Port knocking

- Antonio Mario Molina Saorín
- 13 de Julio de 2011
- TC Caldum

Qué buscamos

- Queremos tener un puerto accesible en el exterior. Ej.: ssh
- No queremos que esté abierto para todo el mundo
- Queremos evitar que lo detecten con un escaneo de puertos
- Pero si está cerrado nosotros tampoco podemos conectarnos
- Solución → golpeo de puertos (**pork knocking**)

Cómo funciona - Conexión

- Cerramos el puerto
- Un programa está escuchando los paquetes que llegan al firewall (ej. intentos de conexión),
- o bien está chequeando el log del firewall
- Si no la detecta, simplemente NO HACE NADA (no envía paquetes de vuelta)
- Si es la correcta abre el puerto
- El cliente ya se puede conectar

En qué consiste

- Tenemos el puerto cerrado
- Mediante un ”santo y seña”, esto es, una secuencia de intentos de conexión a diversos puertos, nos ”identificamos” en el firewall
- El port-knocking server (puede ser un simple script) detecta dicha secuencia y abre el puerto (ejecutando los comandos necesarios)
- Si la secuencia es errónea no hace nada (para que el que lo está intentando no tenga ninguna información sobre el sistema).

Cómo funciona - Desconexión

- Cuando el cliente termina su conexión, el puerto debe cerrarse
- Esto se puede hacer por:
  - Timeout
  - Otra secuencia de golpeos
- En cualquier caso → El puerto queda cerrado de nuevo
- Para otra nueva conexión el cliente debe enviar de nuevo la secuencia de golpeos apropiada

Efectiva y versátil (I)

- Secuencia ejemplo: 1000, 2000, 3000
- ¡18 trillones de paquetes necesarios para encontrar la combinación!
- Aún más complicado si se pone un límite de intentos fallidos de golpeo
- El puerto se abre sólo a la dirección IP que lo ha abierto (aunque se puede hacer de cualquier otra forma)
- Por tanto → Podemos abrir un puerto sin intervención directa del administrador

Efectiva y versátil (II)

- Muy poco overhead (consume poca CPU, poco ancho de banda y poca memoria)
- Se pueden usar:
  - Hash criptográficos
  - Listas blancas
  - Listas negras
- Muy útil no sólo para abrir puertos:
  - Ejecución de comandos o scripts, por ejemplo, para hacer cualquier tarea predefinida

Al ajo: Instalación (servidor)

- Instalamos el software
  - # aptitude install knockd
- Editar /etc/default/knockd

  START_KNOCKD=1

  KNOCKD_OPTS=”-i eth0”
- Editar /etc/knock.conf
  - Cambiar secuencias de golpeos, puertos, etc.
  - Se puede dejar por defecto para probarlo
  - Usa Syslog por defecto, pero se puede cambiar:
    - logfile = /var/log/knockd.log

Instalación (cliente)

- Instalamos el software (igual que antes):
  - `# aptitude install knockd`
- Con esto disponemos de *knock*, con el que podemos realizar los golpeos de puertos
- Antes de ver un ejemplo es importante tener en cuenta la política de seguridad del firewall:
  - La idea es que todo el tráfico se deniegue
  - Sólo se aceptará el que expresamente se acepte
- A continuación veremos como configurar la política de seguridad y un ejemplo

Caso práctico

- En el servidor:
  - `iptables -P input DROP`
- Probamos a conectarnos desde el cliente:
  - `ssh -l root IP_SERVIDOR`
- No está disponible el servicio
- Ejecutamos el golpeo de puertos correspondiente a la apertura del puerto
  - `knock -v IP_SERVIDOR 7000 8000 9000`
- Ya podemos conectarnos

Caso práctico (y II)

- Una vez que salimos de la conexión podemos cerrar el puerto con la secuencia de comandos de cierre:
  - `knock -v IP_SERVIDOR 9000 8000 7000`

    (-v es verbose)
- Intentamos de nuevo conectarnos mediante ssh:
  - `ssh -l root IP_SERVIDOR`
- No nos deja ya que está de nuevo cerrado ;-)

Otras posibilidades

- La secuencia de puertos no tiene por qué ser siempre TCP:
  - `sequence = 2222:udp,3333:tcp,4444:udp`
- También se pueden cambiar los FLAGS:
  - `tcpflags = syn,ack`
- Existen clientes para Windows, MAC OS...
  - `http://www.zeroflux.org/projects/knock`
- Para más info: man knockd

Antes de finalizar

- Licenciado bajo Creative Commons
- Reconocimiento - No Comercial - Compartir igual
- Puedes:
- Copiar, reproducir, mostrar públicamente y modificarlo, siempre y cuando cites al autor (o sea, yo),
- no lo uses para fines comerciales,
- y las obras derivadas se mantengan bajo esta misma licencia.

Preguntas

Gracias por vuestra atención