Seguridad en Redes de Ordenadores
Práctica 5: IPsec

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Abril de 2018

Resumen

El objetivo de esta práctica es comprender el funcionamiento de IPsec e IKEv2. Esta práctica se va a realizar en el entorno de emulación de redes mininet. Para ello usaremos una máquina virtual que contiene todos los paquetes necesarios para realizar la práctica. Si no tienes importada la máquina virtual de la práctica anterior, debes importar en VirtualBox el siguiente fichero que contiene una máquina virtual Linux 16.04: `/var/lib/vms/mininet-sro/mininet-sro.ova`. Asegúrate antes de importar la máquina, que en las opciones de virtualbox tienes algo como:

```
General -> Avanzado -> Carpeta instantáneas = /var/tmp/miusuario
```

De esta forma la máquina virtual se quedará almacenada en una carpeta local en la máquina del laboratorio y no en tu cuenta personal. Es muy importante esta configuración ya que tu cuenta personal es una carpeta en la red y si no almacenas la máquina virtual en una carpeta en local, virtualBox no funcionará bien. Por otro lado, siempre que necesites acceder a los ficheros de esta práctica deberás sentarte en el mismo ordenador donde realizaste la importación, ya que estos ficheros se quedarán localmente almacenados en esa carpeta.

El usuario de la maquina virtual es `sro` contraseña `SRO-URJC`.

1. Configuración IP del escenario

En la figura 1 se muestra una empresa que tiene 2 sucursales que se desean comunicar a través de una red insegura.

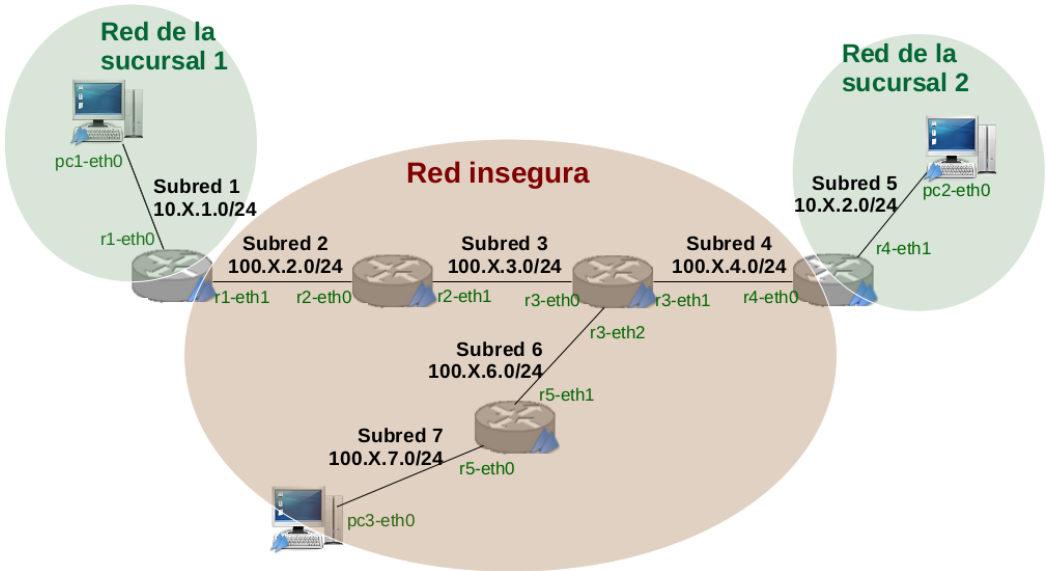

Figura 1: Escenario de red para la práctica openVPN

Descarga de aulavirtual el fichero `lab-ipsec.tgz` dentro de la máquina de virtualBox y descomprímelo en tu carpeta personal (`/home/sro/lab-ipsec`). Observa que la topología de este escenario es igual a la que realizaste en la práctica con openVPN. Copia el fichero `vpn.py` de la práctica anterior a la carpeta `lab-ipsec` y modifica los nombres de carpetas que se montan en cada máquina virtual para que ahora reflejen la carpeta donde has descomprimido el escenario (`/home/sro/lab-ipsec`), añadiendo además la carpeta `/var/run` asociada a la carpeta donde está instalado el escenario:

```
private_dirs = [('/etc',      '/home/sro/lab-ipsec/%(name)s/etc'   ),
                ('/var/log/', '/home/sro/lab-ipsec/%(name)s/var/log'),
                ('/var/run/', '/home/sro/lab-ipsec/%(name)s/var/run')]
```

También será necesario que copies los fichero `etc/hosts` de las máquinas involucradas en las carpetas correspondientes. Por ejemplo, el fichero `lab-openvpn/r4/etc/hosts` deberá estar en `lab-ipsec/r4/etc/hosts`.

Descárgate el fichero `usr.lib.ipsec.charon` y con `sudo` cópialo en `/etc/apparmor.d/` [1]. Ejecuta a continuación el siguiente comando para recargarlo.
`sudo apparmor_parser -r /etc/apparmor.d/usr.lib.ipsec.charon`.

2. Configuración IPsec con ESP

Supón que los trabajadores de la Sucursal1 quieren comunicarse con los trabajadores de la Sucursal2 a través de una red insegura. Para ello, se va a establecer la configuración de IPsec en modo túnel ESP entre `r1` y `r4` para comunicar las direcciones IP entre las subredes: Subred1 y Subred5. Se va a utilizar IKEv2 para que establezca las asociaciones de seguridad SA con los siguientes algoritmos de seguridad (cifrado, integridad y grupo Diffie-Hellman): `aes128-sha256-modp3072`.

IKEv2 va a utilizar certificados X.509 para autenticar a los extremos del túnel, de esta forma cada extremo puede estar seguro de la identidad del otro extremo. A partir de ese momento generarán el secreto compartido Diffie-Hellman y calcularán las claves necesarias para intercambiar de forma segura el contenido de los SAs.

2.1. Generación de certificados en pc3, r1 y r4

Para la creación de certificados vamos a hacerlo todo en la máquina real, no dentro de mininet. Para ello crea una carpeta que se llame por ejemplo `my-rsa-certs` y dentro de ella crea las carpetas: `certs`, `cacerts` y `private`. Desde la carpeta `my-rsa-certs` ejecuta los comandos `ipsec pki` para la creación de cada uno de los certificados que necesitas para que se comuniquen: certificado autofirmado de una autoridad de certificación (CA) y los certificados firmados por la CA para los extremos del túnel (`pc1`, `r1` y `r4`).

En cada extremo deberás dejar la siguiente información:

- En `pc3`: la clave privada de `pc3`, el certificado de `pc3` y el certificado de la CA.
- En `r1`: la clave privada de `r1`, el certificado de `r1` y el certificado de la CA.
- En `r4`: la clave privada de `r4`, el certificado de `r4` y el certificado de la CA.

Explica en la memoria:

1. Indica los nombres de los ficheros de certificados y claves privadas que has generado y en qué carpetas los has almacenado en cada una de las máquinas.
2. Incluye el resultado de imprimir de forma legible cada uno de los certificados que has creado.

2.2. ESP en modo túnel entre r1 y r4

Configura los dos ficheros `ipsec.conf` e `ipsec.secrets` en los routers extremos del túnel ESP `r1` y `r4` para que se puedan comunicar las máquinas de las Subred1 y la Subred5.

Para que la configuración de claves del túnel dure todo el tiempo en el que el túnel esté arrancado asigna valores grandes a los tiempos de vida en `ipsec.conf`:

- `ikelifetime=24h`

1. Incluye en la memoria los ficheros que has configurado en cada uno de los extremos del túnel.

Ten en cuenta a la hora de hacer la práctica que cada vez que reinicies el túnel, las claves cambiarán.

[1] Este fichero está preparado para configurar el escenario que necesariamente debe estar descomprimido en tu cuenta de usuario $(HOME)/lab-ipsec. Si no es así habrá que cambiar el contenido.

2.2.1. Gestión de SAs usando IKEv2

1. Inicia un captura de tráfico en `r1(eth1)` para capturar el intercambio de mensajes IKE (recuerda usar la opción `-s 0` para que se capturen los paquetes completos) y guarda los paquetes capturados en el fichero `ipsec-00.cap`. Arranca IPsec en los extremos y activa la configuración del túnel desde `r1` para que comience el intercambio de mensajes IKE. Comprobarás que los extremos han acordado la SA que van a usar. Interrumpe la captura y cárgala en Wireshark para analizarla.
2. Indica qué campos puedes ver en cada uno de los mensajes IKE capturados. Explícalos.
3. Utilizando Wireshark podrás descifrar los paquetes IKEv2 si configuras en Wireshark las claves que se están utilizando para el intercambio de mensajes IKEv2. Para ello deberás tomar las claves que se encuentran en el fichero de logs de `r1`: `/var/logs/charon.log`. Localiza en ese fichero las claves: Sk_ei (16 bytes), Sk_er (16 bytes), Sk_ai (32 bytes) y Sk_ar (32 butes), véase la figura 2:

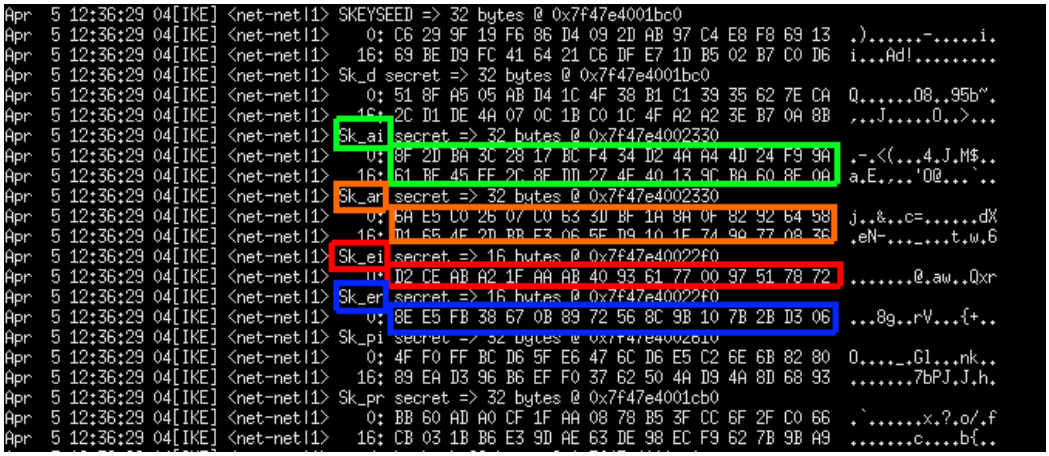

Figura 2: Claves en charon.log

Con la captura que has realizado cargada en Wireshark selecciona en el menú
`Edit -> Preferences -> Protocols -> ISAKMP -> IKEv2 Decryption Table Edit`
y copia allí los valores sin dejar espacios en blanco (es mejor que los copies en un fichero previamente para eliminar los espacios en blanco y después pegues ese valor en la ventana del Wireshark para tratar de no cometer errores):

- Initiator's SPI (8 bytes): valor extraido de los mensajes IKE_SA_INIT
- Responder's SPI (8 bytes): valor extraido de los mensajes IKE_SA_INIT
- SK_ei: valor extraido del fichero charon.log.
- SK_er: valor extraido del fichero charon.log.
- Encryption algorithm: `AES-CBC-128 [RFC3602]`
- SK_ai: valor extraido del fichero charon.log.
- SK_ar: valor extraido del fichero charon.log.
- Integrity algorithm: `HMAC_SHA_256_128 [RFC4868]`

Al configurarlo, wireshark no permite ver bien todos los campos que has copiado en la interfaz. Para comprobar que está bien, puedes consultar el fichero `~/.config/wireshark/ikev2_decryption_table`, donde se ven todos los campos completos. Este fichero no se puede modificar, se genera automáticamente. Debería contener algo similar a la siguiente figura:

```
# This file is automatically generated, DO NOT MODIFY.
fe4b29f1ec75c158,e3412340d516fa99,d2ceaba21faaab409361770097517872,8ee5fb38670b8972568c9b107b2bd306,"AES-CBC-128 [RFC3602]",8f2dba3c2817bcf434d24aa44d24f99a61be45ef2c8edd274f40139cba608e0a,6ae5c02607c0633dbf1a8a0f82926458d1654e2dbbe3065fd9101f749a770836,"HMAC_SHA2_256_128 [RFC4868]"
```

Si ves que los campos no coinciden con los que deberías haber copiado, no puedes cambiarlo en ese fichero, porque está generado automáticamente. Deberás utilizar de nuevo la interfaz de wireshark para modificarlos.

Una vez descifrado el contenido indica en la memoria las siguientes cuestiones:

a) En el mensaje `IKE_AUTH` que envía `r1` a `r4`:

1) Fíjate como cada `payload` contiene un campo `Next Payload` que indica lo que viene a continuación. Indica todos los `payloads` que aparecen y cuál es el campo `Next Payload` del último.
2) Cómo se identifica al extremo `initiator`.
3) Qué certificado se incluye
4) Cómo debe identificarse el otro extremo (`responder`).
5) Cómo el otro extremo (`responder`) va a autenticar a `initiator`.
6) En la SA que se propone indica el protocolo IPsec que se va a utilizar, el SPI y los algoritmos que envía `r1` a `r4` para confidencialidad y autenticación.
7) Indica qué selectores de tráfico se envían, tanto para `initiator` como `responder`.

b) En el mensaje `IKE_AUTH` que envía `r4` a `r1`:
1) Cómo se identifica al extremo `responder`.
2) Qué certificado se incluye
3) Cómo el otro extremo (`initiator`) va a autenticar a `responder`.
4) En la SA que se propone indica el protocolo IPsec que se va a utilizar, el SPI y los algoritmos que envía `r1` a `r4` para confidencialidad y autenticación. Indica qué diferencias ves con respecto a lo que `initiator` envió en su propuesta de SA.
5) Indica qué selectores de tráfico se envían, tanto para `initiator` como `responder`.

4. Consulta SAD y SPD en cada uno de los extremos e incluye en la memoria la información relevante para el túnel IPsec. Fíjate en los valores SPI e indica si estos valores coinciden con los de la SA negociada previamente.
5. Consulta la tabla de encaimunamiento de la máquina en `r1` y `r4`. ¿Qué ocurre con los paquetes enviados a las direcciones internas desde la sucursal1 a la sucursal2? Justifica tu respuesta consultando la tabla de encaminamiento 220 (creada por strongswan).

2.2.2. Comunicación usando IPsec (ESP en modo túnel)

1. Explica detalladamente qué es lo que crees que ocurriría en `r1` cuando:
   - `pc1` le envía un datagrama IP a `pc2`
   - `pc2` le envía un datagrama IP a `pc1`
2. Inicia las siguientes capturas de tráfico:
   - En `r1(eth1)` y guarda los paquetes capturados en el fichero `ipsec-01.cap`.
   - En `r4(eth0)` y guarda los paquetes capturados en el fichero `ipsec-02.cap`.
   - En `pc2` y guarda los paquetes capturados en el fichero `ipsec-03.cap`.

   Realiza un ping desde `pc1` a `pc2`. Interrumpe las capturas y observa su contenido en Wireshark. Wireshark mostrará para cada paquete recibido el paquete cifrado y el paquete en claro[2]. Sin embargo para el paquete enviado sólo lo muestra cifrado.

   Explica el contenido que puedes ver de los paquetes ESP que se corresponden con los paquetes echo request/echo reply capturados y cómo varía el campo `ESP Sequence`.

   Si una máquina maliciosa intermedia capturara los paquetes de la comunicación entre `pc1` y `pc2`, ¿crees que podría saber qué direcciones IP de están comunicando? ¿por qué?
3. ¿Con qué TTL crees que se habrán recibido los paquetes en `pc2`. Compruébalo observando la captura `ipsec-03.cap`. Explica el resultado.
4. Utilizando Wireshark podrás descifrar los paquetes ESP si configuras en Wireshark las claves que se están utilizando para el intercambio de mensajes ESP. Para ello deberás tomar las claves que has mostrado en SAD. Con la captura `ipsec-01.cap` cargada en Wireshark selecciona en el menú:
   `Edit -> Preferences -> Protocols -> ESP`
   marca la opción de descifrar y autenticar paquetes y edita la configuración para copiar allí los valores de cada uno de los SAs que muestra la SAD de `r1` sin dejar espacios en blanco:
   - Protocol
   - Src IP
   - Dest IP
   - SPI
   - Encryption algorithm: `AES-CBC [RFC3602]`.
   - Encryption key

[2]Esto se debe a que una vez que el paquete ha sido descifrado, vuelve a procesarse como si se hubiera recibido descifrado, atravesando nuevamente las cadenas de iptables

- Authentication algorithm: `HMAC-SHA-256-128 [RFC4868]`.
- Authentication key

Al configurarlo, wireshark no permite ver bien todos los campos que has copiado en la interfaz. Para comprobar que está bien, puedes consultar el fichero `~/.config/wireshark/esp_sa`, donde se ven todos los campos completos. Este fichero no se puede modificar, se genera automáticamente. Debería contener algo similar a la siguiente figura:

```
# This file is automatically generated, DO NOT MODIFY.
"IPv4","100.0.2.1","100.0.4.4","0xc993a4ff","AES-CBC [RFC3602]","0xa16eb8e713e1c
e03ffa6881c12d5a0b5","HMAC-SHA-256-128 [RFC4868]","0x684a0e9a8af68971f6d42ddb42f
688fe734c37db0a62aa2c15ae3c4946a7f6ca"
"IPv4","100.0.4.4","100.0.2.1","0xc79f733f","AES-CBC [RFC3602]","0xd0930d7164c73
3ff7658ffd7a7c78930","HMAC-SHA-256-128 [RFC4868]","0xd9295cc387ec8bf65835876325c
f145719f88446efa8f7d96cc52832e6b11fcd"
~
```

5. Explica el contenido de la cabecera ESP de los paquetes que se corresponden con los paquetes echo request/echo reply capturados, observa cómo ahora puedes ver todos los campos.
6. ¿Observando la captura puedes saber si IPsec está trabajando en modo túnel o en modo transporte?
7. ¿Qué crees que ocurrirá si se envía tráfico TCP/UDP de `pc1` a `pc2`? ¿Por qué? Inicia una captura nuevamente en `r1(eth1)` y guarda los paquetes capturados en el fichero `ipsec-04.cap`. Compruébalo utilizando `nc` para lanzar un cliente y un servidor en dichas máquinas, primero con UDP y después con TCP. Examina la captura e indica qué ves.
8. Inicia una captura nuevamente en `r1(eth1)` y guarda los paquetes capturados en el fichero `ipsec-05.cap`. Interrumpe IPsec en `r1` e interrumpe la captura de paquetes. Utiliza Wireshark para visualizar los paquetes capturados explica qué ocurre.

2.3. ESP en modo transporte entre pc3 y r4

Supón que `pc3` quiere establecer una comunicación IPsec ESP con `r4` en modo transporte para una aplicación TCP que se encuentra ejecutándose en `r4` esperando recibir conexiones en el puerto 4444. `pc3` se conectará desde el puerto local 3333 a dicho puerto remoto en `r4`. Se va a utilizar IKEv2 para que establezca las asociaciones de seguridad SA con los siguientes algoritmos de seguridad (cifrado, integridad y grupo Diffie-Hellman): `aes128-sha256-modp3071`.

1. Realiza la configuración en los ficheros que sean necesarios para permitir esta comunicación. Incluye estos ficheros en la memoria. No olvides guardar en la máquina real los ficheros que modifiques, de esta forma tendrás una copia de seguridad.
2. Inicia una captura en `pc3` para guardar su contenido en el fichero `ipsec-06.cap` y establece la configuración ESP en modo transporte entre ambas máquinas. Ejecuta un `ping` desde la máquina `pc3`. Interrumpe la captura y explica su contenido.
3. Observa el contenido de SAD y SDP en `pc3` y explica su contenido.
4. Inicia una captura en `pc3` para guardar su contenido en el fichero `ipsec-07.cap` y establece la configuración ESP en modo transporte entre ambas máquinas. Usando `nc` ejecuta un servidor TCP en `r4` en el puerto 4444 al que se conecta un cliente desde la máquina `pc3` y el puerto 3333. Escribe algo desde el cliente para que se transmita al servidor. Interrumpe la captura y responde las siguientes cuestiones:
   a) ¿Qué campos observas en los paquetes ESP?
   b) Descifra el contenido de ESP para ver exactamente qué es lo que se envía. ¿Qué diferencias observas con respecto al modo túnel?
   c) ¿Con qué TTL se reciben los paquetes IP en `r4`? ¿Por qué?

2.4. AH en modo transporte entre r1 y r4

Utiliza la misma configuración que usaste en el apartado 2.2 y modifica el uso de ESP por AH sustituyendo en `ipsec.conf` la línea `esp=aes128-sha256-modp3072!` por `ah=sha256-sha384!`.

1. ¿Qué crees que ocurrirá si se envía tráfico de `pc1` a `pc2`? ¿Por qué? Inicia una captura nuevamente en `r1(eth1)` y guarda los paquetes capturados en el fichero `ipsec-08.cap`. Compruébalo utilizando `ping` entre dichas máquinas. Examina la captura e indica qué ves.
2. Explica, sólo partiendo de los datos que aparecen en la captura, por qué se puede saber que la configuración IPsec realizada está en modo túnel AH.
3. Explica por qué crees que no se puede realizar un ataque de reproducción con esta configuración.

3. Normas de entrega

Deberás subir al `aulavirtual` un fichero `ipsec.tgz` que contenga los siguientes archivos:

- La memoria en formato pdf.
- Un archivo `capturas.tgz` que contenga los ficheros con las capturas de `ipsec-00.cap` a `ipsec-08.cap`
- Un archivo `config.tgz` que contenga todos los archivos que hay en tu carpeta `$HOME/.config/wireshark`