Implementing Transaction Signatures (TSIG)

LPIC-2: Linux Engineer (202-450)

Objectives:

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

1. Describe transaction signatures and how they secure DNS.
2. Configure Bind to secure server communications by implementing TSIG.

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

- Transaction Signatures (TSIG)
    - Designed to secure server-to-server communications
        - Zone transfers
        - Recursive queries
    - Function
        - Digitally signs messages with a one-way hash
        - Provides authentication and integrity
- Step 1: Generate a key on the primary server
    - `tsig-keygen`
        - Defaults to HMAC-SHA256 with a 256bit key size
        - `tsig-keygen <key-name>`
        - `tsig-keygen ns1-ns2. | sudo tee -a /etc/bind/named.conf.local`
- Step 2: Copy the key data to the other server(s)
    - Key name and hash must match on both servers
- Step 3: Enable TSIG for a particular server
    - `sudoedit /etc/bind/named.conf.local`
    - `server 10.0.222.52 { keys { ns1-ns2. ;};};`
- Step 4: Verify the key is loaded
    - `sudo rndc reconfig`
    - `sudo rndc tsig-list`