

Catalyst Integrated Security Features (CISF)

Este es el resumen de la exposición que hizo Marco Morales, llevado a cabo el 23 de junio, en la UNI-FIIS

CISF es un conjunto de contramedidas frente a ataques en capa 2, que ofrece Cisco. Estas herramientas están disponibles dependiendo del modelo de equipo.

Los temas han sido resumidos en el formato Problema-Solución, es decir, se hace una síntesis de los problemas respecto a un tema y luego la propuesta de solución utilizando las herramientas del CISF.

Temas:

- Storm Control
- Port Security
- DHCP Snooping
- ARP Inspection
- Source Guard
- Trunking
- Spanning Tree
- VACL

Storm Control

Problema

- Una tormenta de paquetes ocurre cuando se reciben en un puerto gran número de paquetes broadcast, unicast o multicast. Reenviar esos paquetes puede causar una reducción del rendimiento de la red o incluso la interrupción del servicio.

Solución

- Storm Control usa umbrales para bloquear y restaurar el reenvío de paquetes broadcast, unicast o multicast.
- Usa un método basado en ancho de banda. Los umbrales se expresan como un porcentaje del total de ancho de banda que puede ser empleado para cada tipo de tráfico.

Port Security

Problema:

- Los switches guardan las asociaciones MAC e información de VLAN en una tabla llamada tabla CAM.
- La tabla CAM de un switch tiene un tamaño fijo y finito.
- Cuando la tabla CAM no tiene espacio para almacenar más asociaciones MAC, envía a todos los puertos las tramas que tengan una dirección MAC destino no almacenada en la tabla CAM. (Actúa como un HUB para cualquier MAC que no haya aprendido).
- Existe un ataque que se basa en el tamaño limitado de la tabla CAM.
- Para realizar el ataque sólo hace falta enviar gran número de tramas con direcciones MAC distintas (usualmente generadas al azar) a cualquier puerto del switch hasta que se llene la tabla CAM.

Solución:

- Port Security es un conjunto de medidas de seguridad a nivel de puertos disponibles
- Permite entre otras cosas: restringir el acceso a los puertos según la MAC, restringir el número de MACs por puerto, reaccionar de diferentes maneras a

violaciones de las restricciones anteriores, establecer la duración de las asociaciones MAC.

- Tomar en cuenta que: No se puede activar port security en puertos dynamic access o trunk, por defecto Port Security está desactivado y sólo almacena una MAC por puerto.

DHCP Snooping

Problema:

- DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
- Los servidores DHCP pueden ser víctimas de ataques, por ejemplo, de denegación de servicios.

Solución

- El DHCP Snooping define los puertos que pueden enviar respuestas de DHCP, por tanto, es recomendable tenerlo configurado.

ARP Inspection

Problema:

- La solicitud ARP se coloca en una trama broadcast y se envía. Todas las estaciones reciben la trama y examinan el pedido. La estación mencionada en el pedido contesta y todas las demás estaciones procesan la misma.
- ARP no proporciona seguridad o algún mecanismo para reservar direcciones IP o MAC.
- Utilizando ARP Spoofing el atacante consigue que todas las tramas dirigidas hacia otro puerto del switch lleguen al puerto del atacante para luego re-enviarlos hacia su destinatario y de esta manera poder ver el tráfico que viaja desde el remitente hacia el destinatario.
- El atacante logra que todas las tramas que intercambian las víctimas pasen primero por su equipo (Inclusive en ambientes switcheados).
- Utilizando ARP Spoofing el atacante puede hacer que un equipo crítico de la red tenga una dirección MAC inexistente. Con esto se logra que las tramas dirigidas a la IP de este dispositivo se pierdan.

Solución:

- ARP Inspection permite VACLs para limitar los paquetes ARP para las direcciones específicas IP a las direcciones específicas MAC.

Source Guard

Problema:

- Relacionado al DHCP, respecto ataques vía IP

Solución

- Source Guard, permite solamente direcciones provenientes del DHCP Snooping Binding Table.
- Cuando un cliente recibe un IP válido del servidor de DHCP, un Port Access Control List (PACL) está instalado en el puerto que permite el tráfico del IP. Este proceso restringe el tráfico del IP del cliente a las direcciones del IP de la fuente que se obtengan del servidor de DHCP.

Trunking

Problema:

- Los puertos trunk por defecto tienen acceso a todas las VLANs.
- Se los emplea para transmitir tráfico de múltiples VLANs a través del mismo enlace físico (generalmente empleado para conectar switches).
- La encapsulación puede ser IEEE 802.1Q o ISL.
- El Dynamic Trunk Protocol (DTP) automatiza la configuración de los trunk 802.1Q/ISL. Sincroniza el modo de trunking en los extremos y hace innecesaria la intervención administrativa. El estado DTP puede ser: *Auto*, *On*, *Off*, *Desirable*, o *Non-Negotiate*. Por defecto, en la mayoría de switches es *Auto*.
- Un equipo puede hacerse pasar como un switch con 802.1Q/ISL y DTP, o bien se puede emplear un switch.
- El equipo se vuelve miembro de todas las VLAN.
- Requiere que el puerto esté configurado con trunking automático.
- Cisco Discovery Protocol (CDP) y VLAN Trunking Protocol (VTP), son protocolos de Cisco comúnmente usados para negociar el estado de puertos trunk, intercambiar información de VLAN, etc. Se transmiten por la VLAN 1.
- Si un atacante logra que su puerto se convierta en trunk, puede enviar mensajes VTP como si fuera un servidor VTP sin VLANs configuradas. Cuando los demás switches reciban el mensaje eliminarán todas sus VLANs.

Solución

- Deshabilitar el auto-trunking.
- Utilizar una VLAN dedicada para los puertos trunk.
- Deshabilitar los puertos no utilizados y colocarlos en una VLAN no utilizada.
- Colocar los puertos de los usuarios como non-trunking (Deshabilitar DTP)
- No utilizar VLAN 1

Spanning Tree

Problema:

- Spanning Tree Protocol (STP) permite lograr topologías libre de bucles en infraestructuras de capa 2 redundantes.
- Esto permite que el tráfico broadcast no se vuelva una tormenta (broadcast storm).
- Los ataques STP, se refieren cuando el atacante envía mensajes BPDU (Bridge Protocol Data Units) anunciándose como bridge con prioridad 0, para convertirse en root, con lo cual puede ver tramas que no debe. Para esto, el atacante debe estar conectado con 2 switches a la vez.

Solución

- Para el funcionamiento correcto de puertos de usuarios es necesario poner el puerto como "spanning-tree portfast", esto deshabilita STP haciendo que si ocurre un loop, este no se detecte.
- BPDU Guard, deshabilita puerto "port-fast" que reciban BPDUs
- Root Guard, bloquea el puerto al dispositivo que intente conectarse como root.

VACL

Problema:

- Proteger los hosts entre las VLAN.

Solución

- El VLAN (Virtual Local Area Network) Access Control List, proporciona el control de acceso para todos los paquetes en una VLAN.