Linux Tools for Encryption and Hashing

HyperionDev

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Explore Linux tools related to Networking
- Recap on Networking components
- Recap on Firewalls
- Explore Firewall management tools
- How the above ties into Security

Objectives

- Recap on Encryption
- Intro to Linux Tools for encryption
- Look at some key management tools
- Discuss the Importance of verification
- Best practices

Why is it important?

- Protection against unauthorized access, malicious attacks, and data breaches requires effective networking and firewall management.

- Reduced attack surfaces and blocked unauthorized network connections are two ways that properly configured networks and firewalls help reduce risks.

- Managing networks and firewalls effectively can boost systems' responsiveness and efficacy.

- Networking and firewall management procedures assist organizations in fulfilling these demands by ensuring they follow laws and standards to network safety and data security.

- By keeping secure and trustworthy network connections, organizations can avoid network outages, safeguard vital systems and data, and lessen the effects of potential security incidents.

Encryption Recap

- Data is encrypted and decrypted using a single shared secret key in symmetric encryption. Both the sender and the recipient use the same key to maintain confidentiality. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are two popular symmetric encryption algorithms.

- Public-key encryption, also referred to as asymmetric encryption, uses a pair of keys—a public key and a private key—to encrypt data. While the private key is kept private and is used for decryption, the public key is used for encryption. Data can be exchanged securely using asymmetric encryption without revealing the private key. RSA and ECC (Elliptic Curve Cryptography) are two examples of asymmetric encryption algorithms.

Linux encryption tools

OpenSSL: OpenSSL is a popular open-source toolkit for cryptographic and SSL/TLS operations. It offers a number of command-line tools and libraries that support various encryption and cryptographic operations. You can create and manage cryptographic keys with OpenSSL, encrypt and decrypt files, generate digital signatures, and create secure network connections. It supports a variety of encryption techniques, such as hash functions, digital certificates, and symmetric and asymmetric encryption.

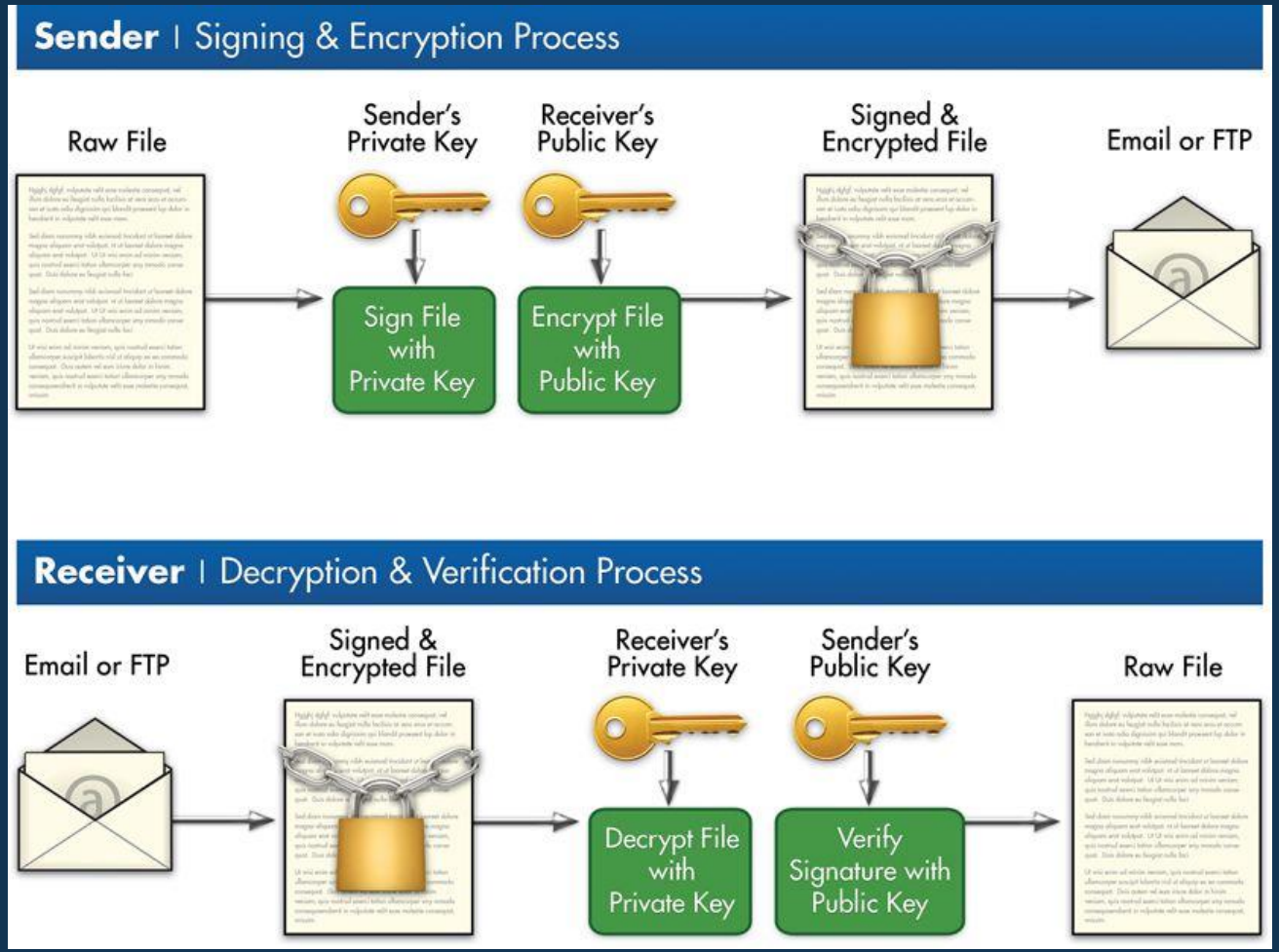
GnuPG (GNU Privacy Guard): Offers cryptographic privacy and authentication for data communication. You can use it to encrypt and sign emails, files, and other types of data because it uses the OpenPGP standard. GnuPG uses both symmetric and asymmetric encryption, offering a safe way to safeguard private data. It facilitates key generation, key management, and user-to-user key exchange

GnuPG e-mail

- *GnuPG uses public-key cryptography, which entails creating a key pair composed of a private key and a public key. While the private key is kept secret and used to decrypt the messages, the public key is distributed to others and used to encrypt messages.*

- *Importing and Exporting Keys: You must import the recipient's public key into your GnuPG keyring in order to send encrypted emails to each other. GnuPG uses a keyring, which is a collection of keys, for encryption and decryption.*

- *Email Encryption and Decryption: You can use GnuPG to encrypt your email messages before sending them once you've imported the recipient's public key. Popular email clients like Thunderbird and Outlook incorporate GnuPG, allowing for seamless encryption within the email interface.*



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fi.pinimg.com%2Foriginals%2Fd9%2Fdd%2Fef%2Fd9ddef219e6cc36fda324c2f68fc0599.jpg&f=1&nofb=1&ipt=04d9e0f93668e2837abafa22faacf1edb3d869f52c8212c7ede77feca73d7785&ipo=images

Key Management Tools

- keyctl: used the command-line tool to control the keys in the kernel keyring. A secure location for keeping and accessing keys is the kernel keyring. You can create, modify, and delete keys with Keyctl, as well as manage who has access to them.

- ssh-agent: SSH authentication requires the use of this tool to manage cryptographic keys. You can use your private keys for SSH connections without repeatedly entering passphrases by storing them in memory with the help of ssh-agent. When necessary, the ssh-agent securely hands over the keys to the SSH client.

Linux Hashing Overview

Several hashing tools, including md5sum, sha1sum, and sha256sum, are available in Linux and can be used to generate cryptographic hash values for files and data. These hash values are one-of-a-kind digital signatures created from the input data, and they're frequently used to protect data integrity and spot any unauthorized changes or tampering.

Using these hashing tools, you can generate hash values for files or data. The specific command may vary depending on the tool being used. For example, md5sum calculates the MD5 hash value, sha1sum calculates the SHA-1 hash value, and sha256sum calculates the SHA-256 hash value.

Once you have the hash value, you can compare it with the original hash value provided by the sender or generated before any changes were made. This comparison allows you to verify the integrity of the file or data. If the hash values match, it means the file or data has not been tampered with, and its integrity remains intact.

Importance of Verification

File Integrity: By checking the hash value before downloading or sending a file between systems, you can make sure that it hasn't been corrupted or altered in any way.

Password Storage: The user's password is hashed and compared to the hash value that has been previously stored. The password is deemed to be valid if the hash values match.

Data Integrity: Hashing is a technique that can be used to guarantee the integrity of important data, including databases or private documents. Any unapproved modifications can be found by routinely computing and comparing hash values.

You can create hash values that serve as digital fingerprints for files and data by using Linux hashing tools. You can ensure data integrity, spot tampering, and maintain the security of your systems and information by verifying these hash values. Making sure that data is authentic and preventing unauthorized modifications is a critical cybersecurity practice.

Best Practices

Create Strong Keys: It's crucial to employ robust algorithms and key lengths that are advised by industry standards when producing cryptographic keys. By doing this, the keys are protected from brute-force attacks.

Secure Keys with Passwords: Put a passphrase on your private keys to encrypt them. By requiring a password to unlock the key, this adds an additional layer of security.

Secure Storage: Your cryptographic keys should be kept in secure locations. Keys should ideally be kept in hardware security modules (HSMs) or encrypted file systems that offer physical security against unauthorized access.

Key Rotation: It is best practice to routinely rotate cryptographic keys. Key rotation ensures improved overall security and lessens the impact of a compromised key.

Observe the principle of least privilege: Only allow key access to services that need it and authorized users.

Wrapping Up.

- OpenSSL and GnuPG .These tools make key generation, key management, and file and email encryption possible. Reputable for their adaptability and widespread use in the Linux community.

- Introduced Linux hashing tools like md5sum, sha1sum, and sha256sum and explained the function of hashing. These tools enable the generation of cryptographic hash values for files and data, assisting in the validation of data accuracy and the detection of data manipulation.

- Emphasized the importance of following legal and ethical guidelines when it comes to encryption and data protection

- By understanding encryption and hashing techniques, individuals can exercise their rights to protect their privacy and maintain control over their personal information.

Next up

- Recap on Linux Tools for Networking and Security

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"