Seguridad en Redes

Práctica 3.3. Seguridad DNS

Preparación del entorno

Para esta práctica necesitaremos una única MV.

Instala la herramienta `dig`:

```
$ sudo apt-get update
$ sudo apt-get install dnsutils
```

Esta herramienta permite realizar consultas DNS con mucha más funcionalidad que los comandos `host` y `nslookup`. Consulta la página de manual del comando `dig`.

Debemos especificar cuáles son nuestros servidores DNS que actúan como *resolvers*. Para ello es necesario editar el fichero `/etc/resolv.conf`, borrar los que haya definidos e introducir la IP de nuestro(s) servidor(es) DNS con la siguiente sintaxis:

```
nameserver <dir_ip_servidor_dns>
```

- Si la práctica se realiza **EN CASA**, se pueden utilizar los servidores de nombres públicos de Google (`8.8.8.8` y `8.8.4.4`). Es decir:

```
$ nano /etc/resolv.conf
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Si la práctica se realiza **EN LA FACULTAD**, sólo se permite utilizar los servidores de nombres de la UCM (`147.96.1.9 y 147.96.2.4`). Es decir:

```
$ nano /etc/resolv.conf
nameserver 147.96.1.9
nameserver 147.96.2.4
```

Introducción al uso de `dig`

El comando `dig` permite consultar distintos tipos de *resource records* (RR) a un servidor DNS. Los tipos de RR más comunes son A, PTR, NS y MX. Por ejemplo:

```
$ dig A www.ucm.es.
```

Para realizar cualquier consulta DNS, es conveniente usar nombres completamente cualificados, que se terminan siempre con un punto (aunque si no se pone el punto final, normalmente también funciona).

Por defecto, este comando realiza la consulta al servidor DNS que tengamos configurado en el archivo `/etc/resolv.conf`. Si queremos especificar otro servidor DNS distinto debemos añadir `@<dir_ip_servidor_dns>` al final de la orden. Por ejemplo, si queremos usar el servidor de OpenDNS `208.67.222.222`, usamos la siguiente orden:

```
$ dig A www.isc.org. @208.67.222.222
```

Consulta de RR tipo A (*Address*)
Las consultas de tipo A permiten conocer la dirección IP asociada a un nombre DNS. Por ejemplo:

```
$ dig A www.ucm.es.
```

Nos devolverla la dirección IP asociada al nombre `www.ucm.es`

Consulta de RR tipo PTR (*Pointer*)
Las consultas de tipo PTR permiten realizar una consulta DNS inversa, es decir, averiguar el nombre DNS asociado a una dirección IP. Para ello debemos escribir la dirección IP en un formato especial (la dirección se escribe de izquierda a derecha, seguida del dominio `in-addr.arpa.`), por ejemplo, para conocer el nombre DNS asociado a la dirección IP `147.96.1.9`, la orden sería la siguiente:

```
$ dig PTR 9.1.96.147.in-addr.arpa.
```

No obstante, existe una forma más cómoda de realizar una consulta DNS inversa mediante la opción `-x`, ya que de esta forma podemos escribir la dirección IP en el formato habitual. Es decir, la orden anterior sería equivalente a esta otra:

```
$ dig -x 147.96.1.9
```

Consulta de RR tipo NS (*Name Server*)
Las consultas de tipo NS permiten conocer los servidores DNS de un determinado dominio, por ejemplo:

```
$ dig NS ucm.es.
```

Nos devolverá la lista de servidores DNS dominio `ucm.es.`

Consulta de RR tipo MX (*Mail eXchange*)
Las consultas de tipo MX permiten conocer los servidores de correo electrónico de un determinado dominio, por ejemplo:

```
$ dig NS ucm.es.
```

Nos devolverá la lista de servidores de correo del dominio `ucm.es.`

Entrega 1: Usando el comando `dig`, averigua los siguientes datos:
a) La dirección IP asociada al nombre `www.rediris.es`
b) El nombre DNS asociado a la dirección IP `199.184.182.1`
c) La lista de servidores DNS del dominio `rediris.es`
d) La lista de servidores de correo del dominio `rediris.es`

Consultas DNS recursivas vs. iterativas

Normalmente, las consultas DNS que se realiza un cliente DNS a su servidor (*resolver*) suelen ser recursivas, como todas las realizadas en los ejemplos del apartado anterior.

Si realizamos una consulta iterativa en vez de recursiva, obtendremos una salida con todo el proceso de resolución, empezando por los servidores raíz. Para ello, debemos usar la añadir la opción `+trace`, por ejemplo:

```
$ dig A www.isc.org. +trace
```

Claves DNSSEC (RR tipo DNSKEY)

Para obtener las claves DNSSEC públicas de una zona, debemos realizar una consulta del RR de tipo DNSKEY. Por ejemplo, para obtener las claves de la zona *root* (`.`), la zona `org` y la zona `isc.org`, usamos las siguientes órdenes (usaremos nombres completamente cualificados):

```
$ dig DNSKEY . +multi
$ dig DNSKEY org. +multi
$ dig DNSKEY isc.org. +multi
```

La opción `+multi` (o `+multiline`) aparte de mostrar la salida en múltiples líneas, muestra el identificador de la clave (*key id*). Analiza los registros DNSKEY generados con los comandos anteriores.

Los datos específicos del registro DNSKEY son:

1. Los indicadores (*flags*)
    - Las claves ZSK (*Zone Signing Key*) tienen el bit 8 (*Zone Key*) activo, por lo que su valor es 256.
    - Las claves KSK (*Key Signing Key*), además, tienen el bit 0 (*Secure Entry Point*, SEP) activo, por lo que su valor es 257.
2. Protocolo (3 = DNSSEC)
3. Algoritmo de firma digital (ej. 8 = RSA/SHA-256)
4. Clave pública en base64
    - La KSK suele ser mayor (es decir, más segura), ya que cambiarla sería más problemático (hay que cambiar el registro DS del dominio de nivel superior y volver a firmarlo).

Si el servidor DNS no implementa DNSSEC, la consulta del registro DNSKEY no devolverá ninguna clave, por ejemplo, en el caso del dominio `ucm.es`:

```
$ dig DNSKEY ucm.es. +multi
```

Entrega 2: Consulta las claves públicas de los dominios que se indican a continuación:
- ietf.org
- rediris.es
- berkeley.edu
- cloudfare.com
- usp.br

Para cada uno de ellos copia el valor de la clave KSK, el valor de la clave ZSK (puede haber más de una), e indica el nombre del algoritmo de firma utilizado.
(listado de algoritmos disponible en:
https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml)

Solicitud de firma digital (RR tipo RRSIG)

Si queremos realizar una consulta con solicitud de firma digital mediante DNSSEC, debemos incluir la opción `+dnssec`. Por ejemplo:

```
$ dig A www.isc.org. +dnssec +multi
```

Esta consulta nos devolverá dos RR:

- Un RR de tipo A con la dirección IP asociada al nombre `www.example.com.`
- Un RR de tipo RRSIG con la firma digital del RR anterior. Esta firma se realiza con la clave pública ZSK del servidor DNS

Analiza esta salida y, en particular, el registro RRSIG. Los campos específicos del registro RRSIG son:

1. Tipo de registro firmado
2. Algoritmo de firma digital usado (ej. 8 = RSA/SHA-256)
3. Número de componentes del nombre de dominio firmado (p. ej. 0 en `.`, 1 en `org.`, 2 en `isc.org.`, 3 en `www.isc.org.`)
4. TTL original de los registros firmados
5. Fecha de expiración de la firma
6. Fecha de firma
7. Identificador de la clave de firma
8. Nombre del dominio firmante
9. Firma digital en base64

Cuando consultamos las claves públicas DNSSEC de una zona (RR de tipo DNSKEY), también podemos solicitar la firma digital de dichos registros la opción `+dnssec`. En este caso, obtendremos dos registros RRSIG uno por cada una de las claves públicas (KSK y ZSK):

```
$ dig DNSKEY isc.org. +dnssec +multi
```

Entrega 3: Realiza una consulta de la dirección IP asociada al nombre `www.rediris.es` con solicitud de firma digital. Identifica y especifica el valor de cada uno de los campos del registro de firma RRSIG.

Negación de existencia autenticada (RR tipo NSEC y NSEC3)

Obtén una negación de existencia autenticada de tipo NSEC:

```
$ dig A fake.isc.org. +dnssec
```

Los datos específicos del registro NSEC son:

1. Siguiente nombre DNS (*next owner name*) existente en la zona
2. Tipos de RR asociados a dicho nombre del dominio

Obtén una negación de existencia autenticada de tipo NSEC3:

```
$ dig A fake.verisign.com. +dnssec
```

Los datos específicos del registro NSEC3 son:

1. El tipo de función hash empleada (1 = SHA-1; 2 = SHA-256)
2. *Flag opt-out*. Indica si esta zona permite la existencia de zonas delegadas inseguras (0 = no se permite; 1 = sí se permite)
3. Iteraciones: número de veces que se aplica la función *hash.*
4. *Salt*: valor adicional para el cálculo del resumen.
5. Función hash del siguiente nombre DNS (*next owner name*) existente en la zona
6. Tipos de RR: indica los tipos de RR existentes asociados al nombre del propietario.

Entrega 4: Busca, entre los dominios utilizados en la Entrega 2, un ejemplo de un dominio que use NSEC y otro que use NSEC3 (para ello inventa un posible nombre de host falso y ejecuta el comando `$ dig A nombre_falso +dnssec`). Copia las salidas generadas para ambos casos. Describe los campos de uno de los registros NSEC y de uno de los registros NSEC3 generados.

Delegación de firmante (RR tipo DS)

Consultar el registro DS del dominio `isc.org`:

```
$ dig DS isc.org. +dnssec
```

La respuesta la proporcionará el servidor autoritativo del dominio `.com`. Dicha respuesta contendrá el hash de la clave pública KSK del dominio `example.com` (permite verificar la validez de dicha clave pública). Como hemos usado la opción `+dnssec`, se incluye también correspondiente registro de firma (`RRSIG`)

Los datos específicos del registro DS son:

1. Identificador de la clave delegada (*key id*)
2. Algoritmo de firma digital (8 = RSA/SHA-256)
3. Algoritmo de resumen (1 = SHA-1, 2 = SHA-256)
4. Resumen en base64

Para comprobar toda la cadena de delegación de firmantes, podemos realizar una consulta de tipo iterativo:

```
$ dig DS isc.org +trace +dnssec
```

Analiza la salida de este comando y, en particular, los registros DS y sus firmas.

Entrega 5: Realiza una consulta recursiva y otra iterativa del registro DS para el dominio `rediris.es`. Copia las salidas generadas para ambos casos. En el caso de la consulta iterativa, identifica los registros de tipo DS y a qué dominio pertenece cada uno de ellos.

Validación de firmas DNSSEC

Crea un archivo con la clave KSK del dominio raíz:

```
$ dig . DNSKEY | grep "DNSKEY.257" > key
```

Realiza una consulta validando las firmas DNSSEC:

```
$ dig A www.rediris.es. +sigchase +trusted-key=key
```

La opción `+sigchase` activa el seguimiento de la cadena de firmas DNSSEC. La opción `+trusted-key` indica el fichero con la clave raíz de confianza.

Por defecto, la validación se hace de abajo a arriba. Para hacerlo de arriba a abajo, como se resuelven las consultas, se puede indicar la opción `+topdown`:

```
$ dig A www.rediris.es. +sigchase +trusted-key=key +topdown
```

La página web http://dnsviz.net muestra una representación visual de la resolución de nombres con DNSSEC. Compárala con la salida del comando anterior.

Entrega 6: Copia la salida del comando anterior. En cada una de las fases de validación que comienzan con el texto "*Launch a query to find ….*" añade un breve texto explicativo indicando qué operación se realiza en dicha fase.

Implementación de un servidor DNS local de tipo "cache-only"

Instala BIND9 (*Berkeley Internet Name Domain version 9*):

```
$ sudo apt-get install bind9
```

BIND9 es ampliamente usado tanto como servidor autoritativo de nombres de dominio, como para implementar un servidor local de tipo "*cache-only*". Se considera un estándar *de facto*. El paquete incluye los servidores de nombres (en `/etc/bind/db.root`) y la clave (en `/etc/bind/bind.keys`) del dominio raíz.

Un servidor DNS de tipo *cache-only* puede se puede configurar para que lance las consultas comenzando por los servidores del dominio raíz o, como haremos en nuestro caso, se puede configurar para que lance las consultas a otros servidores DNS, que se denominan "*forwarders*". En BIND9, la configuración de los *forwarders*, junto con la activación de DNSSEC, se realiza en el archivo de configuración `/etc/bind/named.conf.options`.

```
$ sudo nano /etc/bind/named.conf.options
```

```
// Añadimos las siguientes líneas:
forwarders { 8.8.8.8; 8.8.4.4; };
forward only;

// Si estamos en la red de la UCM, en lugar de los anteriores,
// usaremos los siguientes forwarders:
// forwarders { 147.96.1.9; 147.96.2.4; };
// forward only;

// Comentamos la siguiente línea:
// dnssec-validation auto;

// Y añadimos las dos siguientes:
dnssec-enable yes;
dnssec-validation yes;

// El resto del archivo se deja como está
```

Reinicia el servicio BIND9 con el siguiente comando:

```
$ sudo /etc/init.d/bind9 restart
```

Con esta configuración, BIND9 funciona como resolutor (*resolver*) de nombres en modo *cache-only*. Resolverá las consultas que reciba de los clientes buscando en la *cache* o consultando a los servidores DNS configurados como *forwarders*, y almacenará la respuesta en la *cache*.

Es necesario editar el fichero `/etc/resolv.conf` para establecer la propia máquina local como *resolver* DNS:

```
$ cat /etc/resolv.conf
nameserver 127.0.0.1
```

Realiza una consulta con DNSEC habilitado:

```
$ dig A www.isc.org. +dnssec
```

Repite la consulta y compara el tiempo necesitado (línea `Query time:`).

La *cache* se almacena inicialmente en memoria. Para ver su contenido, ejecuta:

```
$ sudo rndc dumpdb
```

Esto hace que el contenido de la *cache* se almacene en el fichero `/var/cache/bind/named_dump.db`.

Entrega 7: Realiza algunas consultas DNS usando tu servidor *cache-only* como *resolver* y, a continuación, copia el contenido del fichero `/var/cache/bind/named_dump.db`.