Seguridad en Redes de Ordenadores
Práctica 1: OpenVPN

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación
Versión 2

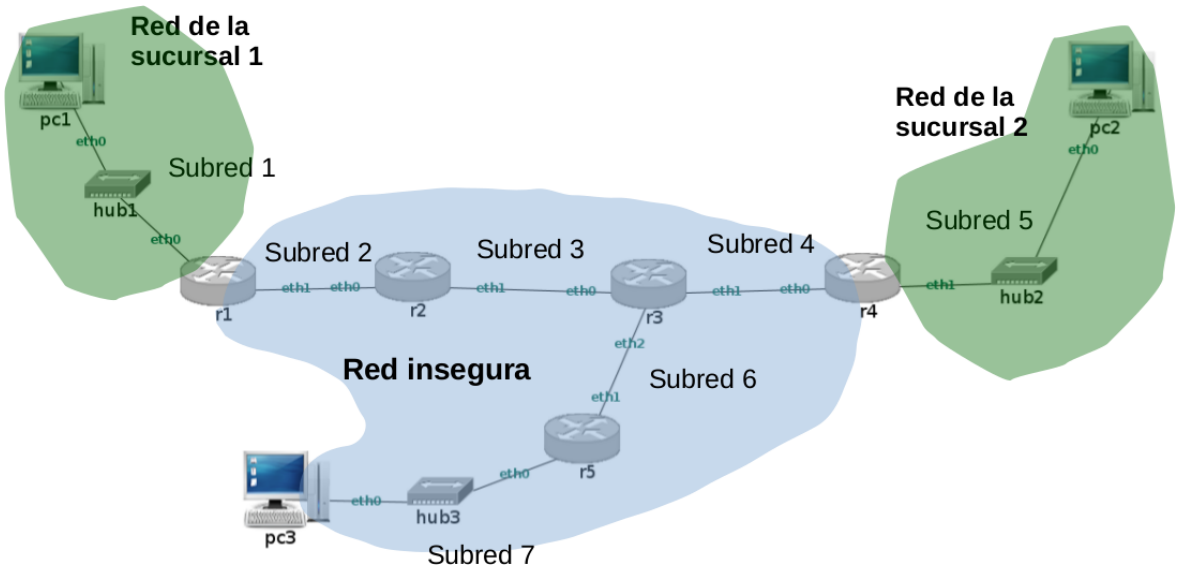
Marzo de 2017

Resumen

El objetivo de esta práctica es configurar VPNs utilizando la herramienta OpenVPN. Esta práctica se va a realizar con la herramienta netgui-ng.sh. Es muy importante que arranques esta herramienta y no `netgui.sh` ya que la nueva versión de NetGUI tiene instalados paquetes necesarios para la realización de la práctica.

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.



Descomprime el escenario de Netgui-NG `lab-ipsec.tgz` y carga ese escenario dentro de NetGUI-NG, se debería mostrar la configuración de la siguiente figura:

Configura las direcciones IP a las interfaces de red en cada subred atendiendo al identificador `<ID>` que se te ha asignado en clase:

Subred 1 (privada)	`10.<ID>.1.0/24`
Subred 2 (pública)	`100.<ID>.2.0/24`
Subred 3 (pública)	`100.<ID>.3.0/24`
Subred 4 (pública)	`100.<ID>.4.0/24`
Subred 5 (privada)	`10.<ID>.2.0/24`
Subred 6 (pública)	`100.<ID>.6.0/24`
Subred 7 (pública)	`100.<ID>.7.0/24`

Utiliza el fichero `/etc/network/interfaces` para que los cambios queden almacenados de forma permanente. Configura también las rutas para que:

- Todos los routers tengan conectividad con todas las subredes de la red insegura.
- Los pcs tengan una ruta por defecto al router al que están directamente conectados.

En el fichero `/etc/hosts` de todas las máquinas añade todas las asociaciones entre direcciones IP y nombres:

```
<IPpc1>          pc1
<IPr1(eth0)>     r1
<IPr1(eth1)>     r1
<IPr2(eth0)>     r2
<IPr2(eth1)>     r2
...
```

Una vez que hayas realizado esta configuración, vas a realizar una copia de seguridad de los ficheros que has modificado. Para ello ejecuta **en cada máquina** el siguiente comando, por ejemplo para `r1`:

```
r1:~# cp /etc/network/interfaces /hostlab/r1.old/etc/network
r1:~# cp /etc/hosts /hostlab/r1.old/etc
```

Si en algún momento alguna máquina virtual no arranca bien, tendrás almacenados los ficheros de configuración en la máquina real. Para recuperar la configuración cierra NetGUI-NG y ejecuta en la máquina real el siguiente comando para matar todos los procesos de NetGUI-NG (por si alguna de las máquinas no se puede cerrar):

```
clean-netgui.sh
```

A continuación recupera los ficheros de la máquina que tenía problemas ejecutando el siguiente comando **en la carpeta donde has descomprimido el escenario** indicando el nombre de la máquina que quieres recuperar:

```
./reset <nombreMáquina>
```

Vuelve a arrancar NetGUI-NG con el comando netgui-ng.sh.

Incluye en la memoria:

1. Una imagen de la interfaz de NetGUI-NG donde se vean las direcciones IP que has configurado en tu escenario.

2. Configuración openVPN

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 openVPN en el que se va instalar un servidor openVPN en `r4` y un cliente openVPN en `r1`.

Adicionalmente hay un trabajador que se encuentra trabajando fuera de las oficinas de la empresa en `pc3` y que desea comunicarse con los ordenadores de la Sucursal2. Por ello, `pc3` también tendrá configurado un cliente openVPN que se comunique con el servidor de `r4`.

2.1. Generación de certificados

La autenticación de los extremos del túnel se va a realizar con certificados X.509. Para ello, la empresa decide crear los certificados necesarios para todos los extremos del túnel.

En `pc1` crea un certificado autofirmado de una autoridad de certificación (CA) que te inventes, los parámetros Diffie-Hellman y los certificados para `r1`, `r4` y `pc3` firmados por la CA.
En cada una de las máquinas `r1`, `r4` y `pc3` deberás dejar los ficheros necesarios para realizar las operaciones de autenticación del túnel en la carpeta `/etc/openvpn`[1].

Indica en la memoria las siguientes cuestiones:

1. 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 en la memoria el resultado de imprimir de forma legible cada uno de los certificados que has creado.
3. Observa los números de serie de los certificados y explícalos.

[1] Para copiar los ficheros en las máquinas adecuadas, primero desde la máquina virtual cópialos a /hosthome y una vez que estén en /hosthome puedes copiar desde /hosthome a la máquina virtual donde los desees dejar. Por ejemplo:
pc1: cp ca.cert /hosthome
r1: cp /hosthome/ca.cert /etc/openvpn

2.2. Configuración del extremo servidor r4

Configura el fichero `server.conf` dentro de `/etc/openvpn` de `r4` para crear una configuración UDP en el puerto 1194. El servidor openVPN deberá asignar a las máquinas que se comunican a través de la VPN el siguiente rango de subred: `10.<ID>.8.0/24`

Haz una copia de la carpeta `/etc/openvpn` de `r4` en la máquina real por si la máquina virtual deja de funcionar:

```
cp -r /etc/openvpn /hostlab/r4.old/etc
```

1. Incluye en la memoria las líneas que no estén comentadas del fichero `server.conf`.

2.3. Configuración del extremo cliente r1

Configura el fichero `client.conf` dentro de `/etc/openvpn` de `r1` para que se conecte al servidor de `r4`.

Haz una copia de la carpeta `/etc/openvpn` de `r1` en la máquina real por si la máquina virtual deja de funcionar:

```
cp -r /etc/openvpn /hostlab/r1.old/etc
```

1. Incluye en la memoria las líneas que no estén comentadas del fichero `client.conf` de `r1`.

2.4. Configuración del extremo cliente pc3

Configura el fichero `client.conf` dentro de `/etc/openvpn` de `pc3` para que se conecte al servidor de `r4`.
Haz una copia de la carpeta `/etc/openvpn` de `pc3` en la máquina real:

```
cp -r /etc/openvpn /hostlab/pc3.old/etc
```

1. Incluye en la memoria las líneas que no estén comentadas del fichero `client.conf` de `pc3`.

2.5. Túnel entre pc3 y r4

En este apartado se va a poner a prueba el túnel OpenVPN entre `pc3` y `r4`:

- Arranca el servidor OpenVPN e inicia una captura de tráfico en `r4(eth0)` de forma que se capture todo el tráfico en el fichero `openvpn-01.cap`[2].
- Arranca el cliente en `pc3`.
- Realiza un `ping` desde `pc3` hacia `r4` enviando 3 paquetes ICMP Echo Request sin usar el túnel.
- Realiza un segundo `ping` desde `pc3` hacia `r4` enviando 3 paquetes ICMP Echo Request usando el túnel.
- Interrumpe la captura que has realizado (Ctrl+C)

Responde a las siguientes cuestiones en la memoria:

1. ¿Qué dirección IP destino has especificado en el `ping` para enviar los paquetes desde `pc3` a `r4` utilizando el túnel y sin utilizar el túnel? ¿Por qué?
2. Indica qué direcciones IP se han asignado al dispositivo `tun0` en `r4` y por qué.
3. Indica qué direcciones IP se han asignado al dispositivo `tun0` en `pc3` y por qué.
4. Explica la tabla de encaminamiento de `pc3`.
5. Explica la tabla de encaminamiento de `r4`.
6. ¿Qué ocurre si se realiza un `ping` desde `pc3` a cada una de las direcciones que muestra `tun0` en `r1`? ¿Por qué?
7. Abre la captura `openvpn-01.cap` en Wireshark y explica el contenido:
   a) Indica el identificador de sesión local y remoto que se establece en los mensajes `P_CONTROL_HARD_RESET` y fíjate como aparece en todos los mensajes posteriores.
   b) Observa el campo `Message Packet-ID` indica cuál es su valor incial para el cliente y para el servidor. Explica cómo va cambiando en cada uno de los paquetes `P_CONTROL` que se envían.
   c) ¿Por qué los mensajes `P_ACK` no llevan el campo `Message Packet-ID`?
   d) ¿En qué paquete se asiente el mensaje `P_CONTROL_HARD_RESET_CLIENT_V2`? ¿Cómo lo sabes?
   e) ¿En qué paquete se asiente el mensaje `P_CONTROL_HARD_RESET_SERVER_V2`? ¿Cómo lo sabes?

[2] r4: tcpdump -i eth0 -s 0 -w /hosthome/openvpn-01.cap

f) El primer mensaje que envía el cliente al servidor del SSL/TLS handshake es `Client Hello`. ¿Alguno de los campos viaja cifrado?

g) Localiza el primer mensaje que envía el servidor al cliente para establecer SSL/TLS handshake, es `Server Hello`. ¿Alguno de los campos viaja cifrado? Indica si contiene certificados y cuáles contiene. Localiza los parámetros Diffie-Hellman e indica la longitud de p y el valor de g. Fíjate como el servidor le envía un valor `PubKey` del servidor para crear el secreto compartido. Indica el algoritmo de cifrado que ha elegido el servidor [3].

h) Localiza el siguiente mensaje que envía el cliente al servidor `Certificate, Client key Exchange ...`. ¿Alguno de los campos viaja cifrado? Indica si contiene certificados y cuáles contiene. Fíjate como el cliente le envía al servidor el valor `PubKey` del cliente.

i) Localiza el siguiente mensaje que envía el servidor al cliente `New session ticket ...`. ¿Alguno de los campos viaja cifrado?

j) Observa el contenido de los mensajes `P_DATA`. ¿Por qué no llevan el campo `Message Packet-ID`?

k) ¿Qué crees que hay dentro de los mensajes `P_DATA`?

2.6. Conectividad entre entre pc3 y pc2

Responde razonadamente a las siguientes cuestiones en la memoria:

1. ¿Qué crees que ocurrirá si desde `pc3` se envía un `ping` a `pc2`?
2. Modifica la configuración de `r4` para que el `ping` de `pc3` a `pc2` vaya a través del túnel OpenVPN. Explica en la memoria qué has modificado.
3. Realiza una captura en `r4(eth0)` (fichero `openvpn-02.cap`) y en `pc2` (fichero `openvpn-03.cap`) mientras ejecutas el `ping` y explica las capturas.
4. Explica la tabla de encaminamiento que tiene `pc3` y las diferencias con la tabla de encaminamiento que viste en el apartado anterior.
5. ¿Crees que `pc2` sabe que se está usando un túnel openVPN? ¿Por qué?

2.7. Túnel entre r1 y r4

En este apartado se va a poner a prueba el túnel OpenVPN entre `r1` y `r4`. Mantén la configuración realizada anteriormente y ahora:

- Inicia una captura de tráfico en `r4(eth0)` de forma que se capture todo el tráfico en el fichero `openvpn-04.cap`.
- Arranca el cliente en `r1`.
- Realiza un `ping` desde `r1` hacia `r4` enviando 3 paquetes ICMP Echo Request sin usar el túnel.
- Realiza un segundo `ping` desde `r1` hacia `r4` enviando 3 paquetes ICMP Echo Request usando el túnel.
- Interrumpe la captura que has realizado (Ctrl+C)

Responde razonadamente a las siguientes cuestiones en la memoria:

1. ¿Qué crees que ocurrirá si desde `r1` se envía un `ping` a `pc2`?
2. Explica la tabla de encaminamiento que tiene `pc3` y las diferencias con la tabla de encaminamiento que viste en el apartado anterior.
3. ¿Qué crees que ocurrirá si desde `pc1` se envía un `ping` a `pc2`? ¿Por qué?
4. Modifica la configuración en `r4` para permitir que `r4` alcance las direcciones IP de la Subred1. Indica las modificaciones en la memoria. Comprueba que ahora funciona. No olvides guardar el fichero de configuración que has modificado en la máquina virtual.

2.8. Conectividad entre entre pc3 y pc1

Responde razonadamente a las siguientes cuestiones en la memoria:

1. ¿Qué crees que ocurrirá si desde `pc3` se envía un `ping` a `pc1`? ¿Por qué?
2. Modifica la configuración en `r4` para permitir que `r4` anuncie las subredes internas del cliente `r1` (Subred1) al cliente `pc3`. No olvides guardar el fichero que has modificado en la máquina virtual.
3. Realiza una captura de tráfico (`openvlan-05.cap`) en `r4(eth0)` que muestre que funciona un `ping` desde `pc3` a `pc1`. Explica los paquetes capturados.
4. Explica la tabla de encaminamiento que tienen `pc3` y `r1` y las diferencias con la tablas de encaminamiento que tenían previamente.

[3] Este algoritmo usa Diffie Hellman efímero (Diffie Hellman Ephemeral, DHE), donde DH sólo se utiliza para establecer una clave de sesión TLS, a partir de ese momento se descarta DH y se usa clave de sesión TLS. Por este motivo no se pude descifrar el contenido con Wireshark.

3. Normas de entrega

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

- La memoria en formato pdf.
- Un archivo `openvpn-caps.tgz` que contenga los ficheros con las capturas de `openvpn-01.cap` a `openvpn-05.cap`