Resumen Modulo 2

El router borde es el último entre la red interna y una red poco segura, es donde se realiza la filtración inicial y final de paquetes, por lo que es donde se deben concentrar las políticas de seguridad.

La implementación de políticas de seguridad depende del tamaño de la red:

- Enfoque router único: Todas las PS se configuran en este.
- Defensa en Profundidad: Múltiples capas de seguridad. Más de un router. Uso firewall como disp. de control. Filtrado a diversos en puntos de control.
- Enfoque DMZ: Zona desmilitarizada. Filtra algo de tráfico. Un router de seguridad hace la mayoría del trabajo.

Áreas de seguridad de un router:

- Seguridad Física: Accesible físicamente solo a personal autorizado. Requiere de sistema de alimentación ininterrumpida. Libre de interferencia electrostática o magnética, incendios, humedad y control de temperatura.
- Sist. Operativo: Máxima versión estable, suficiente memoria y almacenar copia de seguridad del archivo de configuración de la imagen del S.O.
- Router endurecimiento: Asegurar control administrativo, acceso, deshabilitar puertos, interfaces y servicios no utilizados.

Tareas para acceso administrativo seguro:

+ Restringir acceso al dispositivo
+ Registro de cuenta de todo acceso
+ Autenticar acceso
+ Autorización de acciones
+ Presentación de notificación legal
+ Garantizar confidencialidad de los datos

Precauciones pra acceso remoto:

- Cifrar tráfico (SSH en Telnet y HTTPS en HTTP)
- Establecer red de gestión dedicada (interfaz dedicado en router)
- Acceso al router solo a host administrativos identificados
- Contraseñas seguras

Otras actividades de mejora de seguridad

- Asegurar puertos aux, consola y vty con contraseñas seguras y nombres de usuario.
- Servidores de autenticación para acceso a dispositivos
- Cifrar las contraseñas
- Desactivar sesiones desatendidas (exec-timeout)
- Contraseñas de cierta longitud mínima.

Mejorar login al negar nuevas peticiones o entrar en edo. de bloqueo ante intentos constantes fallidos de conexión

Configuración de mejoras de login

Comando utilizado para bloquear ante un número determinado de log ins.

R2(config)# login block-for seconds attempts tries within seconds

Habilitar mejoras de login

El bloqueo de login monitorea actividad del dispositivo en los nodos.

- Normal: Cuenta número de intentos fallidos de conexión dentro de cierto tiempo
- Silencioso: Si el no. de log ins fallidos pasa el umbral configurado, se niegan todos los intentos de conexión por el tiempo configurado.

Log ins fallidos

R(config)# login on-success log [every login]
R(config)# login on-failure log [every login]
R(config)# security authentication failure rate threshold-rate log.

"Login on-success" y "on-failure" generan mensajes syslog, según sea el caso. El tercer comando podría configurarse para dar un msj. de registro cuando se supera la tasa de fallidos.

Proveer notificaciones legales

Mensajes banner para notificaciones legales a usuarios no bienvenidos.

Configurar SSH

1: Crear nombre de dominio: ip domain-name nombre
2: Generar llave RSA: crypto key generate rsa general-keys modulus
3. "nuevo usuario": username name secret secret
4: Activar VTY para SSH: login local
transport input ssh

Conexión a Router con SSH:

Puede ser de dos maneras: 1: Consola del modo EXEC privilegiado
2: Usando un cliente SSH.

Asignar Roles Administrativos

Niveles de privilegio: 0: Fijos. de acceso a nivel usuario (disable, enable, exit, help, logout).
1: Nivel predeterminado de log in con indicador ">"
2-14: Personalizados para los privilegios de nivel usuario
15: Reservado para privilegios de modo enable.

Configurar niveles de privilegios

- Para el nivel privilegiado: enable secret level/level/password
- " usuario al que se le otorga un nivel de privilegio específico: username name privilege level/secret password

Limitaciones de los niveles de privilegio

- No hay ctrl de acceso a interfaces, puertos y slots.
- Comandos disponibles en nivel bajo son ejecutables en nivel alto.
- Administrador con cuenta tiene casi todos los comandos pero no todos

Acceso a CLI basado en Roles:

Crtl más fino y granular que especifica qué comandos están disponibles para funciones específicas. Permite crear vistas de config. para diferentes usuarios:

- Root view: Privilegios de nivel 15.
- CLI view: No tiene jerarquía de mando
- Supe views: Permite al administrador asignar usuarios y grps. de estos múltiples vistas de la CLI a la vez.

Configuración de CLI en roles

1: R(config)# aaa new-model (Habilita AAA)
2: Crear vista: parse view view-name
3: Asignar contraseña a vista: secret password.
4. Asignar comandos permitidos: parser-mode {include|include-exclusive|exclude} [all] [interface int-name | command]
5: exit.

Recuperación de contraseña en router

1. Conectarse al puerto consola
2. Revisar código de configuración
   R1> show version
   Reg de config es: 0x2102
4. Apagar y encender el router.
5. Emitir la break sequence para poner el route en ROMmon
6. Reinicie el router (reset)
7. Saltar proceso de configuración (Ctrl + C)
8. Entrar a modo EXEC privilegiado
9. Copy o r
10. Verifique la config (show run)
11. Cambie contraseña de activación (enable secret)
12. Habilitar todas las interfaces
13. Cambiar config de reg. (config)# config-register 0x2102
14. Copy r s

Desactivación de recuperación de contraseña

R(config)# no service password-recovery

Gestión y supervisión de dispositivos de red

Consideraciones y pares administrativos como políticas de seguridad y la creación de un plan de gestión que abarca cada cambio, mantenimiento o agregaciones a la red.

Gestión de Acceso

- In-band: Canales de datos regulares (requiere internet o servicios de protección)
- Out-of-band: Canales de datos usados para la gestión sin tráfico de producción.
  + Proporcionar el más alto nivel de seguridad
  + Mitigar el riesgo de transmisión de protocolos de gestión de inseguridad en la red de producción.
  + Solo se aplican a los dispositivos que deben ser gestionados o monitoreados.
  + Se usa IPsec, SSH o SSL cuando sea posible.
  + Decide si la gestión del canal debe estar abierto en todo momento

Introducción a Syslog

Protocolo para acceder a los mensajes del sistema. Desarrollado para sistemas UNIX en la década de 1980. Proporciona 3 funciones principales:

- Capacidad de reunir info. de registro
- " " seleccionar el tipo de información de registro que se capture.
- " " especificar los destinos de mensaje syslog capturados

Funcionamiento de Syslog

Pueden enviarse mensajes desde:
- Buffer de registro
- Consola
- Líneas terminales
- Servidor syslog.

Sistema Syslog

- Servidores: Aceptan mensaje de registro de proceso de clientes de reg. de sistema
- Clientes: Routers u otros que generan mensajes de registro a plazo a servidor

Configuración de System Logging

1. Configurar host server
   R(config)# logging host {hostname | ip-addr}
2. Ajuste el nivel de gravedad del registro (Opcional).
   R(config)# logging trap level
3. Configure la interfaz de origen
   R(config)# logging source-interface int-type int-number
4. Habilitar el registro
   R(config)# logging on

Monitoreo de Mensajes usando CCP

CCP puede ser usado para monitorear los registros.

Utilizar SNMP

- Administrar nodos, servidores, estaciones de trabajo, etc
- Gestionar el desempeño de la red.
- Encontrar y resolver problemas en la red
- Planear el crecimiento de la red.

Consiste de 3 elementos:
- SNMP Manager
- SNMP agent
- MIB

Funcionamiento de SNMP

Los agentes SNMP que residen en los dispositivos administrados recopilan y almacenan info. del dispositivo y su operación localmente en el MIB. Luego el SNMP manager utiliza el agent para acceder a la info. contenida en el MIB

Hay dos solicitudes primarias del SNMP manager

- GET: Hace consulta a la info. de un dispositivo
- SET: Inicia acción dentro de un dispositivo

Un SNMP responde al manager de la siguiente manera

- GET AN MIB VARIABLE
- SET AN MIB VARIABLE

SNMP Community Strings

- Read ONLY: Acceso de solo lectura a objetos en el MIB
- Read-Write: " " lectura y escritura

SNMPv3

- Integridad de mensajes y autentificación
- Encriptación
- Control de acceso

Uso de NTP (Network Time Protocol)

Métodos de configuración de hora y fecha: Manual y con NTP

NTP sincroniza sus config. de horario con un servidor NTP.

NTP server

- Privado: Sincronización UTP por radio o satélite.
- Público: Muchos proyectos no seguros entran a la red y hay fallas de mala configuración a menos que se tenga una fuente fidedigna

NTP

- En una red NTP la comunicación es estática.
- Uno o más routers designados como NTP master.
- Clientes contactan al master para sincronizar sus relojes (ntp server ip add)
- Configuración de Broadcast (ntp broadcast client interface)

Autenticación NTP

- Esquema de restricciones basado en ACL
- Esquema de autenticación cifrado de NTP 3 o posterior

Habilitar NTP usando CCP

1. En la barra de menú cisco config. professional, clic en Configurar > Routr > Tiempo > NTP y SNTP
2. Agregar nuevo servidor NTP (Clic en Agregar.
3. Agregar servidor NTP por nombre o ip
4. Clic en casilla "Preferido" si así lo es un servidor NTP.
5. Autenticación (Clic en casilla de verificación e introduzca núm. y valor clave)
6. Aceptar.

Protocolos y servicios predeterminados

- Deshabilitar servicios e interfaces innecesarias.
- Desactivar y restringir servicios de gestión comúnmente configurados (como SNMP)
- Deshabilitar sondeo y exploración
- Inhabilitar transmisiones dirigidas por IP

Herramientas de seguridad de Cisco IOS

- Asistente de autoría de seguridad.
- Cisco AutoSecure
- One-Step lockdown