Exam Report: 15.12.3 Practice Questions

Date: 4/4/28 6:59:41 pm
Time Spent: 0:14

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

For Linux systems where physical access could be compromised, which of the following best practices should be implemented to prevent a user from booting into single user mode with root access?

○ Set a UEFI/BIOS password.

○ Disable Ctrl+Alt+Delete.

➡ ◉ Set a bootloader password.

○ Separate sensitive data from the operation system.

Explanation

A best practice is to set a password in a bootloader such as GRUB. These passwords help prevent others from booting to Linux, entering single user mode, and compromising the system.

References

Linux Pro - 15.12 Security Best Practices
[e_sec_prac_lp5.exam.xml Q_SEC_PRAC_LP5_BOOT_PSWD]

Question 2: Incorrect

You would like to make it harder for malicious users to gain access to sensitive information.

Which of the following techniques can be used to remap the root directory to include only certain directories and files?

○ SSH certificate

➡ ○ chroot jail SSH

○ One-time password

◉ ~~PKI~~

Explanation

The chroot jail notion uses the **chroot** command to remap the root directory to include only certain directories and files. This makes it harder for malicious users to gain access to other sensitive information.

PKI provides private and public keys.

SSH certificate is used to provide passwordless logins via SSH.

One-time password is a form of multifactor authentication.

References

Linux Pro - 15.12 Security Best Practices
[e_sec_prac_lp5.exam.xml Q_SEC_PRAC_LP5_CHROOT_JAIL]

▼ **Question 3:** Incorrect

You work for a growing small business where the executives are traveling and working remotely.

Which of the following would offer the BEST protection for sensitive data on their laptops?

● ~~Multifactor authentication~~

➡ ○ LUKS disk encryption

○ Bitlocker encryption

○ Enable bootloader passwords

Explanation

Disk encryption is an effective security practice. Linux Unified Key Setup (LUKS) is an open-source disk encryption software. It requires a user to enter a password to access data on a disk.

In the event that a laptop is stolen or lost, disk encryption would protect the data. Bitlocker is only available on a Windows system. Multifactor authentication does not protect data on the computer's disk drive. Enabling bootloader passwords helps prevent other from booting Linux in single user mode but does not protect the data on the disk. Disk encryption is the best way to protect sensitive data on a Linux-based laptop.

References

Linux Pro - 15.12 Security Best Practices
[e_sec_prac_lp5.exam.xml Q_SEC_PRAC_LP5_LUKS]

▼ **Question 4:** Incorrect

Which of the following are multifactor authentication supported by Linux? (Select THREE.)

➡ □ Fingerprint

□ Kerberos

□ TACACS+

□ Mantrap

☑ ~~LDAP~~

➡ □ One-time password (OTP)

➡ □ Iris pattern

Explanation

Multifactor authentication adds an extra layer of security to user logins. In the past, only one factor was used to authenticate a user. The user presented something they knew, like a password. Today, good authentication methods use more than one factor. Other factors might include something the user possesses, like a fob or card, or something that the user is, like a fingerprint or iris pattern. Increasingly popular is a one-time-password (OTP) that is delivered to the user via text message or email.

Mantrap is a physical security measure.

Kerberos, TACACS+, and LDAP are all primary authentication technologies and do not refer to multifactor authentication.

References

Linux Pro - 15.12 Security Best Practices
[e_sec_prac_lp5.exam.xml Q_SEC_PRAC_LP5_MULTIFACTOR]

Question 5: Incorrect

Which of the following technologies can used to set up passwordless SSH logins by distributing a server SSH certificate?

➡ ○ Public key infrastructure (PKI)

● ~~chroot jail SSH~~

○ Kerberos

○ LDAP

Explanation

PKI has all the hardware, software, and people necessary to support the creation and distribution of digital certificates. Certificates are required to enable SSL and TLS cryptographic security protocols to secure communication.
One of the benefits of using PKI is that you can set up passwordless SSH logins by distributing a server SSH certificate.

LDAP and Kerberos are authentication technologies.

chroot jail SSH uses the**chroot** command to remap the root directory to include only certain directories and files. This makes it harder for malicious users to gain access to other sensitive information.

References

Linux Pro - 15.12 Security Best Practices
[e_sec_prac_lp5.exam.xml Q_SEC_PRAC_LP5_PASSWORD_LESS]