Seguridad en Redes de Comunicación

Práctica 5. IPSec

Jorge Lanza Calderón

Luis Sánchez González

Departamento de Ingeniería de Comunicaciones

PRÁCTICA 5
IPSec

1. Objetivos de la Práctica

El desarrollo de la práctica pretende complementar el aprendizaje de los conceptos teóricos que se han visto durante las sesiones de teoría.

Los principales objetivos de esta práctica son:

- Analizar y comprender los mecanismos y protocolos involucrados en IPSec.
- Monitorizar y analizar una comunicación protegida mediante IPSec.
- Monitorizar y analizar el establecimiento de una SA mediante IKEv2.

2. Introducción

Durante las sesiones teóricas se han descrito los aspectos fundamentales y los protocolos involucrados en el protocolo IPSec.

A lo largo de la práctica utilizaremos el marco que nos facilita `ipsec-tools`. Este entorno nos permite interactuar con la implementación de IPSec del kernel de Linux estableciendo de manera estática Security Associations (SA).

Asimismo, para el análisis del protocolo IKEv2 utilizaremos una implementación open source de este protocolo llamada `racoon2`. Esta implementación nos permitirá establecer de manera dinámica SAs IPSec.

3. Desarrollo de la Práctica

La práctica se desarrollará en un entorno Linux, para lo cual los datos de acceso a la cuenta definidos son:

```
Nombre de usuario: Alumnos General
Contraseña: telematica
```

3.1 Creación estática de Security Associations IPSec

En lugar de utilizar directamente el PC y la red del laboratorio, se empleará una herramienta de emulación de redes en la cual los diferentes elementos de la red (dispositivos de usuario y routers) se implementan a través de máquinas virtuales Linux. Netkit [1] es un entorno software que permite realizar experimentos con redes de ordenadores virtuales sin necesidad de disponer de dispositivos de comunicaciones ni ordenadores reales. Netkit permite interconectar varios nodos virtuales (ordenadores, hubs y routers) que emulan el funcionamiento de nodos con el S.O. GNU/Linux. Por su parte NetGUI [2] es una interfaz gráfica para el sistema Netkit que permite una interacción más amigable e intuitiva.

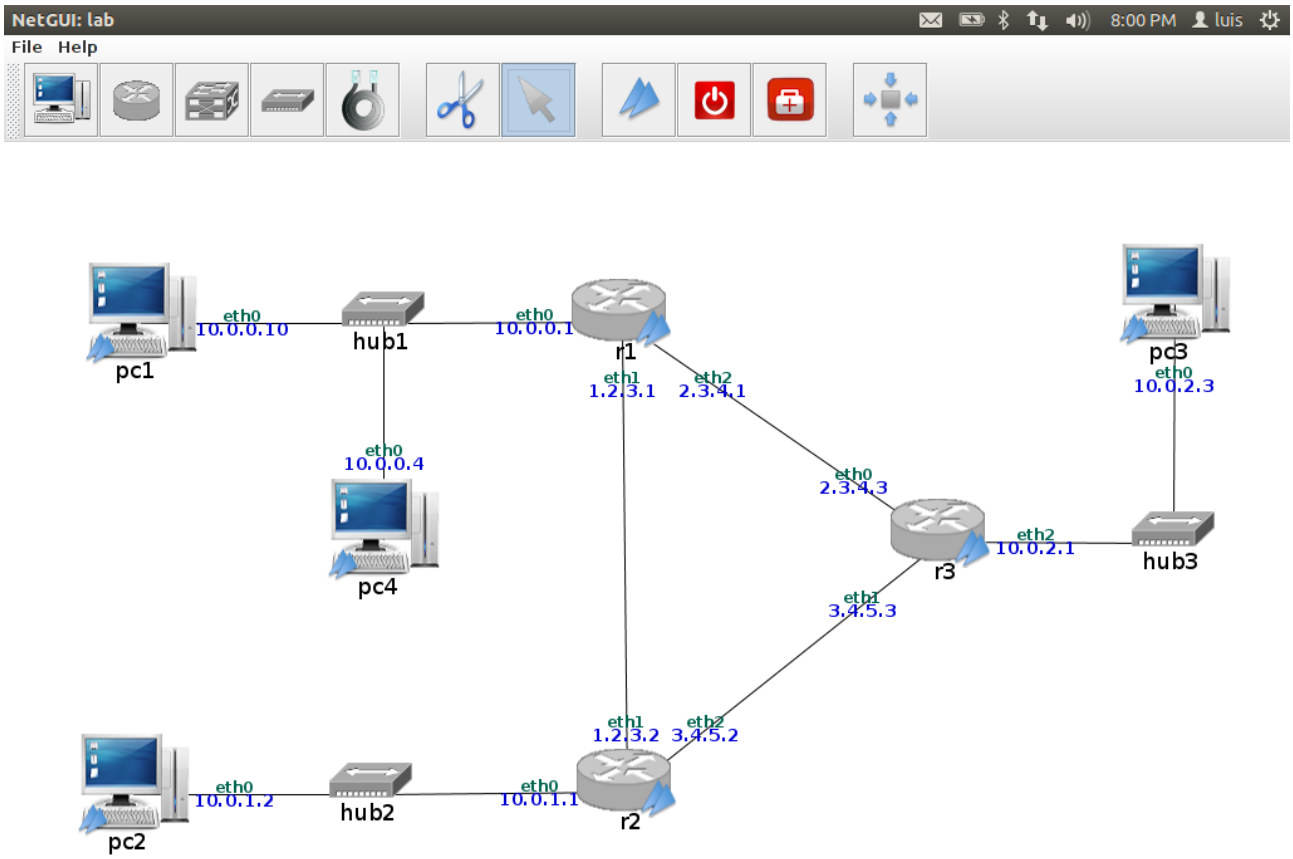
En esta práctica se procederá a cargar una red usando el entorno de NetGUI (Ver Anexo 1) para posteriormente mediante el uso de las herramientas de configuración de IPSec y análisis de la red que implementa Linux monitorizar su funcionamiento y el de los protocolos implicados.

El comando:

```
$ netgui.sh
```

lanza la aplicación NetGUI.

Cargad la red que se encuentra en el directorio `network` que dentro de `/home/alumnos/Asignaturas/SRC/ipsec`.



3.1.1 SA estática en modo transporte

Para este primer apartado crearemos una SA estática que proteja las comunicaciones entre `pc1` y `pc4`.

Arrancaremos únicamente `pc1` y `pc4` en NetGUI.

Las máquinas virtuales con las que trabajaremos en NetGUI tienen un directorio que se mapea directamente sobre el directorio de usuario de la máquina real. De esta manera, el `/hosthome` en `pc1` o en `pc4` es el directorio `/home/alumnos` en vuestro PC. Para facilitar el desarrollo de la práctica se sugiere que dentro de las máquinas virtuales se trabaje siempre en el directorio `/hosthome/Asignaturas/SRC/ipsec`.

El comando **setkey** permite manipular la Security Associations Database (SAD) y la Security Policies Database (SPD) con las que trabaja la implementación de IPSec el kernel de Linux.

```
$ man setkey
```

nos muestra las opciones de este comando. También podéis encontrar la misma información en http://www.freebsd.org/cgi/man.cgi?query=setkey&sektion=8

Ejecutando:

```
# setkey -D
# setkey -DP
```

mostraremos la SAD y la SPD respectivamente.

Inicialmente ni `pc1` ni `pc4` tienen ninguna SA ni ninguna política de seguridad pre-establecida.

La opción **-f** del comando **setkey** permite definir tanto SAs estáticas como políticas de seguridad a través de un fichero de configuración.

En el directorio `/home/alumnos/Asignaturas/SRC/ipsec` podéis encontrar el fichero `pc1-ipsec.conf`:

```
# Flush the SAD and SPD
flush;
spdflush;

# AH
spdadd 0.0.0.0/0 10.0.0.0/24 any -P out ipsec ah/transport//require;
add 10.0.0.10 10.0.0.4 ah 1234 -m transport -A hmac-sha1
"01234567890123456789";


# ESP
#spdadd 0.0.0.0/0 10.0.0.0/24 any -P out ipsec esp/transport//require;
#add 10.0.0.10 10.0.0.4 esp 1234 -m transport -E aes-cbc "0123456789012345"
-A hmac-sha1 "01234567890123456789";
```

La sintáxis del fichero de configuración está explicada en detalle en la ayuda del comando.

En nuestro caso el fichero añade una política de seguridad a la SPD (**spdadd**) por la cual cualquier datagrama IP con destino a la red 10.0.0.0/24 (**src_range** es **0.0.0.0/0** y **dst_range** es **10.0.0.0/24**) independientemente del protocolo de nivel superior (**upperspec** es **any**) que salga del equipo (**policy** es **-P out**) deberá protegerse utilizando el protocolo AH de IPsec en modo transporte de manera obligatoria (**policy** es **ipsec ah/transport//require**).

Dada esta política de seguridad es necesario asimismo definir la SA asociada. En nuestro caso el fichero añade una SA (**add**) identificada por el Security Parameter Index el 1234 (**spi** es **1234**) válida para los datagramas IP cuya dirección origen sea 10.0.0.10 (**src** es **10.0.0.10**) y cuya dirección destino sea 10.0.0.4 (**dst** es **10.0.0.4**) que utilizará el protocolo AH (**protocol** es **ah**), en modo transporte (**extensions** es **-m transport**) empleando el algoritmo HMAC-SHA1 con la clave correspondiente (**algorithm** es **-A hmac-sha1**).

La definición de una política y su correspondiente SA utilizando ESP en lugar de AH también está recogido en el fichero aunque inicialmente comentada.

Tras ejecutar

```
# setkey -f pc1-ipsec.conf
```

Comprobaremos como se han añadido la política y la SA correspondientes en la SPD y SAD respectivamente.

Haced un ping desde pc1 a pc4. Capturad en pc4 y observad lo que ocurre.

Para capturar en el entorno virtual es necesario utilizar tcpdump:

```
# tcpdump -i <interfaz de red> -w <nombre del fichero de captura>
```

> ¿Por qué no se pueden comunicar pc1 y pc4?
>
> Si en la captura se ve como los datagramas que envía pc1 llegan a pc4 ¿por qué pc4 no responde?

Haced las modificaciones necesarias para que la comunicación entre `pc1` y `pc4` sea posible. Haced un ping desde `pc1` a `pc4`. Capturad en `pc4` y observad el intercambio de datagramas.

Repetid el proceso utilizando el protocolo ESP en lugar de AH.

3.1.2 SA estática en modo túnel

Como hemos visto en clase, una aplicación de IPSec es la creación de Redes Privadas Virtuales (VPNs). Una de las configuraciones más típicas es el establecimiento de un túnel IPSec entre los routers de acceso de dos redes distantes de forma que los datagramas sólo se transmitan en claro dentro de estas redes mientras que fuera de ellas estén completamente cifrados.

En el directorio `/home/alumnos/Asignaturas/SRC/ipsec` podéis encontrar el fichero `r1-ipsec.conf`:

```
# Flush the SAD and SPD
flush;
spdflush;

## R1 Policies
spdadd 10.0.0.0/24 10.0.1.0/24 any -P out ipsec esp/tunnel/1.2.3.1-
1.2.3.2/require;
spdadd 0.0.0.0/0 10.0.0.0/24 any -P in ipsec esp/tunnel/0.0.0.0-
0.0.0.0/require;

## Tunel ESP R1 <-> R2
add 1.2.3.1 1.2.3.2 esp 34500 -m tunnel -E 3des-cbc
"123456789012123456789012" -A hmac-md5 "1234567890123456";
add 1.2.3.2 1.2.3.1 esp 34501 -m tunnel -E 3des-cbc
"123456789012123456789012" -A hmac-md5 "1234567890123456";
```

La sintáxis del fichero de configuración es similar al caso del modo transporte. La única diferencia está en que a la hora de definir las políticas de seguridad, los parámetros dentro de la sección **`policy`** de la línea **`spdadd`** deben incluir los endpoints del túnel que se usará (**`policy`** es **`ipsec esp/tunnel/1.2.3.1-1.2.3.2/require`**). Es posible definir una política que imponga el uso del modo túnel pero se dejen sin especificar los endpoints de dicho túnel (uso de las direcciones **`0.0.0.0`**).

Ejecutad en `r1`:

```
# setkey -f r1-ipsec.conf
```

¿Qué sentido tienen las políticas añadidas?

¿Por qué `pc2` no se puede comunicar con `pc1` o `pc4`?

Editad un fichero `r2-ipsec.conf` de forma que ejecutando en `r2`:

```
# setkey -f r2-ipsec.conf
```

sea posible la comunicación entre `pc2` y `pc1`.

Haced un ping desde `pc2` a `pc1`. Capturad en el interfaz `eth0` de `r1` y en el interfaz `eth1` de `r2` y observad los datagramas intercambiados.

¿Podría un atacante pinchando en el enlace `r2 – r1` saber que dos dispositivos están comunicándose?

¿Podría ese atacante saberlo si el protocolo usado hubiera sido AH en lugar de ESP?

¿Puede `pc3` comunicarse con `pc2`?

¿Por qué `pc3` no se puede comunicar con `pc1` o `pc4`?

3.1.3 Establecimiento dinámico de SAs IPSec. Protocolo IKEv2

Hasta ahora hemos hecho uso de IPSec dentro del entorno generado por Netgui. Para esta parte de la práctica volveremos a usar el entorno real del laboratorio. Esto se debe a que las herramientas para gestión dinámica de SAs IPSec instaladas en las máquinas virtuales de Netgui sólo soportan la versión 1 del protocolo IKE. Esta versión está en desuso y declarada obsoleta por el IETF.

En este apartado de la práctica, en lugar de fijar de manera manual los detalles de las SAs IPSec utilizaremos las herramientas que ofrece el Racoon2Project (http://www.racoon2.wide.ad.jp/w/), una implementación del protocolo IKEv2 que interactua con la implementación de IPSec del kernel de Linux.

Las aplicaciones que usaremos en esta práctica son spmd e iked. La primera es un demonio que hace de interfaz con el kernel de Linux y define las políticas de seguridad IPSec a utilizar. La segunda se trata de un demonio que implementa el protocolo IKEv2. Ambas cooperan para el establecimiento dinámico de SAs IPSec.

Los comandos para ejecutar ambas aplicaciones son respectivamente:

```
$ sudo spmd -F -f <configuration file>
$ sudo iked -F -f <configuration file>
```

En el directorio `/home/alumnos/Asignaturas/SRC/ipsec/racoon` podéis encontrar el fichero `racoon.conf`:

```
interface {
  # specify the I/F.
  # make sure the directory permission is 700 and the owner is root.
  spmd { unix "/home/alumnos/Asignaturas/SRC/ipsec/racoon2/spmif"; };

  # specify the password file in order to communicate
  # between spmd(8) and others.
  # create it by 'pskgen -r -o FILE-NAME' command and
  # make sure the file permission is 600 and the owner is root.
  spmd_password "/home/alumnos/Asignaturas/SRC/ipsec/racoon2/spmd.pwd";

  # listen to all addresses.
  ike { MY_IP; };
};

selector slt-A-B-any {
  direction outbound;              # set "inbound" at B
  src 192.168.110.3;
  dst 192.168.110.2;
  upper_layer_protocol "any";
  policy_index policy-A-B;
};

selector slt-B-A-any {
  direction inbound;             # set "outbound" at B
  src 192.168.110.2;
  dst 192.168.110.3;
  upper_layer_protocol "any";
  policy_index policy-A-B;
};

remote remote-A {
  acceptable_kmp { ikev2; };

  # ikev2 configuration
  ikev2 {
    peers_ipaddr    192.168.110.2;                # 192.168.110.3 at B
    peers_id        ipaddr 192.168.110.2;         # 192.168.110.3 at B
    my_id           ipaddr 192.168.110.3;         # 192.168.110.2 at B
    kmp_enc_alg     { aes128_cbc; 3des_cbc; };
    kmp_prf_alg     { hmac_md5; };
    kmp_hash_alg    { hmac_sha1; hmac_md5; };
    kmp_dh_group    { modp1024; modp2048; };
    kmp_auth_method { psk; };

    # make sure the file permission is 600 and the owner is root.
    pre_shared_key  "/home/alumnos/Asignaturas/SRC/ipsec/racoon2/AB.psk";
  };
};

policy policy-A-B {
  action auto_ipsec;
  remote_index remote-A;
  ipsec_mode transport;
  #ipsec_index { ipsec-esp-b-a; };
  ipsec_index { ipsec-ah-b-a; };
  ipsec_level require;
  peers_sa_ipaddr 192.168.110.2;        # 192.168.110.3 at B
  my_sa_ipaddr 192.168.110.3;           # 192.168.110.2 at B
};

ipsec ipsec-esp-b-a {
  ipsec_sa_lifetime_time 150 sec;
  sa_index { sa-esp-1; };
};

ipsec ipsec-ah-b-a {
  ipsec_sa_lifetime_time 150 sec;
  sa_index { sa-ah-1; };
};

sa sa-esp-1 {
  sa_protocol esp;
  esp_enc_alg { aes128_cbc; 3des_cbc; };
  esp_auth_alg { hmac_sha1; hmac_md5; };
};

sa sa-ah-1 {
  sa_protocol ah;
  ah_auth_alg { hmac_sha1; hmac_md5; };
};
```

La sintáxis del fichero de configuración queda fuera de los objetivos de la práctica. Sin embargo, será necesario editar el fichero adaptando las direcciones IP de las líneas resaltadas en negrita de forma que se adapten a cada caso.

Trabajando por parejas en dos PCs diferentes, **adaptad el fichero de configuración para adaptarlo a la configuración de los equipos de la pareja.**

Lanzad las aplicaciones `spmd` e `iked` (en este orden). Observad que la opción `-F` hace que las aplicaciones se lancen en foreground por lo que tendréis que hacerlo en terminales distintas.

Haced un ping entre los dos PCs. Capturad el intercambio de paquetes usando Wireshark y analizad el intercambio.

¿Se ven en la captura todas las fases del intercambio IKE? ¿Qué algoritmos de cifrado y hash se han usado en la IKE_SA? ¿Qué algoritmos de cifrado y hash se usan en la IPSEC_SA?

Una vez establecidas las IPSEC_SA es posible consultarlas mediante el comando `setkey`.

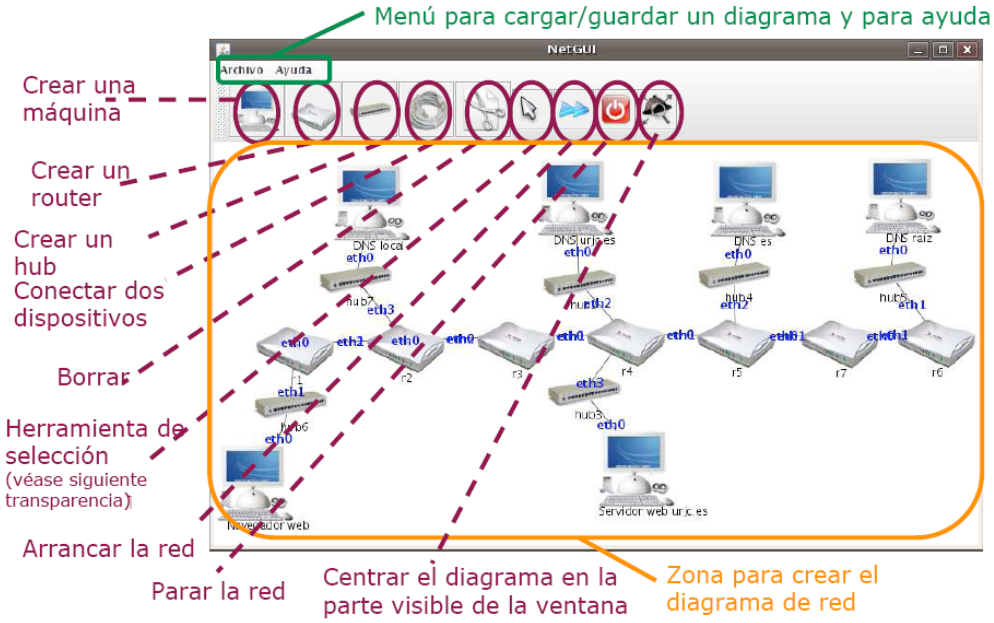
Referencias

[1] Netkit, http://wiki.netkit.org/
[2] NetGUI, http://netlab.sourceforge.net/

Anexo 1: NetGUI

NetGUI se arranca con la orden netgui.

La siguiente figura muestra la pantalla principal de NetGUI.



Para empezar a trabajar con NetGUI es necesario visualizar la red con la que queremos trabajar. En NetGUI hay dos posibilidades para ello. La primera es utilizar la zona para crear el diagrama de red y la herramienta de selección para ir creando la red. La segunda es abrir a través del menú Archivo>Abrir una red previamente guardada.

La herramienta de selección (botón con una flecha con el cursor de un ratón) permite las siguientes funcionalidades:

- Mover un elemento: con el botón izquierdo del ratón se pulsa sobre el elemento a mover y se arrastra al destino.

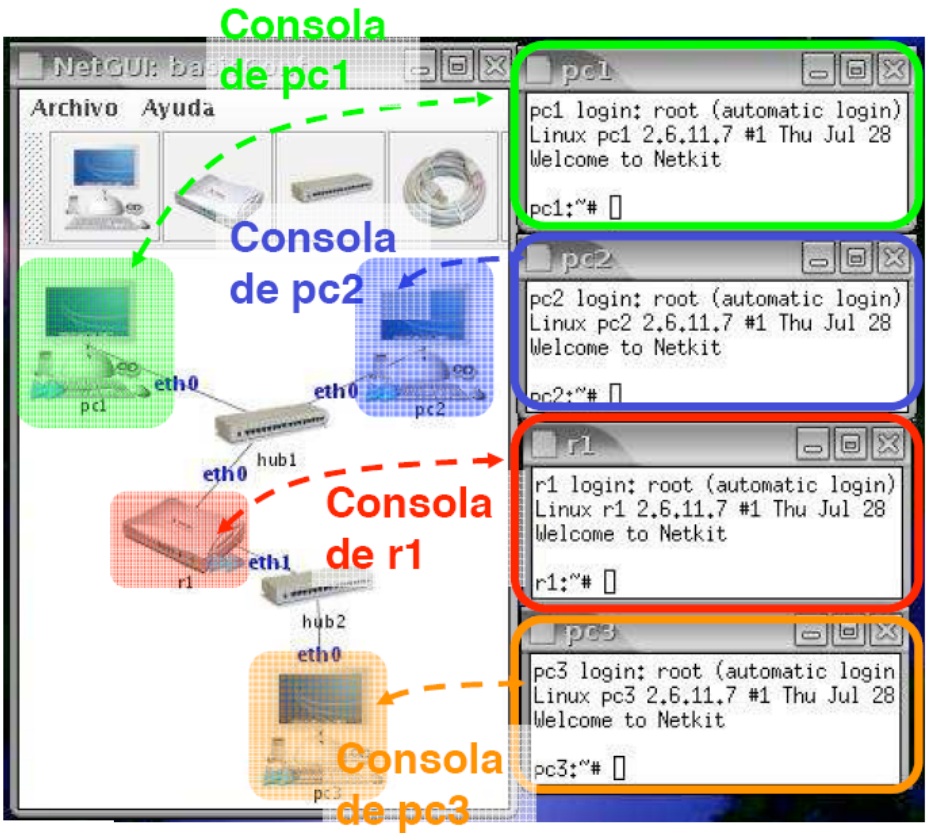
- Arrancar/Parar un nodo (ordenador o router): se pulsa con el botón derecho sobre el nodo. Si está parado se arranca, y si esta arrancado se para. Cuando un nodo está arrancado aparecen dos flechas azules en su icono.

- Mostrar la consola de un nodo arrancado: cuando se arranca un nodo, se lanza una ventana con la consola de ese nodo. Sobre esa consola es sobre la que se trabajará para la configuración del nodo y el análisis del tráfico que lo atraviesa. Haciendo doble click con el botón izquierdo sobre el nodo aparece en primer plano la ventana de la consola del nodo.

- Zoom: pulsando el botón derecho del ratón sobre el fondo de la ventana en cualquier lugar en la que no haya un elemento y moviendo el ratón a derecho o izquierda, se obtiene el efecto de zoom.

- Desplazamiento: pulsando el botón izquierdo del ratón sobre el fondo de la ventana en cualquier lugar en la que no haya un elemento y moviendo el ratón mientras se mantiene el botón pulsado, se puede cambiar la situación de la red dibujada.

En la siguiente figura se muestran las consolas abiertas para las máquinas de una red:



Como se puede comprobar, cada nodo que está arrancado tiene asociada una consola de Linux.