Trabajo Práctico #11 Seguridad en Redes

“Redes Virtuales mediante OpeVPN / TLS”

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

OpenVPN es un software basado en Transport Layer Security (TLS) que permite crear redes privadas virtuales entre dos o más nodos, sobre una red pública tal como es Internet. Opera en forma cliente/servidor mediante en la creación de interfaces de red virtuales denominadas tunel (para túneles que transportan paquetes IP) o tap (en el caso de túneles transportan tramas Ethernet).
En esta práctica crearemos un túnel para transporte de paquetes IP utilizando OpenVPN en modo “routing”

Prueba de una conexión VPN local. Para ello, iniciar el extremo del túnel en el servidor:

```
root@Redes:~# openvpn --dev tun1 --ifconfig 10.9.8.1 10.9.8.2
Thu Nov 10 15:22:57 2016 OpenVPN 2.3.4 i586-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[EPOLL] [PKCS11] [MH] [IPv6] built on Nov 19 2015
Thu Nov 10 15:22:57 2016 library versions: OpenSSL 1.0.1t  3 May 2016, LZO 2.08
Thu Nov 10 15:22:57 2016 ******* WARNING *******: all encryption and
authentication features disabled -- all data will be tunnelled as cleartext
Thu Nov 10 15:22:57 2016 TUN/TAP device tun1 opened
Thu Nov 10 15:22:57 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu Nov 10 15:22:57 2016 /sbin/ip link set dev tun1 up mtu 1500
Thu Nov 10 15:22:57 2016 /sbin/ip addr add dev tun1 local 10.9.8.1 peer 10.9.8.2
Thu Nov 10 15:22:57 2016 UDPv4 link local (bound): [undef]
Thu Nov 10 15:22:57 2016 UDPv4 link remote: [undef]
```

Verificar que la interfaz del túnel (tun1) punto a punto está activa mediante el comando ip:

```
root@Redes:/home/alumno# ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
mode DEFAULT group default qlen 1000
    link/ether 90:2b:34:6e:73:3c brd ff:ff:ff:ff:ff:ff
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state
DOWN mode DEFAULT group default qlen 1000
    link/ether a0:f3:c1:00:dc:43 brd ff:ff:ff:ff:ff:ff
4: tun1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
state UNKNOWN mode DEFAULT group default qlen 100
    link/none

root@Redes:/home/alumno# ifconfig tun1
tun1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00-00
          inet addr:10.9.8.1  P-t-P:10.9.8.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

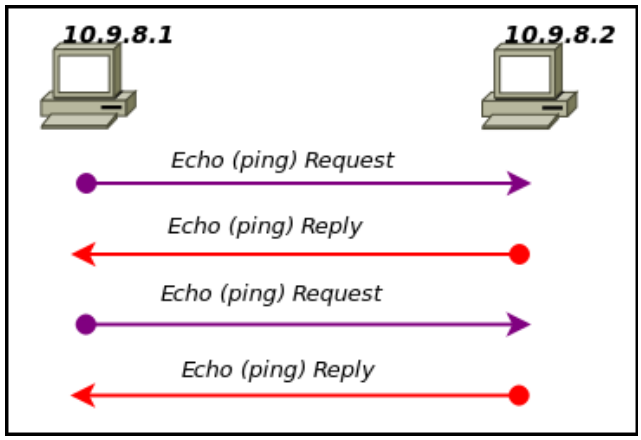
Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

Comprobar que el túnel opera adecuadamente realizando un echo request/reply:

```
PING 10.9.8.2 (10.9.8.2) 56(84) bytes of data.
64 bytes from 10.9.8.2: icmp_seq=1 ttl=64 time=0.885 ms
64 bytes from 10.9.8.2: icmp_seq=2 ttl=64 time=0.865 ms
64 bytes from 10.9.8.2: icmp_seq=3 ttl=64 time=0.856 ms
64 bytes from 10.9.8.2: icmp_seq=4 ttl=64 time=0.856 ms
^C
--- 10.9.8.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.856/0.865/0.885/0.031 ms
root@Redes:/home/alumno#
```

En la captura solamente puede observarse que para establecimiento de conexión se transmiten y reciben paquetes OpenVPN sobre UDP por la red fisica. El software utilizado para capturar (Wireshark) no interpreta bien las tramas como para realizar un esquema de intercambio de mensajes.

Cuando hacemos ping, vemos que los paquetes ICMP se transmiten y reciben por la red virtual (PPTP), para ello se transmiten y reciben paquetes por la red fisica, utilizando el protocolo OpenVPN sobre UDP.



Bajo esta configuración no se provee ningún servicio de seguridad ya que no se esta haciendo uso de ningún protocolo.

a) En el servidor, crear una nueva clave:

En el servidor, crear una nueva clave, dicha clave es generada al azar:

```
root@Redes:~# openvpn --genkey --secret static.key
```

b) Configuración de la interfaz. En el servidor, cree el archivo /etc/openvpn/tun0.conf para configurar la interfaz y luego incorpore los siguientes parámetros:

```
dev tun0
```

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
ifconfig 10.9.8.1 10.9.8.2
secret /etc/openvpn/static.key
```

¿Qué identifican las direcciones IP del comando ifconfig?
Dichas direcciones identifican al servidor y al cliente de la conexión.

c) En el cliente, configure también una interfaz en el archivo /etc/openvpn/tun0.conf con los siguientes parámetros:

```
remote ip-del-servidor
dev tun0
ifconfig 10.9.8.2 10.9.8.1
secret /etc/openvpn/static.key
```

d) Por último, para levantar la VPN utilice la siguiente instrucción:

```
openvpn --config /etc/openvpn/tun0.conf
```

- Realice una captura antes de establecer la VPN en el punto

c) - En función de quienes poseen la clave, ¿Qué tipo de seguridad le sugiere esta solución de VPN? ¿Qué método de seguridad se utiliza para autenticar los extremos?

Se procede a levantar el archivo de configuración para que la misma sea cargada:

```
root@Redes:~# openvpn --config /etc/openvpn/tun0.conf
Thu Nov 10 16:05:50 2016 OpenVPN 2.3.4 i586-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[EPOLL] [PKCS11] [MH] [IPv6] built on Nov 19 2015
Thu Nov 10 16:05:50 2016 library versions: OpenSSL 1.0.1t  3 May 2016, LZO 2.08
Thu Nov 10 16:05:50 2016 TUN/TAP device tun0 opened
Thu Nov 10 16:05:50 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu Nov 10 16:05:50 2016 /sbin/ip link set dev tun0 up mtu 1500
Thu Nov 10 16:05:50 2016 /sbin/ip addr add dev tun0 local 10.9.8.1 peer 10.9.8.2
Thu Nov 10 16:05:50 2016 UDPv4 link local (bound): [undef]
Thu Nov 10 16:05:50 2016 UDPv4 link remote: [undef]
```

<Aca se conecta el cliente>

```
Thu Nov 10 16:08:39 2016 Peer Connection Initiated with [AF_INET]10.4.10.32:1194
Thu Nov 10 16:08:39 2016 Initialization Sequence Compled
```

Esta configuración provee servicios de confidencialidad. No se autentican los extremos, así que no provee Autenticación ni No Repudio.
La solución que se sugiere de VPN es criptografía simétrica.

Agregamos la linea

```
proto tcp-server
```

Al archivo de configuración, y volvemos a correr el servidor:

```
root@Redes:~# openvpn --config /etc/openvpn/tun0.conf
```

Trabajo Práctico #11 Seguridad en Redes

"Redes Virtuales mediante OpeVPN / TLS"

Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

```
Thu Nov 10 16:22:26 2016 OpenVPN 2.3.4 i586-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[EPOLL] [PKCS11] [MH] [IPv6] built on Nov 19 2015
Thu Nov 10 16:22:26 2016 library versions: OpenSSL 1.0.1t  3 May 2016, LZO 2.08
Thu Nov 10 16:22:26 2016 TUN/TAP device tun0 opened
Thu Nov 10 16:22:26 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Thu Nov 10 16:22:26 2016 /sbin/ip link set dev tun0 up mtu 1500
Thu Nov 10 16:22:26 2016 /sbin/ip addr add dev tun0 local 10.9.8.1 peer 10.9.8.2
Thu Nov 10 16:22:26 2016 Listening for incoming TCP connection on [undef]
Thu Nov 10 16:22:30 2016 TCP connection established with
[AF_INET]10.4.10.32:38004
Thu Nov 10 16:22:30 2016 TCPv4_SERVER link local (bound): [undef]
Thu Nov 10 16:22:30 2016 TCPv4_SERVER link remote: [AF_INET]10.4.10.32:38004
Thu Nov 10 16:22:40 2016 Peer Connection Initiated with
[AF_INET]10.4.10.32:38004
Thu Nov 10 16:22:41 2016 Initialization Sequence Completed
```

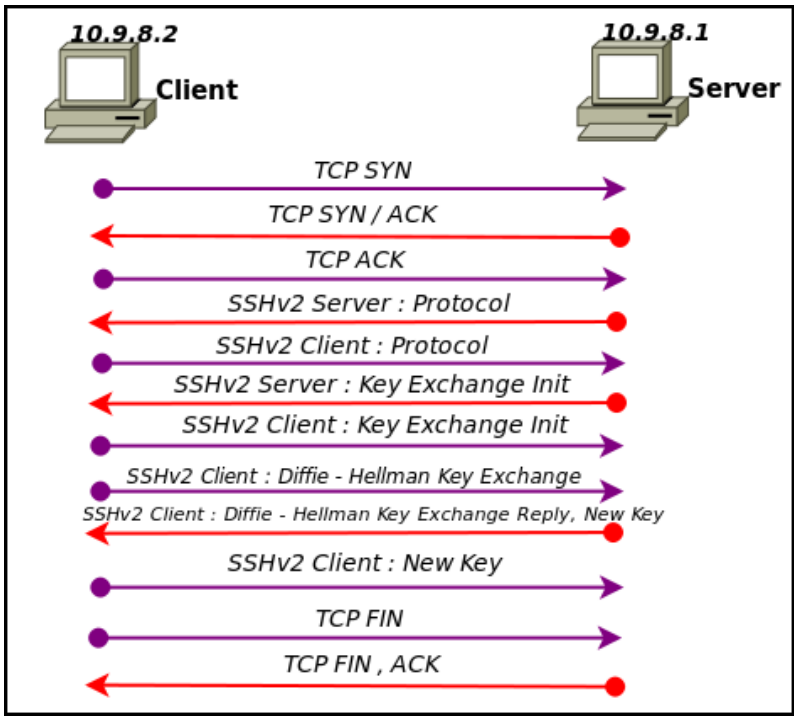
Enunciados:

1. Antes de reiniciar los servicios inicie la captura sobre la interfaz física ethN. Luego haga una prueba con ping. ¿Es posible ver los mensajes ICMP que viajan a través de la VPN?

Al no utilizar ninguna configuración de seguridad, es posible visualizar el intercambio de mensajes echo/request. En cambio, con los servicios de seguridad activos, ya sea mediante criptografía simétrica o asimétrica, no es posible ver los mensajes ICMP que viajan encapsulados por la interfaz física.

2. Intente realizar una conexión SSH a través de la VPN ¿Qué se observa en la captura?

En la captura se observa que el cliente y el servidor realizan un intercambio de claves publicas, y a continuación, los paquetes se transmiten encriptados.



Medina, Ma. Victoria [117024]
medina.vicc@gmail.com

3. Cambie en ambos extremos el parámetro PROTO a tcp y reinicie los servicios. Repita la prueba anterior. ¿Qué diferencias se observan en la captura? ¿Se perciben cambios en el comportamiento de SSH? ¿Cómo puede impactar esto al rendimiento? ¿Por qué considera que es así?

No se perciben diferencias en el comportamiento.
Utilizar TCP para transportar OpenVPN implica realizar dos veces el control de flujo y de congestión que provee TCP. Esto no solo es innecesario, sino que puede impactar negativamente en el rendimiento.