#Jenny

Finally I get this ebook, thanks for all these I can get now!

#Rio

Cool! I'am really happy

#Markus Jensen

I did not think that this would work, my best friend showed me this website, and it does! I get my most wanted eBook

#Hun Tsu

wtf this great ebook for free?!

#Che Salsa

My friends are so mad that they do not know how I have all the high quality ebook which they do not!

#Diego Butler

so many fake sites. this is the first one which worked! Many thanks

Capítulo 7. IPsec: IP segura sobre Internet

7.1. Introducción al intercambio manual de claves

IPSEC es un tema complicado. Hay mucha información en la red, pero este COMO se concentrará en enseñarle a ponerlo a funcionar y explicar los principios básicos. Todos los ejemplos están basados en Racoon, que encontrará en el enlace anterior.

Nota: ¡Muchas configuraciones de iptables eliminan paquetes de IPSEC! Para dejar pasar IPSEC, use: "iptables -A xxx -p 50 -j ACCEPT" o "iptables -A xxx -p 51 -j ACCEPT"

IPSEC ofrece una versión segura del Internet Protocol. La seguridad en este contexto significa dos cosas diferentes: cifrado y autentificación. Una visión inocente de la seguridad ofrece sólo cifrado, pero es sencillo demostrar que esto es insuficiente: puedes estar comunicándote de forma cifrada, pero no hay garantías de que en el otro extremo esté quien tú esperas.

IPSEC admite "Encapsulated Security Payload" (ESP) para el cifrado y "Authentication Header" (AH) para autentificar al otro extremo. Puede configurarlos ambos, o decidir usar sólo uno.

Tanto ESP como AH dependen de asociaciones de seguridad (security associations). Una asociación de seguridad (SA) consiste en origen, destino y una instrucción. Un ejemplo de autentificación por SA podría ser así:

```
add 10.0.0.11 10.0.0.216 ah 15700 -A hmac-md5 "12345678901234567";
```

Esto significa «el tráfico que va de 10.0.0.11 a 10.0.0.216 que necesita AH puede ser firmado usando HMAC-MD5 usando la clave 12345678901234567». Esta instrucción va etiquetada con el identificador SPI ("Security Parameter Index") "15700", hablaremos de ello más adelante. La parte interesante sobre los SA es que son simétricos. Ambos extremos de una conversación comparten exactamente el mismo SA; en el otro extremo no encontraremos una copia especular. Tenga en cuenta sin embargo que no hay una regla "autoreverse": esta SA sólo describe una autentificación posible desde 10.0.0.11 a 10.0.0.216. Para tener tráfico en las dos direcciones, hacen falta dos SA.

Un ejemplo de SA ESP:

```
add 10.0.0.11 10.0.0.216 esp 15701 -E 3des-cbc "123456789012123456789012";
```

Aquí dice que «el tráfico que va de 10.0.0.11 a 10.0.0.216 que necesita cifrado puede serlo usando 3desvbc con la clave 123456789012123456789012». El identificador SPI es "15701".

Hasta ahora, hemos visto que las SA describen instrucciones posibles, pero en realidad no describen normas sobre cuándo se deben usar. En realidad, podría haber un número arbitrario de SA idénticas que sólo difirieses en sus id SPI. Casualmente, SPI significa Security Parameter Index. Para hacer cifrado realmente, necesitamos describir una norma (policy). Esta norma puede incluir cosas como «usa ipsec si está disponible» o «corta el tráfico a menos que haya ipsec».

25

Download PDF version of :

Manual Iptables Avanzado