Securing BIND with DNSSEC

LPIC-2: Linux Engineer (202-450)

Objectives:

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

1. Describe the purpose and function of DNSSEC
2. Implement DNSSEC for a zone hosted on a Bind server

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

- Domain Name System Security Extensions (DNSSEC)
    - DNS is not secure
        - Records are transmitted in plain text
        - DNS servers trust other servers by default
        - Cache takes priority over reality
    - Designed to combat DNS poisoning attacks
    - Digital signature that validates a DNS response
        - Provides authentication and integrity
- Getting prepared
    - Tools
        - `sudo apt install bind9-utils`
        - `dnssec-keygen`
    - Server
        - Have a zone already created
    - Registrar
        - Have your login credentials
        - Will need to upload hashes at the end
- How DNSSEC works
    - Each zone will have its own key pair
    - Two keys
        - Zone Signing Key (ZSK)
            - Signs individual records or record sets in a zone
        - Key Signing Key (KSK)
            - Signs the SZK
            - Prevents man-in-the-middle attacks that replace the ZSK
            - Hashed copy of the KSK is stored at the registrar
- Step 1: Enable DNSSEC in Bind
    - May not be enabled by default
    - `sudoedit /etc/bind/named.conf.options`
        - `dnssec-enable yes;`
        - `dnssec-validation yes;`
        - `dnssec-lookaside auto;` (for TLDs that don't support DNSSEC)
    - `sudo rndc reconfig`
- Step 2: Creating the ZSK for a zone
    - Creating a ZSK
        - `cd /etc/bind`

        - `sudo dnssec-keygen -a ECDSA256 lab.itpro.tv`
        - NOTE: `ECDSA256` is an alias for `ECDSAP256SHA256`

- Step 3: Creating the KSK for a zone
    - Creating a KSK
        - `sudo dnssec-keygen -f KSK -a ECDSA256 -n ZONE lab.itpro.tv`

- Step 4: Attaching the keys to the zone
    - Add the public keys to the zone file
    - `sudoedit /etc/bind/lab.itpro.tv.dns`
    - Add the following lines after the TTL
        - `$INCLUDE "Klab.itpro.tv.+013+32683.key"`
        - `$INCLUDE "Klab.itpro.tv.+013+52794.key"`

- Step 5: Sign the zone with the keys
    - Use dnssec-signzone to sign the zone
        - `dnssec-signzone -o <zone name> -N <serial format> -k <KSK> <zone filename> <ZSK>`
        - `-t` will show statistics
        - `sudo dnssec-signzone -o lab.itpro.tv -N INCREMENT -t lab.itpro.tv.dns`
        - A new file with `.signed` will be generated

- Step 6: Activate the signed zone
    - Change the config to point to the signed file
        - `sudoedit /etc/bind/named.conf.local`
        - Update the file name

- Step 7: Upload the KSK hash to the registrar
    - Steps vary based on provider
    - Hash is stored in:
        - `/etc/bind/dsset-<zone>`
        - `/etc/bind/dsset-lab.itpro.tv.`