1. ¿Qué sabe la gente de Seguridad sobre Redes ?

Necesidad de nuevos servicios (sink hole, redirección de trafico, etc . a nivel de seguridad).
- bloqueo de usuarios infectados
- Denegaciones de servicio, etc.

Dos grupos separados .
- Area de Red , NOC, etc. -encargados de la gestión de la infrastructura.
- Equipo de seguridad, CERT, CSIRT,etc. problemas de seguridad, mucho tcpdump, firewall y demás.

¿Cómo planificar un servicio de sink hole BGP a nivel de seguridad ?

Solución: Probar las configuraciones en una maqueta , desde el enfoque de seguridad, hasta comprobar que hace falta para que funcione.

- La maqueta debe ser lo suficientemente realista para que la solución sea fácilmente tranportable al mundo real.

- Habrá que hacer simplificaciones, pero estas deben ser razonadas realistas

---

Maquetas:
Una maqueta "fisica", con equipos similares a los de producción.
- Costosa
- dificil de gestionar (ruido, espacio, corriente , etc).

Maquetas virtuales.
- GN3, http://www.gns3.net
- VNX, http://www.dit.upm.es/vnx

Elección de VNX por dos motivos:
- Posibilidad de distribuir escenarios "complejos" en varios equipos
- Cercania con los desarrolladores.

¿Qué hace falta para simular el troncal ? / Creación de la maqueta.

- Simplificación de las conexiones a nivel físico, solamente interfaces ethernet.
  * Solo los enlaces troncales,
  * reducción de los enlaces a redes externas
  * Agregación de enlaces en uno solo .

II / Direccioamiento.

- Direccionamiento estático (/30) para los enlaces entre equipos.
- Asignación de direccioamiento de loopback.
    - No suele utilizarse en los sistemas finales.
    - Resaltar la importancia del interface de loopback en los routers como interface "siempre vivo".

III/ Routing interno.

IS-IS en nuestro caso para poder distribuir la información de enlace entre los distintos routers de la red.

Necesario para que los routers se vean unos a otros.

Malla BGP interna a la hora de enrutar las distintas redes , con un servidor de rutas central.

¿que se tiene con esto ?

Una simulación, de la red en producción donde los de seguridad podamos jugar sin alterar la red.

¿Para qué se puede experimentar ?

-- Sink Hole BGP.
    * Inyección de prefijos por motivos de seguridad.
    * Bloqueos de direcciones IP infectadas
    * Mitigación de DDOS

¿Cómo lo probamos ?

Varias enfoques:
    - Usar el Servidor de Rutas del Area de Red.
    - Servidor de rutas independiente , dentro de la malla BGP.
    - Servidor BPG independiente, como un route reflector. http://tools.ietf.org/html/rfc4456

¿Qué hace falta ?

1. Tener en todos los router una ruta estática a discard (por ejemplo la red 192.168.0.0/16)
Esta red es la que se utilizará para los bloqueos de red.

2. Si se quiere reencaminar el tráfico una red que nos permita el "spoofing"

3. Un servidor de rutas/reflector

El usar el route reflector nos permite:

* Separar la gestión de seguridad de la del área de red.
* Tener "controlados" que puede hacer los de seguridad.
  - Limitar el tamaño del prefijo anunciado.

Configuración en el servidor de rutas/noc:

```
group iBGP-EGIDA {
    type internal;
    local-address route_server_noc;
    import ps-EGIDA-IN;
    family inet {
        any;
    }
    export ps-EGIDA-OUT;
    cluster route_Server_noc;
    neighbor route_server_sec {
        authentication-key "XXX!";
    }
}
```

Politica del route server:

```
policy-statement ps-EGIDA-IN {
    term Aceptar {
        from {
            protocol [ static bgp ];
            route-filter 0.0.0.0/0 prefix-length-range /32-/32;
            prefix-list-filter pl-EGIDA orlonger;
        }
        then {
            local-preference 200;
            community add RedIRIS_egida;
```

```
            accept;
        }
    }
    term Rechazar {
        then reject;
    }
}
```

Configuración del reflector:

```
protocols {
    bgp {
        group egida {
            type internal;
            local-address route_server;
            import politica-egida-IN;
            family inet {
                any;
            }
            family inet6 {
                any;
            }
            export politica-egida;
            cluster route_server_noc;
            neighbour route_server_noc {
                authentication-key "XXXXX; ## SECRET-DATA
            }
        }
```

```
configuration policy-options policy-statement politica-egida-IN
term Rechazar_ALL {
    then reject;
}

term Aceptar {
    from protocol [ static aggregate bgp ];
    then accept;
}
```

Usos:

* En modo experimental para la mitigación de DNS changer.

--> Cansados de las alertas de entes externos notificando máquinas infectadas
--> Redirección de todas las redes DNSchanger a servidor DNS propio.
---> Respuesta "limpia" y aviso a los clientes infectados.

* Problema: Los usuarios no limpiaban el equipo.
---> Redirección de las peticiones DNS (usando RPZ) a página indicando la infección.

Filtros mantenidos hasta mayo 2013.

Usos 2: Bloqueo de máquinas infectadas.

---> redirección de maquinas infectadas// Páginas WWW de phising o malware. cuyos administradores no responden.

-----> reenvio a dirección IP con servidor WWW de notificación.
---> Bastante efectivo , los usuarios quieren que se vea su página.

Otros usos:

- Reutilización de rangos no usados como Darknet.
- Mitigación de ataques DDOS
    - descarte del tráfico
    - Reenvio a máquinas específicas

Estado real del proyecto:
- Todo el sistema esta ahora mismo en modo experimental.
- Servidor de rutas en máquina virtual con Junos
- Red de de trafico no separada del trafico real.