Enabling Certificate Authentication in SSH

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Describe how SSH uses certificate-based authentication.
2. Configure a Linux user account to use certificates to authenticate with SSH.
3. Strengthen the certificates used by an SSH server.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Enabling Certificate Authentication in SSH
    - Certificate-based Authentication
    - Configuring User Keys
    - Configuring Server Keys
- Certificate-based Authentication
    - Improved security
        - Virtually impossible to brute force
        - Much more secure than passwords
        - Key lengths are typically over a thousand characters
    - Certificate
        - Private key is generated by the client
        - Public key is added to their home directory on the server
        - The public key can be loaded to multiple servers
- Configuring User Keys
    1. Generate a key on your client
        - `ssh-keygen`
        - Keys are output to `~/.ssh`
        - `id_rsa` is the private key
        - `id_rsa.pub` is the public key
    2. Copy your key from the client to the server
        - `ssh-copy-id <username>@<server_name>`
- Disable password authentication on the server
    1. `sudoedit /etc/ssh/sshd_config.d/hardened.conf`
    2. Set `PasswordAuthentication no` on the server
- Configuring Server Keys
    1. Delete pre-existing keys
        - `sudo rm /etc/ssh/ssh_host*`
    2. Generate new keys
        - `sudo ssh-keygen -q -N "" -t rsa -b 4096 -f /etc/ssh/ssh_host_rsa_key`
            - `q` Quiet output
            - `N` Passphrase
            - `t` Type
            - `b` Bits
            - `f` Filename
        - `sudo ssh-keygen -q -N "" -t ed25519 -f /etc/ssh/ssh_host_ed25519_key`
    3. Update the configuration to use the new keys

- `sudoedit /etc/ssh/sshd_config.d/hardened.conf`
    - `HostKey /etc/ssh/ssh_host_rsa_key`
    - `HostKey /etc/ssh/ssh_host_ed25519_key`
    - `HostKeyAlgorithms ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,sk-ssh-ed25519@openssh.com,sk-ssh-ed25519-cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-512,rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512-cert-v01@openssh.com`