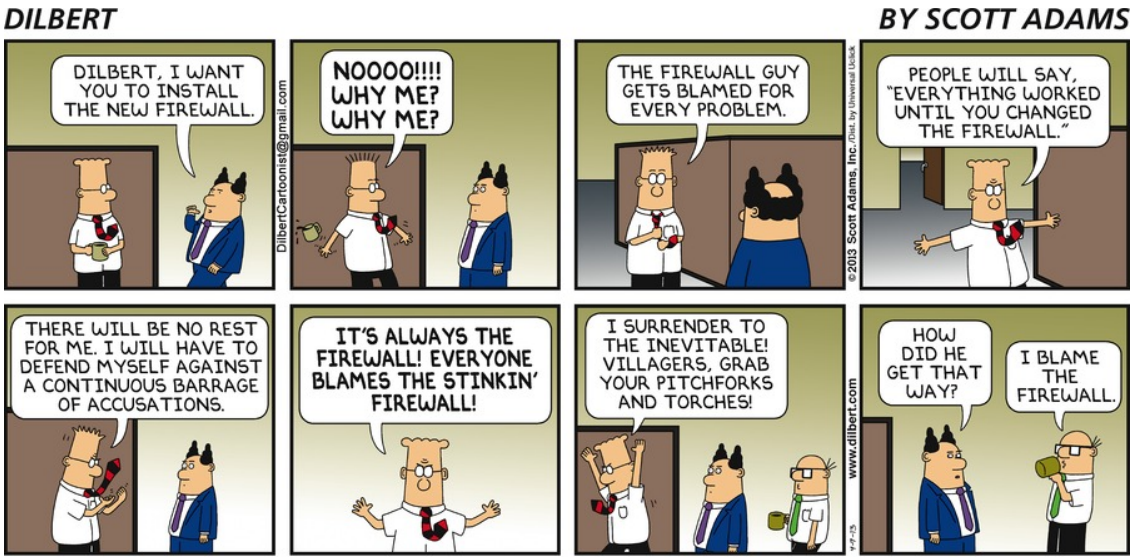
Taller 4: Administración del *firewall* `iptables`

Para el desarrollo de este taller debe crear un informe en formato `.doc` o formato `.odt` en el cual debe colocar las respuestas a todas las preguntas **resaltadas en negritas** que encuentre en las siguientes Secciones. Al finalizar el taller envíe su respectivo informe al profesor. El informe debe incluir su nombre y número de cédula al principio.

1. Taller



`Iptables` y `ip6tables`, su equivalente para el protocolo IPv6, es el sistema de *firewall* o cortafuegos estándar de Linux, el cual se basa en el *framework* de manipulación de paquetes de red *Netfilter*.

El firewall *iptables* se basa en una serie de estructuras lógicas que rigen su funcionamiento. Estas estructuras son:

Tablas corresponden categorías de funcionalidades a aplicar sobre paquetes de red (por ejemplo filtrado, enrutamiento o manipulación). Esta estructura es la que da su nombre a `iptables`.

Cadenas conjuntos de reglas asociadas a una tabla que se aplican sobre los paquetes. Todas las tablas incluyen una serie de cadenas por defecto, aunque es posible definir cadenas personalizadas.

Objetivos acciones que se aplican cuando las reglas de una cadena coinciden con las características de un paquete.

Usando el comando "`man iptables`" investigue cuales son las tablas incluidas en `iptables` y cuales son las cadenas por defecto de cada tabla. No es posible crear nuevas tablas con el comado `iptables`.

Un punto importante a distinguir es que `iptables` puede referirse tanto a el módulo del kernel que implementa el *firewall* como al comando de terminal `iptables` que se usa para configurar el módulo de kernel. El módulo de kernel y el comando son dos componentes de software separados, siendo el comando la única forma disponible al usuario de interactuar y configurar el módulo de kernel. De ahora en adelate cuando este taller indique `iptables` se estará haciendo referencia al comando de terminal a menos que se indique lo contrario. **NOTA:** el comando `iptables` siempre debe ser ejecutado como usuario `root`, de lo contrario fallará.

Para visualizar las cadenas asociadas a una tabla se utiliza el comando "`iptables -t TABLA -L CADENA`", sustituyendo `TABLA` con el nombre de alguna de las tablas disponibles y `CADENA` por el nombre de la cadena a visualizar. **Imprima las reglas disponibles para la cadena `OUTPUT` de la tabla `RAW` usando el comando "`iptables -t raw -L OUTPUT`"**.

Si no se especifica una cadena con la opción `-L` de `iptables` entonces el comando imprimirá las reglas de todas las cadenas asociadas a la tabla. **¿Que tabla se usa por defecto si no se especifica una con `-t`?**.

Para agregar o eliminar reglas con `iptables` se usan las opciones `-A` de *append* y `-D` de *delete* respectivamente. Veamos un ejemplo de como agregar una regla con `iptables`:

```
iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -d DESTINO -m state --state NEW,ESTABLISHED,RELATED -j REJECT
```

Examinemos las opciones usadas en el comando anterior:

- La opción `-A INPUT` indica que se está añadiendo una regla a la cadena `INPUT` de la tabla `filter` (la tabla por defecto).
- La opción `-p icmp` indica el protocolo que debe verificar cada paquete para hacer *match* con la regla. En este caso la regla afecta mensajes del protocolo ICMP.
- La opción `--icmp-type 8` es una opción específica para el protocolo ICMP, la cual indica que solo se deben tratar los paquetes ICMP que poseen tipo ICMP 8[1].
- La opción `-s 0/0`, indica que los paquetes provenientes de cualquier dirección deben ser tratados. Esta opción acepta direcciones IP de la forma `xxx.xxx.xxx.xxx/yy`, donde `yy` es la máscara de red.
- La opción `-d DESTINO`, indica la dirección IP o nombre de dominio de destino que debe poseer el paquete. Es particularmente util en servidores que tienen más de una interfaz de red.
- La opción `-m state` indica el *match* o la regla específica que se quiere validad con respecto al paquete. En este caso se está usando un *match* incluido con el módulo `iptables` que verifica el estado del protocolo. Este estado se especifíca con la opción `--state NEW,ESTABLISHED,RELATED`, la cual es una opción específica del submódulo `state` de `iptables`.
- La opción `-j REJECT` especifica la acción a realizar cuando se consigue un paquete que coincida con la regla especificada. `Iptables` incluye 3 acciones por defecto, las cuales son `ACCEPT`, `DROP`, `REJECT` y `LOG`.

Esta regla especificamente se encargará de bloquear los *ping* entrantes. **Verifique esto ejecutando el comando anterior y luego haciendo un *ping* a la máquina. Verifique que la regla se añadió correctamente usando el comando "`iptables -L`"**.

Para borrar la linea añadida use el comando "`iptables -D INPUT 1`". El número 1 en el comando anterior es el número de la regla dentro de la cadena `INPUT`. **Busque en el manual de `iptables` usando el comando "`man iptables`" en la descripción de la opción `-D` como se enumeran las reglas en `iptables`. Verifique nuevamente con el comando "`iptables -L`" que la regla en cuestión se eliminó correctamente**.

[1] *echo request*, el mensaje que se utiliza para solicitar un *ping*.

2. Post-Taller

1. Diseñe comandos de *iptables* para implementar las siguientes reglas. Pruebe cada comando que diseñe y coloque capturas de pantalla o texto de terminal que demuestren que las reglas funcionan.

   a) Descartar cualquier paquete TCP saliente que tenga como puerto destino el puerto 22. Para especificar el puerto destino de una regla se usa la opción `-dport` *`PUERTO`* del comando `iptables`.

   b) Rechazar todo paquete UDP entrante.

   c) Descartar las respuestas *ping* salientes. El tipo ICMP de la respuesta a un *ping* es `--icmp-type 0` (*echo reply*).

   d) Bloquear toda conexión saliente que vaya a la red local, independientemente del protocolo.

   e) Bloquear todo *ping* **saliente** (nótese que la regla mostrada anteriormente bloque los *ping* **entrantes**).

2. Cambie la regla para bloquear los *pings* mostrada en la sección anterior para que use la acción `DROP` en lugar de `REJECT` y luego ejecute un *ping* a su computadora. ¿Nota alguna diferencia con respecto a la corrida anterior?

`Iptables` es un sistema de cortafuegos considerablemente poderoso. Para averiguar más se recomienda revisar el libro *Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort* de Michael Rash, disponible con la bibliografía recomendada de la materia.