RED NACIONAL ACADEMICA
DE TECNOLOGIA AVANZADA

DNSSEC para zona ENUM

Estes es un paso-a-paso para la instalación/configuración para proveer DNSSEC utilizando OpenDNSSEC y BIND. ENUM está involucrado debido a que usa registros NAPTR.

Instalar dependencias/paquetes

```
:~# apt-get update && apt-get upgrade
```

```
:~# apt-get install softhsm opendnssec opendnssec-enforcer opendnssec-enforcer-sqlite3
```

Copiar tu zona al directorio de zonas sin firmar de OpenDNSSEC

```
:~# cp /path/to/your/zone/file /var/lib/opendnssec/unsigned/
```

Inicializar un token con SoftHSM

```
:~# softhsm --init-token --slot 0 --label "OpenDNSSEC"
```

Esto solicitará la creación de un código PIN el cuál se debe recordar.

Editar el archivo de configuración de OpenDNSSEC

```
:~# vim /etc/opendnssec/conf.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
  <RepositoryList>
    <Repository name="SoftHSM">
      <Module>/usr/lib/softhsm/libsofthsm.so</Module>
      <TokenLabel>OpenDNSSEC</TokenLabel>
      <PIN> ---> CODIGO PIN <---  </PIN>
      <SkipPublicKey/>
    </Repository>
    ...
```

Editar tu archivo de zonas como sigue:

```
:~# vim /etc/opendnssec/zonelist.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<ZoneList>
  <Zone name="example.com">
    <Policy>default</Policy>
    <SignerConfiguration>
       /var/lib/opendnssec/signconf/example.com.xml
    </SignerConfiguration>
    <Adapters>
      <Input>
        <File>/var/lib/opendnssec/unsigned/db.example.com</File>
      </Input>
      <Output>
        <File>/var/lib/opendnssec/signed/db.example.com</File>
      </Output>
    </Adapters>
  </Zone>
</ZoneList>
```

Actualizar la lista de zonas

```
:~# ods-ksmutil update zonelist
```

Añadir tu zona a la lista de zonas

```
:~# ods-ksmutil zone add -zone example.com
```

Firmar tu zona

```
:~# ods-signer sign example.com
```

Listar los estados de las claves

```
:~# ods-ksmutil key list -v
```

Deberá observar la siguiente salida:

```
Keys:
Zone:         Keytype:  State:    Date of next transition:  CKA_ID:   Repository:     Keytag:
example.com   ZSK       active    2010-10-15 06:59:28       ...      OpenDNSSEC      XXXX
example.com   KSK       ready     waiting for ds-seen       ...      OpenDNSSEC      KEYTAG
```

Notificar el Enforcer cuando puedas observar DS RR en la zona padre

```
:~# ods-ksmutil key ds-seen --zone example.com --keytag KEYTAG
```

Podrá observar lo siguiente:

```
Result:
Found key with Keytag KEYTAG
Key KEYTAG made active
```

Luego, al listar las zonas nuevamente se mostrará activa

```
:~# ods-ksmutil key list -v
```

```
Keys:
Zone:                           Keytype:      State:    Date of next transition:
example.com                     ZSK           active    2010-10-15 07:20:53
example.com                     KSK           active    2010-10-15 07:31:03
```

Comprobar que su zona ha sido firmada

```
:~# ls -lta /var/lib/opendnssec/signed/
```

Encontrará un archivo de su zona con regisros RRSIG y DNSKEY contenidos dentro

Apuntar BIND a tu nueva zona

```
:~# vim /etc/bind/named.conf.enum
```

```
  zone "example.com" {
    type master;
    file "/var/lib/opendnssec/signed/db.example.com";
  };
```

Ahora puede consultar su zona utilizando el comando “dig” y DNSSEC

```
:~# dig @ -t NAPTR 3.2.1.example.com +dnssec
```

Enlaces de Referencia

1. OpenDNSSEC Documentation, Uploading a Trust Anchor (Publishing DS record to the parent). https://wiki.opendnssec.org/display/DOCS/Running+OpenDNSSEC#RunningOpenDNSSEC-UploadingaTrustAnchor%28PublishingDSrecordtotheparent%29
2. Github Gist – OpenDNSSEC Installation/Configuration. https://gist.github.com/hernandanielg/f854e085a29943848196