Exam Report: 15.3.7 Practice Questions

Date: 5/26/2020 7:41:40 pm
Time Spent: 0:19

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following uses on-the-fly encryption, meaning the data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded?

- VeraCrypt
- ~~BitLocker~~
- Secure Sockets Layer (SSL)
- Transport Layer Security (TSL)

Explanation

VeraCrypt is software for establishing and maintaining an encrypted volume for data storage devices. VeraCrypt uses on-the-fly encryption, meaning the data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded. It requires no user intervention.

BitLocker encrypts the entire contents of a hard drive, protecting all files on the disk.

SSL is a protocol for managing the security of message transmission on the Internet.

TSL is a protocol that establishes a secure connection between a client and server.

References

TestOut Ethical Hacker Pro - 15.3 Cryptography Implementations
[e_crypt_implement_eh1.exam.xml Q_DISK_EMAIL_ENCRYPT_DISK_TOOL_01_EH1]

Question 2: Correct

Alan wants to implement a security tool that protects the entire contents of a hard drive and prevents access even if the drive is moved to another system. Which of the following tools should he choose?

- BitLocker
- EFS
- IPsec
- VPN

Explanation

BitLocker is a Microsoft security solution that encrypts the entire contents of a hard drive, protecting all files on the disk. BitLocker uses a special key that is required to unlock the hard disk. You cannot unlock/decrypt a drive simply by moving it to another computer.

Windows Encrypting Files System (EFS) is a file encryption option, but only encrypts individual files. Encryption and decryption is automatic and dependent upon the file's creator and whether other users have read permissions.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.
IPsec is suite of network protocols that provides data authentication, integrity, and confidentiality between two communication points in an IP network.

References

TestOut Ethical Hacker Pro - 15.3 Cryptography Implementations
[e_crypt_implement_eh1.exam.xml Q_DISK_EMAIL_ENCRYPT_DISK_TOOL_02_EH1]

Question 3: Incorrect

Which of the following encryption tools would prevent a user from reading a file that they did not create and does not require you to encrypt an entire drive?

- SSL
- VPN
- ~~IPsec~~
- EFS

Explanation

Windows Encrypting File System (EFS) encrypts individual files so that only the user who created the file can open it. Decryption is automatic when the file owner opens it. Other users cannot open the encrypted file unless specifically authorized.

IPsec is suite of network protocols that provides data authentication, integrity, and confidentiality between two communication points in an IP network.

A virtual private network (VPN) uses an encryption protocol (such as IPsec, PPTP, or L2TP) to establish a secure communication channel between two hosts or between one site and another site. Data that passes through the unsecured network is encrypted and protected.

Secure Sockets Layer (SSL) is an Application layer protocol that secures message transmission on the Internet.

References

TestOut Ethical Hacker Pro - 15.3 Cryptography Implementations
[e_crypt_implement_eh1.exam.xml Q_DISK_EMAIL_ENCRYPT_DISK_TOOL_03_EH1]

Question 4: Incorrect

Donna is configuring the encryption settings on her email server. She is given a choice of encryption protocols and has been instructed to use the protocol that has the most improvements. Which of the following cryptographic protocols should she choose?

- ~~VeraCrypt~~
- SSL
- OpenSSL
- TLS

Explanation

Transport Layer Security (TLS) is a protocol that is used to establish a secure connection between a client and a server and ensure the privacy and integrity of information during transmission. TLS is a replacement for SSL.

Secure Socket Layer (SSL) is an Application layer protocol developed for managing the security of a message transmission on the internet. SSL 2.0 and 3.0 have been deprecated by the IETF in favor of the TLS protocol.

OpenSSL is not a cryptographic protocol, but an open-source cryptography toolkit that can be used to implement SSL and TLS network protocols and the related cryptography standards they require.

VeraCrypt is not a cryptographic protocol, but is software that establishes and maintains on-the-fly encrypted volumes for data storage devices.

References

TestOut Ethical Hacker Pro - 15.3 Cryptography Implementations
[e_crypt_implement_eh1.exam.xml Q_DISK_EMAIL_ENCRYPT_MAIL_TOOL_01_EH1]

Question 5: Incorrect

Which of the following is an open-source cryptography toolkit that implements SSL and TLS network protocols and the related cryptography standards required by them?

- Symantec Drive Encryption
- ~~BitLocker~~
- OpenSSL
- EFS

Explanation

OpenSSL is an open-source cryptography toolkit that implements SSL and TLS network protocols and the related cryptography standards they require.

Symantec Drive Encryption is not an open-source cryptography toolkit. It is software that provides organizations with complete, transparent drive encryption for all data, including user files, swap files, system files, and hidden files on laptops, desktops, and removable media.

BitLocker is not an open-source cryptography toolkit; it is drive encryption software.

Window Encrypting File System (EFS) is a proprietary function of Windows operating systems that encrypts files.

References

TestOut Ethical Hacker Pro - 15.3 Cryptography Implementations
[e_crypt_implement_eh1.exam.xml Q_DISK_EMAIL_ENCRYPT_MAIL_TOOL_02_EH1]