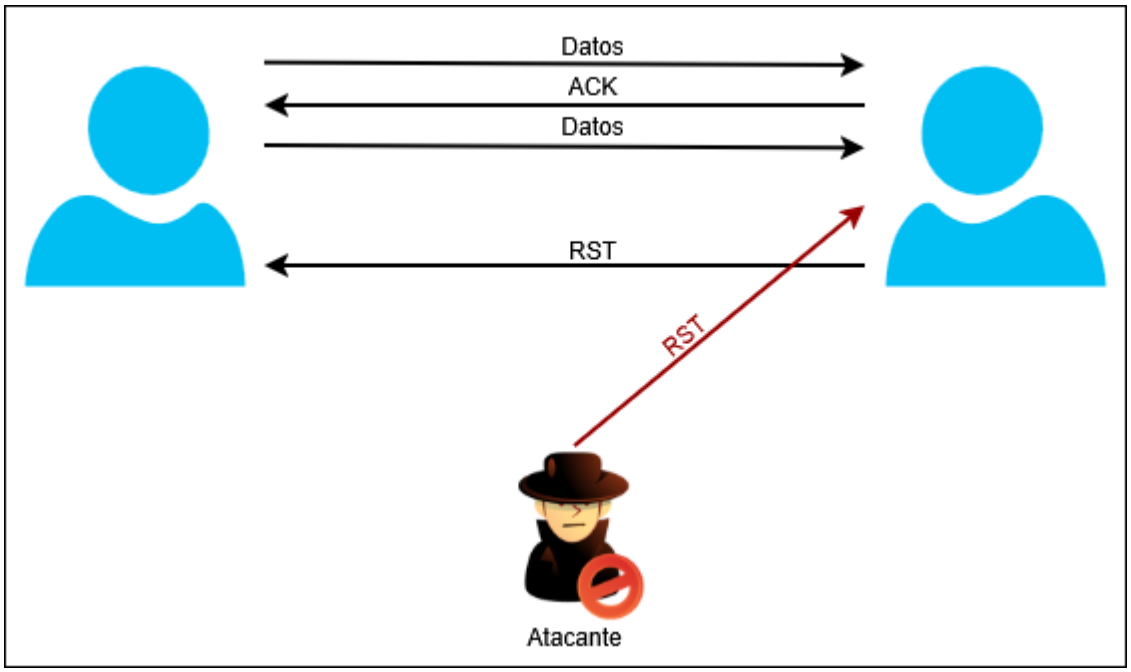
Securizando la infraestrucura de internet

Problemas de seguridad comunes en TCP

Disponibilidad

Ataque TCP reset

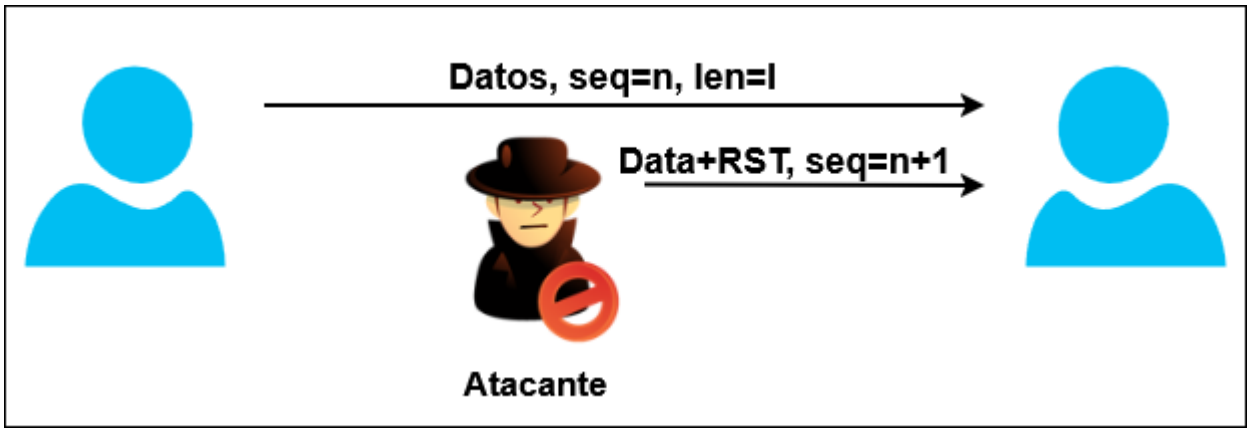
El Flag ReSeT (RST) provoca la caida de la conexión, normalmente se usa para recuperación de errores. El atacnte ijecta un marco con el flag RST activo, provocando que el receptor corte la conexión inmediatamente.



El ataque tiene los siguientes requisitos:

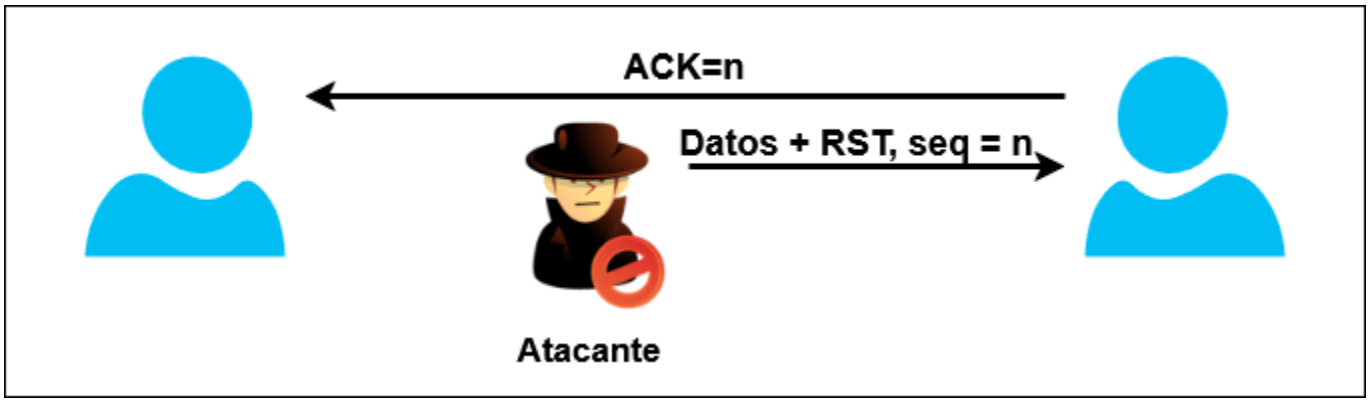
- RST se encuentra dentro del rango permitido
  - En todos los estados salvo SYN-SENT, todos los fragmentos RST son validados revisando sus campos SEQ (Número de secuencia).
  - Un reset es válido si el número de secuencia está dentro del rango
  - En el estado SYN-SENT el RST es aceptable si el campo ACK reconoce el SYN
  - Número de escuencia entre RCV.NXT y RCV.NXT+RCV.WND
  - Rangos históricos < 64 kbytes.
- Right 4-tuple
  - Se deben conocer la IP y puerto del server
  - Se deben conoce la Ip y el puerto del cliente

Ataque TCP reset - Sin limitación de posición: Atacante en la red del cliente



- El atacante inspecciona los datos enviados por el primer equipo al segundo equipo
- Antes de que el primer equipo envíe el siguiente paquete, el atacante genera un paquete RST válido con:
  - Misma Dirección IP
  - Mismos Puertos TCP
  - Número de secuencia correcto.

Ataque TCP reset - Sin limitación de posición: Atacante en la red del servidor



- El atacante inspecciona el tráfico del segundo equipo al primero
- Antes de que el primer equipo envíe el siguiente paquete, se genera un paquete RST válido
  - Misma IP
  - Mismos puertos TCP
  - Número de secuencia correcto

Ataque TCP reset - Posición limitada: Blind Data/RST Injection

Es un ataque difícil de realizar, las direcciones de ambos extremos no suelen ser conocidas, aunque se suelen conocer las direcciones de los servidores, las de los servidores suelen ser desconocidas. Los puerto de los dos extremos suelen ser desconocidos, el de server a veces es conocido, pero el de los clientes suele ser impredecible. El número de secuencia tampoco es conocido. Las conexiones suelen tener un tiempo de vida muy corto y el rango del número de secuencia valido cambia, por lo que cualquier intento de adivinar estos datos es poco útil.

Por otro lado, los protocolos tienen un amplio tiempo de vida y las direcciones se pueden saber por adelantado.

Defensas contra ataque TCP reset

- Solo aceptar el segmento RST si el número de secuencia es el primero en el rango (proveido por el sistema operativo)
- Filtrar paquetes spoofeados a nivel IP (Tiene que ser realizado por los servidores de autenticación en los extremos)
- Usar tmarcas de tiempo como defensa adicional: PAWS (Protection Against Wrapped Sequences)
- Paquetes TCP autenticados (TCP-AO)

Ataque SYN Flooding

Una tacante agota la tabla de conexiones

1. El atacante envía paquetes SYN con su dirección real pero nunca completa las conexiones (Filtrado fácilmente del lado del servidor)
2. El atacante envía paquetes SYN con direcciones suplantadas (El receptor suplantado envía RST y el servidor elimina la conexión)
3. El atacante envía paquetes SYN con direcciones suplantadas que no responden (Ataque DoS)

Para defendernos de SYN Flood podemos hacer lo siguiente:

- Dropear conexiones
- Reducir el uso de memoria para conexiones noe stablecidas
- No almacenar nada (Como se establece la conexión entonces?)

SYN Cookies

Se cifra la información de conexión dentro del ISN

- Primeros 5 bits: número lentamente incremental basado en el tiempo
- Siguientes 3 bits: Se codifica el MSS anunciado del cliente
- Últimos 24 bits: Hash secreto de la IP y portes del cliente y los primeros 5 bits.

Cuando se recibe un ACK sin una conexión establecida:

1. Se sustrae 1 del número ACK
2. Se Recalcula el hash y se compara con los últimos 24 bits, si el hash coincide, se almacena la ifnormación de la conexión.

Este mecanismo no necesita cooperación por parte del cliente.

Las SYN Cookies tienen algunos puntos negativos:

- Falta de espacio para negociar opciones

    - MSS: solo 3 bits, aproximadamente 65000 valores
    - SACK: No hay espacio para el
    - Rangos grandes: No hay espacion para ellos
- Soluciones:
    - Incrementar los bits para codificación de información (Reduce la resistencia del hash)
    - Usar SYN Cookies solo cuando se está bajo ataque, mejor tener mal rendimiento que perder el servicio
    - Tomar ventaja de otras opciones para incrementar el espacio
        - Marca de tiempo del servidor enviada de vuelta en CAK, usa la parte final para cofigicar información

---

Ataque SlowLoris sobre HTTP

Busca agotar la thread pool de un servidor web:

1. Se hacen muchas peticiones HTTP incompletas
2. Se envían encabezados periódicamente para mantenerlos abiertos
3. Nunca cerrar y sie el server cierra, volver a abrir

Esto se puede mitigar de la siguiente manera:

- Incrementar el número de hilos (Poco efectivo)
- Limitar Tiempo de conexión, conexiones por IP…
- Proxy inverso en la nube: No se envía nada al servidor web.

Este ataque también se puede realicar sobre QUIC

Autenticación

La ausencia de autenticación tiene los siguientes problemas:

- Identificación de conexión
    - Puerto e IP de destino: Conocidos
    - Puerto de origen: puede ser adivinado
    - IP de origen: Puede ser suplantada
- La falta de autenticación puede llevar a:
    - Ataques DoS: RST attack y SYN flooding
    - Ataques de inyección de datos.

Autenticación basada en posición

Controla la conexión entre host y routers adyacentes donde ambas partes residen en la misma LAN o se sabe que ambas partes están como mucho a n saltos de distancia.

Generalized TTL Security Mechanism (GTSM)

El procedimiento de transmisión consiste en enviar todos los datagramas IP con TTL/Hop limt de 255, de forma que podemos saber que los paquetes solo han dado n saltos. Los datagramas relacionados con ICMP también usan TTL=255. En recepción:

- Unknown: Cualquier datagrama IP no telacionado con una sesión protegida GTSM
- Trusted: Un datagrama de una sesión GTSM con valor TTL correcto, normalmente 254
- Dangerous: Un datagrama de una sesión GTSM con valor TTL incorrecto. Se les da poca prioridad o se dropean para evitar DoS.

TCP Authentication Option (TCP-AO)

Tiene como objetivo proteger la capa de transporte para conexiones de protocolo de enrutado de larga duración y cualquier otra conexión de larga duración, sustituye TCP-MD5. Complementa IPsec e IKE. TCP-AO esta pensada para IPSec inviable, protegiendo los protocolos de enrutado. Mientras que TLS protege los datos, TCP-AO protege los protocolos de información.

TCP-AO es una mejora sobre TCP-MD5 ya que provee de algoritmos más fuertes, seguridad Two-Fold (Klaves de tráfico generadas a partir de la clave configurada por el usuario), mejor manejo de claves y agilidad (Cambio de claves al momento sincronizando el cambio entre los dos lados de la conexión) y es mejor para conexiones de larga duración.

Claves TPC-AO

- Master Key Tuples (MKT): Describe propiedades asociadas a las conexiones
  - ID: número único representando un MKT
  - Identificador de Conexión TCP: Direcciones ip y puertos asociados con la conexión
  - TCP Option Flag: Opciones para ser autenticado
  - Master Key: Secuencia de bits aleatoria segura usada para generar las claves de tráfico (Traffic keys)
  - Key Derivation Function (KDF)
  - Algoritmo MAC
- Traffic Keys: Derivadas de MKT, ambas direcciones IP, ambos puertos y ambos ISN
- Send_SYN_traffic_key: No usa ISN
- Receive_SYN_traffic_key: No usa ISN, solo para conexiones abiertas simultáneamente
- Send_other_traffic_key
- Receive_other_traffic_key

Protegiendo el DNS

El DNS o Domain Name Service es una base de datos distribuida que mapea nombres a direcciones IP, los principales elementos son resolvers, protocol y servers. tiene una estructura jerárquica:

- Root
- Top-Level-Domain (TLD)
- Second-Level-Domain (SLD)

Resolución de Nombres:

- Los equipos tiene una rutina resolutora de nombres (Resolver). El resolver sabe el nombre de los servidores DNS locales
- El servidor DNS local recibe una consulta recursiva
- El Servidor DNS local pasa la consulta a otro servidor DNS
- El servidor DNS realiza una de las siguientes acciones:
    - Respoonde la consulta
    - Pasa la consulta
    - hace un refer a otro server.

Los servidores locales DNS deben conocer las direcciones de los Servidores DNS de la zona raíz. Los servidores Autorizados deben ser replicados (Un servidor primario y muchos secundarios). Cada entrada de la base de datos tiene un tiempo de vida máximo (TTL). Usado para cacheado por parte de los servidores DNS intermedios. Dentro de un DNS se guardan registros de recursos:

- A: Dirección IPv4
- AAAA: Dirección IPv6
- CNAME: Nombre canónico o alias
- NS: Nombre de un servidor
- MX: Intercambio de correo
- PTR: Puntero a un nombre para resolución inversa
- SOA: Comienzo de la zona de autoridad
- TXT: Texto arbitrario

Vulnerabilidades DNS

DNS transmite información sin cifrar, sin autenticación ni pruebas de integridad. Identificaciónde respuestas DNS.

- TCP: la conexión TCP identifica la sesión
- UDP: La respuesta es aceptada si:
    - Va dirigido al puerto de origen, debería ser aleatorio, pero a veces está puesto al 53
    - Usa el ID de transmisión correcto, cuanto más difícil de adivinar, mejor.

Cache Poisoning

Se engaña al servidor DNS para que guarde en cache un mapeo incorrecto. Esto se puede prevenir con las siguientes contramedidas:

- Uso de puertos de origen aleatorios e IDs de transacción en las peticiones
- Evitar el cacheo de información no relacionada con la petición
- Se recomienda usar software DNS actualizado
- DNS Cookies: El server no envía respuestas grandes sin haber recibido antes una cookie.

Ataque de Rebinding

Los navegadores de interent tienen cache DNS interna. Funcionamiento:

1. La víctima entra en www.elmal.com
2. El NS de elmal.com responde con la direción IP real con un TTL muy bajo
3. El navegador descarga un script y accede a www.elmal.com
4. El NS de elmal.com responde con la IP objetivo.

Contramedidas:

- DNS Pinning: El navegador gruarda la dirección IP de la primera respuesta, no puede prevenir ataques más elaborados.
- Filtrado de direcciones IP privadas, previene ataques cuyo objetivo es la red interna de la víctima.
- Revisar cabeceras HTTP Host.

Ataque de reflejo y amplificación

En el ataque de reflejo el atancate envía peticiones con direcciones de origen falsificadas, el server DNS responde a la víctima (dirección falsificada.) El ataque de amplificación de tamaño de paquete:

- Query: Pequeño paquete de petición a un resolver DNS, normalmente con un argumento como ANY para recibir la respuesta más grande posible
- Reply: El resolver DNS envía un paquete grande a la ip falsificada.
- Para DDoS se hace uso de resolvers DNS públicos.

Contramedidas:

- Servidor Revursivo: Debe estar restrigido a la organización o a rangos IP del cliente para prevenir abuso
- Servidores Autoritativos: No deben ofrecer recursividad, pero puieden ser usados en un ataque, se recomienda configurar DSN RRL (Response Rate Limiting)
- Customer Premise Equipment (CPE): No debe escuchar paquetes DNS en la interfaz WAN.

DNS Cache Snooping

Los servidores DNS de cacheo pueden filtrar información sobre peticiones resueltas.

1. Corre una petición no recursiva para un nombre objetivo, solo responde si estaaba en la cache. El servidor se puede defender realizando igualmente una consulta recursiva.
2. Revisar el valor TTL: Si es cercano al del servidor autoritativo, no fue visitado, el server se puede defedner añadiendo ruido al TTL
3. Medir el tiempo de respuesta: Si el tiempo de respuesta es muy bajo, estaba en cache.

Contramedidas:

- Deshabilitar el cacheo en los servidores DNS autoritativos.
- Hacer los servidores DNS locales inaccesibles desde fuera de la organización

---

Secure DNS (DNSSEC)

Domain Name Security Extension

- Autenticación de origen de datos e integridad de datos
- Asocia firmas digitales con sets de registros de recursos (RRsets)
- Se autentica el nombre y la no existencia del tipo

New Resource Record Types:

- RRSIG: Contiene la firma cirptográfica de un RRset
- DNSKEY: Contiene la clave pública
- DS: Contiene el Hash de un registro DNSKey
- NSEC/NSEC3: Para la denegación de existencia explícita de un registro DNS
- CDNSKEY y CDS: para zonas hijo que solicitan actualizaciones a los record DS en las zonas padre.

Procedimiento de validación DNSSEC

- Validación de respuesta
  - Un resolver recibe un RRset y un RRSIG
  - El resolver obtiene el DNSKEY
  - El resolver extrae el Zone Signing Key (ZSK) del DNSKEY
  - El ZSK es la clave pública usada para validadr el RRset con el RRSIG
- Validación de firma
  - El DNSKEY contiene una o más Key Signing Keys (KSK)
  - EL DNSKEY RRset es firmado con KSK
  - El resolver valida el DNSKEY RRset con la clave pública KSK
- Dos claves de firma
  - ZSK: poca longitud, gestionada por el administrador de la zona
  - KSK: longitud larga, almacenada offline

- Autenticidad de KSK: Cadena de confianza
  - La clave DS almacena una fingerprint del KSK
  - El DS se almacena en la zona padre

Un resolver valida el RRsig del DS en el padre: confia en el KSK. Las claves públicas de la zona raíz deben ser conocidas y de confianda para todos los resolvers (Root Signing Ceremony)

Auntenticación de entidades nombradas basadas en DNS (DANE)

DNSSEC permite la distribución confiada de claves públicas asociadas con un dominio. DANE (DNS-Based Authentication of Named Entities) ofrece la opción de usar la infraestructura DNSSEC para almacenar yu firmar claves y certificados que son usados por TLS.

Certificate Authority Authorization

Capa de seguridad añadida sobre PKI:

- Dice explícitamente que Certification Authorities pueden emitir certifcados para nuestro dominio o subdominio
- Puede añadir procedimientos de notificación a seguir si un CA no autorizado es detectado. (Email o Real Time Inter-network Defense (RID))
- IODEF: Incident OIObject Description Exchange Format

Transportes alternativos para DNS

DNS filtra mucha información ay que se transmite en palno, el ISP puede ver la solicitudes realizadas por sus clientes, el ISP puede modificar los resultados devueltos por los servidores DNS (A menos que usen DNSSEC).

Transporte DNS sobre conexiones seguras:

- DNS sobre TLS y DTLS: mismo formato que DNS plano pero sobre Sesión TLS/TCP o DTLS/UDP
- DNS sobre HTTPS (DoH): Formato JSON o DNS plano sobre una conexión HTTPS o HTTPS2. Como muchas consultas son resultado de búsquedas web, los server web pueden proveer respuestas DNS firmadas.
- DNS sobre QUIC (DoQ): Menor latencia, mejor multiplexación y resistencia abloqueos head-of-line
- DNS sobre HTTP3 (DoH3): Intergración del acceso web y DNS con respecto a DoQ

Problemas de Seguridad del Enrutado

Problemas de Seguridad Interior Gateway Routing protocol (IGP)

Open Shortest Path First (OSPF)

Usado en empresas y redes IPS. Estandarizado por IETF. IGP basado en estado de link:

- Topología almacenada en una colección de Link-State-Advertisments (LSAs)
- Todos los routers tienen una copia idéntica de la topología AS
- Los routers realizan computaciones SPF individuales cuando la topología cambia.

Vista general del procedimiento OSPF:

1. Los routers vecinos forman adyacencias
    1. Los routers vecinos son los que comparten un enlace de capa 2
    2. Una vez se forma la adyacencia, se intercambian los LSA conocidos.
2. Diseminación de Información
    1. Cuando la topología cambia, el nuevo LSA se emite en todas las redes
    2. el LSA es originado por los routers directamente afectados.
3. Computaciones de enrutado:
    1. Se calcula 2 tipos de rutas:
        1. Interna: Calculada por el SPF
        2. Externa: Iyectada en el AS por un OSPF ASBR (AS Border Router) por que reside fuera del dominio OSPF

Consecuencias de ataque

- Starvation: el tráfico de datos destinado para un nodo se pasa a una parte de la red que no lo puede entregar
- Network Congestion: Se pasa más trafico del que se debería por una porción de la red que no debería transportarlo
- BlackHole: Grandes cantidades de tráfico se dirigen a un solo router que no puede manejar el incremento de tráifco, lo que provoca que se dropeen parte de los paquetes o todos.
- Delay: El trafico de datos destinado para un nodo se pasa por un camino que es peor al que debería toamr
- Looping: El tráfico de datos se pasa por un camino que tiene un bucle, por lo que los datos no son entregados nunca.
- Eavesdrop: El tráfico de datos pasa por un ruouter o red que no debería ver el tráfico, creando una oportunidad para ver los datos
- partition: Una porción de la red cree que está separada del resto de la red cuando no lo está
- Cut: Una porción de la redd creo que no tiene salida de red cuando si tiene
- Churn: El paso de paquetes de la red cambia rápidamente, resultando en grandes variaciones en los patrones de entrega de datos.

- inestabilidad: OSPF se vuelve inestable, por lo que la convergendcia de un estado globla de entrega no se alcanza
- Overload: Los mensajes OSPF se vuelven una porción insifnificante del tráfico que transporta la red.
- Resource exhaustion: Los mensajes OSPF causan la sobrecarga de recursos críticos del router, como el tamaó de tabla y colas.

Técnicas de ataque genéricas contra OSPF

- Eavesdropping: Información de enrutado transmitida en texto plano
- Message Replay: Se evitan en la mayoría de los escenarios con autenticación criptográfica
- Message Insertion: Solo con autenticación criptográfica deshabiltiada o realizado por un insider
- Message Deletion: Es detectado tanto para el LSI (Link-State Update) y para Hllos por adyacencia
- Message Modification: Solo con autenticación criptográfica deshabilitada o realizado por un insider
- Man in the Middle: solo si la autenticación criptográfica está deshabilitada o realizado por un insider.
- Denial of service

Defensas integradas

- Autenticación por link: La contraseña comaprtida por todos los routers en el enlace debe ser diferente en cada enlace. Dificil ya que no hay función de gestión de claves
- Flooding: los LSU se emiter por fooding. Un adversario no puede prevenir la propagación de LSUU en presencia de caminos alternativos
- Fight-Back: Si un router recibe un LSU con un LSA que solo el puede originar, contraataca con una LSU actualizada y corregida.
- LSA solo contiene elaces de 1 solo router: Los atacantes tienenq ue falsificar el LSA de muchos routers para causar daño.
- Enlaces de transito bidireccionales. Un enlace de tránsito es considerado solo si es anunciado por 2 routers, uno en cada extremo del enlace.

Auntenticación de Mesnajes OSPF

- Mecanismos disponobles:
    - NULL: Envia mensaje sin autenticación
    - Simple Password: Añade una contraseña en texto plano a cada LSU.
    - Criptografía MD5 o HMAC-SHA: No provee ni confidencialidad ni robusted contra ataques replay. Los ataques replay son solo posibles cuando se reusa una secuencia de números. Puede ser forzado rompiendo una adyacencia.
    - Claves de Autenticación Criptográficas: Deben usar una clave única por enlace. Mútiples claves para rollover.

Ataques comunes contra OSFP

MaxAge LSA

- BASE: LSA tiene una validez máxima normalmente de unos 30 minutos y debe ser refrescada pasada dicho plazo de tiempo.
- El LSU emitido con un LSA establecido a MaxAge, hace que el LSA desaparezca de los routers.
- Esto resulta en un Network Churn
  - Black-Holing de tráfico a las redes en LSA
  - Recomputación de las tablas de enrutado
  - Flooding de LSA
- Mitigación
  - El roputer puede contraatacar si recibe una LSU falsificada.

Seq++

- BASE: Las SLA tienen un número de secuencia, los números de secuiencia más altos reemplazan las viejas LSA.
- Un LSU con una LSA con un numero de secuencia más alto e infomración falso.
- Efectos:
  - Modificación de la tabla de enrutado para toda la red
  - Loops, black-hole, redirección de tráfico…
- Mitrigación:
  - El router original puede contraatacar si recibe un LSU falsificado.

Seq++ y MaxAge LSA permanentes

Bajo circusntancias normales, los mecanismos de contraataque previenen cambios permanentes por dichos ataques, pero, si un roauter nunca emite sus LSA más rápido más de una vez dada MinLSInterval (5 segundos):

1. En la recepción de un LSA falso el router victima contraataca.
2. Se ataca el router enviando de nuevo el LSA falso
3. Si el router atacante manda el LSA falso más rápido que el MinLSInterval los cambios son permatentes

Esto se puede mitigar notificando al adminsitrador cada vez que ocurre un contraataque (SNMP traps), un gran numero de traps debería alertar al administrador para tomar acciones.

LSA Disfrazado

- Base: un LSA se considera identico si tiene el mismo número de secunecia, checksum y edad.
- Un LSA falso con la misma secuencia y checksum pero con datos diferentes. El tiempo es crítico, debe ser enviado antes de que la víctima envíe otro LSA.
- Efectos
    - Muchos routers reciben información falsa y obtiene una tabla de enrutado invalida
    - Los efectos son persistentes, no hay contraataque al ser iguales los LSA.
- Mitigación:
    - Randomizar los numeros de sevuencia para hacer más difícil la predicción del checksum.

Remote False Adjacency

- BASE: el procedimiento de adyacencia no revisa las respuestas de un router descubierto.
- Se envían Hellos al router existente pero con una IP de origen falsa. Es necesario saver las claves criptográficas o la autenticación NULL.
- Efecto: crea un router fantasma
    - Nuevo enlace de transito falso entre el router real y el fantasma (Black Hole)
    - El router fantasma puede inyectar LSAs con información arbitraria.
    - Los efectos son persistentes:
- Mitigación:
    - Habilitación de autenticación criptográfica con diferentes claves en cada enlace
    - Se unsa GTSM para prevenir ataques remotos.

Evenenamiento Persistente

- BASE: Los routers no activan el contraataque si el ID de router de una LSA no coincide.
- Un router comprometido manda un LSA al router víctima con LS ID coincidente pero no adv. Router ID.
- Efectos: El cálculo de la tabla de enrutado usa el SLA envenenado en vez del LSA del router victima.
- Mitigación:
    - Es un bug del diseño del protocolo, esta arreglado en versiones más nuevas de OSPF

Buenas prácticas

- Transit-Only Networks: Oculta prefijos de enrutado de redes de tránsito internas en las tablas de enrutado
    - Previene atacantes remotos
    - Conocido como Prefix Suppression en Cisco
- Unnumbered Interface: Interfaces que comaprte la IP de otra interfaz en el mismo host. No se genera ruta para estas interfaces.
- Cryptographic Autentication: Previene bugs de corrupción ya que es más robusto que el checksum de OSPF. Uso de diferentes claves en cada enlace
- Generalized TTL Security Mechanism: Previene la mayoría de ataques remotos.
- RPF (Anti Spoofing or Ingress Filtering): Utilizado en el ingreso de una red donde se usa

enrutado simétrico, se configura en todos los AS Border Routers. Revisa quel paquete IP lelga a través de una interfaz utilizada para enviar tráfico a su dirección IP de origen.
- Fight-back Traps / Notification: Mecanismo apra notificar al administrador que OSPF esta activando contraataques. Muchas notificaciones juntas indican un problema, avisa de entidades maliciosas, malas configuraciones de Router-id o partición.
- Consistence Check Tools: El LSA de cada router puede ser obtenido por SNMP u otras herramientas. LSA debe ser identico en todos los routers.
- Misceláneo:
    - Se recomienda tener hardware y software de red diverso, no solo una marca.
    - Los fabricantes parchean las vulnerabilidades tan rárpido como se reportan, es recomendable tener siempre todo actualizado
    - Interfaces pasivas por defecto (No broadcasting de LSA), limita las adyacencias accidentales.

Problemas de Seguridad Exterior Gateway routing Protocolo (EGP)

Internet es una colección de AS y un AS es una colección de prefijos IP con una política de enrutado común, hay 2 variantes:

- Transit AS: Conecta múltiples AS para enviar su tráfico entre ellos.
- Non-Transit AS: Conectado a uno o más AS para reenviar su tráfico.

BGP es el único EGP en uso en internet, mantiene listas de caminos eficientes entre prefijos de redes entre los AS. Un camino es una lista rodenada de números de AS. hay 2 variantes, e-BGO e i-BGP. Los Peers BGP intercambian datos por conexión TCP al puerto conocido BGP (179). Normalmente, los peer e-BGP residen en la misma subred.

Precocupaciones de seguridad BGP

- Denegación de servicio:
    - Starvation: Gran parte del tráfico se direcciona a nodos que no lo pueden reenviar
    - Blackhole: El trafico se envía a routers que lo dropean
    - Delay: El tráfico se envía por caminios poco optimizados
    - Churn: Cámbios rñapidos en la información de enrutado
- Wedgies: BGP no es determinista, un atacante puede falsificar una tabla de estado poco nodeseada rompiendo una sesión BGP.
- Eavesdroping: BGP se transmite en claro
- Session Hijacking.

Peer Spooging y TCP Resets

- BASE: Se inyecta tráfico en la sesión TCP entre dos peers con dirección IP false.

- Se otienen la IP de un peer (con traceroute) y se envían paquetes falsificados con información malintecionada.
- Efecto:
  - Route churn
  - DoS
  - Redirección de Tráfico
- Mitigación
  - Aleatorización del numero de secuencia inicial TCP
  - Aleatorización del puerto del cliente TCP
  - Uso de autenticación TCP
  - Uso de GTSM para e-BGP
  - Sesion BGP protegida con IPsec

TCP resets con ICMP

- BASE: un mensaje de error ICMP puede romper conexiones TCP
- Se envía un mensaje de error ICMP falsificado al servicor BGP víctima.
- Efectos:
  - Route Churn
  - DoS
- Mitigación
  - GTSM para e-BGP
  - Proteger la sesión BGP con IPSEC
  - Filtrar ICMP tipo3, code 2, 3 y 4

Route Flapping

- BASE: Route Flapping con alta cadencia causa que los anuncios BGP peer to peer sean ignorados (Route flap damping)
- El atacante desactiva un speakr BGP múltiples veces para que sus vecinos anuncien continuos cambios en los caminos.
- Efectos
  - Las rutas afectadas son eliminadas de la red, lo que puede causar caidas o degradación.
- Mitigación
  - Configuración correcta de Route Flap Campling (RTD)
  - Habilitar Graceful Restart en BGP

Malicious Route Injection / BGO Keak

- BASE: Los pregijos anunciados por BGO suelen ser no autenticados.
- Un adversario anuncia un prefijo específico más largo que el anunciado por el AS real.
- Efecto:
  - El trafico a los prefijos anunciados va al AS adversario. El atacante puede escuchar el tráfico o realizar ataques MitM

- Mitigación:
    - Route filtering
    - Resource PKI (RPKI): Login de autenticación
    - Despliegue de BGPsec (Autenticated advertisements)

Sesión BGP TCP

La seción TCP entre 2 peer BGP puede ser protegida para evitar inyección de tráfico o ataques RST. Se recomienda usar TCP-AO, implementar GTSM y considerar el uso de IPsec.

Filtrado de prefijos

Considerando un proveedor Tier 2, tiene muchas relaciones:

- Relaciones con otros proveedores tier 2
- Relación de cliente con proveedores Tier 1
- Relación de proveedor con sus clientes.

Filtros con clientes

- Inbound: Solo acepta prefijos asignados acl cliente, la lista puede ser configurada manualmente
- Outbound: Depende del cliente:
    - Muchos clientes solo necesitan recibir la ruta por defecto (0.0.0.0/0)
    - Si necesita la tabla completa, debe filtrar:
        - Prefijos no globalmente enrutables
        - Rutas demasiado específicas
        - La ruta por defecto

Filtros con Proveedores upstream

- Inbound: Solo la ruta por defecto y/o prefijos no globalmente enrutables, prefijos no alocados por la IANA, rutas demasiado específicas, prefijos pertenecientes al AS local, Prefijos IXP LAN.
- Outbound: Permite solo prefijos del AS local y para abajo y deniega;
    - Prefijos no globalmente enrutables
    - Rutas demasiado especificas
    - Prefijos IXP LAN
    - Ruta por defecto
    - Cualquier prefijo no pensado apra ser enrutado por upstream.

AS Path Filtering

- Solo acepta caminos conteniendo ASN perteneciendo o transitando a través del cliente
- Solo acepta caminos con logitudes apropiadas para el tipo de cliente

- Rechaza caminos incluyendo ASN de upstream providers
- Rechaza prefijos con números ASN privados
- Rechaja prefijos si el primer ASN no es el peer del IXP
- No anuncia prefijos si transmite servicios que no deben.