

El Día a Día del Administrador de Sistemas: Autenticación de Paquetes Individuales

EXPERIENCIA CON CLAVES

Normalmente, la técnica del golpeo de puertos está abierta a atacantes que utilizan la fuerza bruta o algún sniffer. Enviar un paquete cifrado con la petición de acceso al servidor es más seguro y moderno. Aprenda más sobre Firewall Knock Operator, también conocido como Fwknop.

El golpeo de puertos convencional, que expliqué el mes pasado [1], le protege contra atacantes que escanean de forma rutinaria redes enteras buscando cualquier oportunidad. Un cracker que se tome su tiempo y registre la comunicación puede identificar señales de golpeo, ya que las secuencias se repiten.

En teoría, podría considerarse el uso de listas de señales de golpeo de un sólo uso que quedan obsoletas tras utilizarse. Desafortunadamente, es muy complejo. Además, si el administrador no es muy creativo, un atacante podría intentar con secuencias conocidas de golpeo (puerto 7000, 8000, 9000, ...) para conseguir el acceso.

Una posible solución puede ser la Autenticación de Paquetes Individuales (SPA). El sistema de golpeo envía un sólo paquete conteniendo las credenciales de autenticación cifradas, normalmente una frase de paso, y el cliente responde abriendo un puerto específico. Una imple-

```

charly@funghi:~$ fwknop -A tcp/22 -a 10.254.75.80 -k 10.254.75.80

[+] Starting fwknop client (SPA mode)...
[+] Enter an encryption key. This key must match a key in the file
/etc/fwknop/access.conf on the remote system.

Encryption Key:

[+] Building encrypted Single Packet Authorization (SPA) message...
[+] Packet fields:

    Random data:    7842749886485723
    Username:      charly
    Timestamp:     1214918141
    Version:       1.9.5
    Type:          1 (access mode)
    Access:        10.254.75.80, tcp/22
    SHA256 digest: evcTZFKgUbKIk/Nm28LaJwFInmIb/ENFTFiTooKSTIA

[+] Sending 182 byte message to 10.254.75.80 over udp/62201...

charly@funghi:~$

```

Figura 1: El cliente llama a la puerta del puerto 22 permitiéndole el paso porque tiene la clave correcta.

mentación SPA que funciona muy bien es Firewall Knock Operator, o Fwknop [2].

Además de las herramientas de compilación, la instalación requiere Perl, el paquete libpcap-dev y el módulo Net::Pcap. Tras la instalación de todos estos recursos, se instala Fwknop, que es una gozada gracias al instalador basado en Perl.

Encontrando el Picaporte

Fwknop se compone del servidor *fwknopd* y del cliente *fwknop*. El servidor puede configurarse editando dos ficheros bajo */etc/fwknop/*; *fwknop.conf* contiene la configuración básica. Inicialmente necesitará cambiar un par de parámetros, que están etiquetados con `__CHANGE__`.

Los demás parámetros que se pueden utilizar aquí vienen ya por defecto. Nótese que necesitará sincronizar el tiempo entre el servidor y el cliente, ya que si la diferencia es muy grande, *fwknopd* ignorará el golpeo del cliente.

Las entradas en */etc/fwknopd/access.conf* definen cómo

contesta *fwknopd* a un golpeo del cliente. La clave secreta que el cliente utiliza para identificarse se almacena aquí. La línea *SOURCE* puede utilizarse para restringir redes desde las que el servicio acepta golpes. Para configurar el puerto que el sistema abre para golpes con éxito (por ejemplo, *tcp/22* para SSH) puede utilizar *OPEN_PORTS*. La Figura 1 muestra un intento con éxito. El cliente *fwknop* recoge la clave de su propio */etc/fwknop/access.conf*.

Si la conexión SSH no se abre lo bastante rápido, *FW_ACCESS_TIMEOUT* se dispara en el servidor. Este tiempo normalmente está establecido en 30 segundos, pero yo lo suelo doblar ¡Nunca le meta prisa a un administrador en su trabajo!

SYSADMIN

KSplice68
Cómo actualizar el kernel sin tener que reiniciar la máquina.

RECURSOS

- [1] "Knock-Knock" por Charly Kühnast, Linux Magazine, edición en castellano, Nº 44.
- [2] Fwknop: <http://www.cipherdyne.org/fwknop/>