-signed certificates are configured to be used only by users of a specific mail server. You cannot send encrypted mail to these addresses.
 - D. When you send your first message from a new mail account to the self-signed server, you will receive a response email that will automatically add their certificate to your login keychain.

9. **What are three (3) security features provided by Safari 2.x? (Choose THREE.)**
 - A. disable plug-ins
 - B. enable private browsing
 - C. disable java and javascript code
 - D. encrypt data sent to a proxy server
 - E. block forms requesting personal information

F. enable anonymous browsing of secure websites

10. Which command will display processes that are currently running, ranked by CPU usage?

- A. `top -r`
- B. `top -S`
- C. `top -t`
- D. `top -u`

Answer Key

- 1. A
- 2. B
- 3. B
- 4. D
- 5. C
- 6. A
- 7. C
- 8. B
- 9. ABC
- 10. D

For More Information

Please visit www.apple.com/training or call 800-848-6398 for more information about all Apple Training courses and certification programs.

© 2005 Apple Computer, Inc. All rights reserved. Apple, the Apple logo, AppleTalk, Mac, Mac OS, QuickTime, and WebObjects are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Mention of non-Apple products or services is for informational purposes only. Product specifications are subject to change without notice. December 2005