ISLEVER

9L0-612

Security Best Practices for Mac OS X v10.4 Exam

DEMO

https://www.islever.com/9l0-612.html

https://www.islever.com/apple.html

For the most up-to-date exam questions and materials, we recommend visiting our website, where you can access the latest content and resources.

QUESTION NO: 1

WEP authentication _____; 802.1X does not.

A. provides a secure connection between any two points
B. uses a shared encryption key for all devices on the network
C. supports per-user passwords without a RADIUS server
D. requires a RADIUS server to support encryption

Answer: B

QUESTION NO: 2

You must configure Mac OS X so that each of your users can access his or her home folder over the network. Which service, if used to accomplish this goal, would cause a weak hash of each user's password to be stored in the shadow hash file?

A. Windows Sharing
B. Remote Login
C. Personal File Sharing
D. Personal Web Sharing
E. FTP

Answer: A

QUESTION NO: 3

Where should you look to determine which Certificate Authorities are trusted by Safari?

A. In Safari preferences, click the Advanced button, then select X509Anchors.
B. In Keychain Access, select the X509Anchors keychain.
C. In Security preferences, select the X509Anchors tab.
D. In Network preferences, select Security, then X509Anchors.

Answer: B

QUESTION NO: 4

When configuring Bluetooth on your Mac OS X v10.4 computer, which three (3) security options should you set to restrict access to your computer via Bluetooth?

(Choose THREE.)

A. Prompt for each file received via Bluetooth File Transfer.
B. Require TKIP for all Bluetooth connections.
C. Enable the firewall for Bluetooth File Transfer service in System Preferences.
D. Turn off discoverability in the Bluetooth Status menu.
E. Require pairing for all Bluetooth file transfers.
F. Require Bluetooth serial port for all file transfers.

Answer: A,D,E

QUESTION NO: 5

You want to give the group labadmin the ability to unlock any user's screen saver, but not give the group any further administrative rights. How do you do this?

A. Use Desktop and Screen Saver preferences to allow the labadmin group to unlock the screen saver.
B. Create a new right and rule in the /etc/authorization file
C. Add all members of the labadmin group to the admin group.
D. Make the labadmin group a subgroup of the admin group.

Answer: B

QUESTION NO: 6

Which command will create an encrypted disk image?

A. hdiutil create SecretImage.sparseimage -size 2g -encryption -fs HFS+
-volname SecretImage.sparseimage
B. mkdisk /mnt/SecretImage.sparseimage mount -encryption -fs HFS+
/dev/ram /mnt/SecretImage.sparseimage
C. mkdisk create SecretImage.sparseimage -size 2g -encryption -fs HFS+
-volname SecretImage.sparseimage
D. hdiutil /mnt/SecretImage.sparseimage mount -encryption -fs HFS+
/dev/ram /mnt/SecretImage.sparseimage

Answer: A

QUESTION NO: 7

What two (2) steps are necessary to configure your HTTP website to forward to an SSL website?

(Choose TWO)

A. In Server Admin's Web pane, edit the http:// site, and select "Add new alias or redirect", then enter the URL
for the secure site.
B. In Server Admin's Web pane, create a rule that forwards all traffic through port 8080
C. In Server Admin, start the https service.
D. In Server Admin's Web pane, select the Enable Secure Forwarding checkbox and click OK.
E. In Server Admin's Web pane, select the Enable Secure Sockets Layer (SSL) checkbox and click OK.

Answer: A,E

QUESTION NO: 8

Which command will find files that have the SUID bit set?

A. sudo locate -s
B. sudo find / -perm suid -print
C. sudo find / -perm +4000 -print
D. sudo locate -perm suid

Answer: C

QUESTION NO: 9

Which security technology protects email passwords from network snooping?

A. Kerberos
B. SAPL
C. Shadow Hash
D. Digital Signatures

Answer: A

QUESTION NO: 10

Which two (2) authentication mechanisms are available to SSH users?

(Choose TWO.)

A. NTLM (NT LAN Manager)
B. public/private key pair