Seguridad y Auditoría Informática

Auditoría de Redes

Factibilidad de Administración de Redes

- Enfoque típico
  - Realizar un escaneo, obtener un reporte de 1000 páginas y que el entorno de red permanezca sin cambios
- La organización y la gestión de las mitigaciones es clave
- Realizar una Evaluación de Riesgos para priorizar los componentes de red
  - Hacer la auditoría por partes

Metodología General

1. Determinar áreas de responsabilidad
2. Investigar riesgos y vulnerabilidades
3. Asegurar el perímetro
4. Asegurar la DMZ y sistemas críticos
5. Eliminar vulnerabilidades accesibles externamente
6. Eliminar vulnerabilidades accesibles internamente
7. Buscar malware

Personalización de la Metodología

- Identificar sistemas/dispositivos clave
  - Pueden haber sistemas adicionales que necesiten ser auditados antes en el proceso de auditoría de redes
- ¿Dónde están las joyas de la corona en la red?
- Mantener una lista organizada de qué componentes de red existen y cuándo será auditado cada uno
  - Auditar redes por funciones
  - Muchos dispositivos cumplen hoy múltiples funciones

Routers

Preparación de la Auditoría

- Definir el Alcance
- Realizar la Investigación
  - ¿Qué está siendo protegido?
  - ¿Qué riesgos existen?
  - ¿Cómo está configurado el router?
  - ¿Cuál es la arquitectura?
  - ¿Qué procesos existen?

Fuentes para Investigación

- Entrevistas
  - Equipo de Auditoría
  - Administradores de Sistemas
  - Administradores de Red
  - Equipo de Políticas
  - Seguridad de la Información
- Documentación del Router
  - Definición funcional del Router
  - Diagramas de Red
- Fuentes Externas
  - Alertas y boletines del fabricante del Sistema
  - Alertas de Vulnerabilidades de SANS
  - Grupos de usuarios/grupos de discusión
  - Fuentes de “Mejores Prácticas”

Arquitectura

- La Arquitectura de los Routers debe soportar el flujo de información
  - ¿Qué información está siendo protegida?
- ¿Qué Sistema Operativo y nivel de parches está siendo usado?
- ¿Cuál es el rol del Router?
  - Router de Borde
    - Opciones de Arquitectura:
      - Router como única línea de defensa
      - Router trabajando con un firewall
  - Router Interior
  - Router Backbone

Procesos de Prueba

- Procesos
  - Control de Cambios
  - Copias de Seguridad
  - Administración de Usuarios
  - Política de Contraseñas
  - Actualizaciones de Parches
  - Construcciones seguras y estandarizadas para plataformas de Routers
- Conducir entrevistas
- Revisar documentación
- Realizar Simulacros

Verificación del Proceso de Simulacros

- Mostrar una alerta reciente
- Entender el procedimiento utilizado actualmente por los Administradores para abordar las alertas
- Obtener evidencia de auditoría de que el proceso está en funcionamiento
  - Entrevista
  - Observación
- Sugerir mejoras al proceso

¿Por qué Routers Cisco?

- Tiene la mayor cuota de mercado de Routers de Internet
- Los conceptos pueden ser aplicados a cualquier Router
- Al ser basados en línea de comandos, pueden ser más difícil de administrar y aprender a auditarlos posibilitará aplicar este conocimiento a routers de otros vendedores

Archivos de Configuración

- Startup-Config
  - Cargado al inicio
  - Router# ***show startup-config***
- Running-Config
  - Configuración real siendo utilizada
  - Los cambios en vivo son hechos a running-config
  - Router# ***show running-config***
- Almacenar la configuración actual como configuración de inicio
  - Router# ***copy running-config startup-config***

Filtrado Estático de Paquetes

- Es el Control de Tráfico implementado en la mayoría de los routers
- Funciona dividiendo y midiendo
  - Si le decimos al router “permit traffic to 220.10.5.0/24”
    El router evalúa:
    - ¿El byte 16 en el encabezado IP contiene 220?
    - ¿El byte 17 en el encabezado IP contiene 10?
    - ¿El byte 18 en el encabezado IP contiene 5?
    - De ser así, permitir que el tráfico pase
    - De no ser así, procesar la siguiente regla

Filtrado Con Estado

- La mayoría de las conexiones de red están basadas en estímulos de respuesta
  - Esto significa que tenemos que permitir que las respuestas entren a nuestra red.
- **Problema**: los paquetes pueden ser manipulados para parecer respuestas inofensivas
- El Filtrado Con Estado “recuerda” el tráfico saliente entonces solo las respuestas legítimas son permitidas para ingresar.

Cuando usar Estático o Con Estado

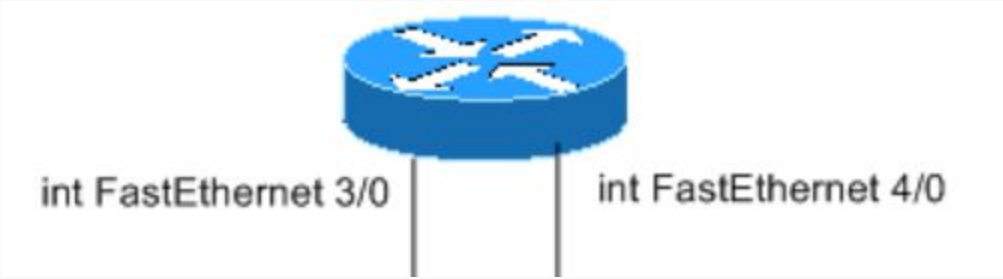
- Usar **Estático** para decisiones absolutas
  - Bloquear tráfico originado desde una dirección IP privada
  - Bloquear todo el tráfico direccionado a los puertos SNMP
  - Bloquear todos los echo-requests (Ping) entrantes
- Usar **Con Estado** para decisiones condicionales
  - Nada o… para todo lo demás
  - El despliegue del Router es dependiente en la configuración del perímetro

Listas de Control de Acceso (ACLs)

- Las ACLs controlan el tráfico hacia y a través del router
- Cisco tiene múltiples tipos de ACLs
  - **ACLs Estándar**: 1-99 o 1300-1999. Dirección IP Origen.
  - **ACLs Extendidas**: 100-199 o 2000-2699. Encabezado del paquete.
  - **ACLs Reflexivas**: Usan tablas de estados. Son dinámicas.
  - **ACLs Nombradas**: se asignan nombres descriptivos en lugar de números.
- Las ACLs pueden ser Estáticas o Con Estado dependiendo del fabricante y de las capacidades del router

Creando el Filtrado de Paquetes

- Para usar una ACL, el Router necesita saber donde debería ser aplicada
  - ¿Qué interfaz debería usar la ACL?
  - ¿En qué dirección? (Entrante/Saliente)



Revisando las ACLs

- Revisar cantidades para cada regla
  - ¿Están siendo usadas las reglas?
  - Sino, ¿por qué no?
    - El tráfico no ha sido visto
      - Generar el patrón y probar nuevamente
    - El orden de las reglas es incorrecto
      - Sugerir remediación basada en reglas
  - Comparar contra una base de reglas
    - ¿Están las reglas que coinciden con más frecuencia al principio?
    - Sino, sugerir optimizar el orden de las reglas

Accediendo a los Routers

- Métodos de Administración y Configuración
  - Local
    - Es el mejor, pero no siempre es realista
  - Remoto
    - Telnet, SSH, HTTP, SNMP, TFTP
- Acceso Seguro
  - Red de Administración
  - Comunicación Cifrada
    - SSH, IPSec

Auditando Métodos de Acceso

- Deshabilitar acceso administrativo que no es necesario
  - El acceso remoto (directo) debería ser deshabilitado si no es necesario
- Acceso cifrado (por ejemplo, SSH, IPSec) es preferido sobre telnet para acceso remoto
  - Controlar el acceso remoto al router a través de ACLs
- Usar timeouts para inactividad de la sesión

Autenticación

- Usar cuentas individuales por Administrador para control de accesos
- Administrar Autenticación, Autorización y Responsabilidad (Accountability)
- Las cuentas centralizadas pueden ser usadas a través de RADIUS, TACACS, etc.

SNMP

- Es recomendable deshabilitar SNMP completamente
- Prohibir las “community strings” de lectura-escritura
- Prohibir las “community strings” por defecto
  - Públicas
  - Privadas
- Acotar el acceso a direcciones autorizadas con ACLs

Deshabilitar los Servicios de Administración Innecesarios

- Finger
  - Provee información de un usuario en un sistema
- Identd
  - Identifica el propietario de una conexión entre un cliente y un servidor
- HTTP
  - Servidor web

Cifrado de Contraseñas

- Verificar como están almacenadas las contraseñas
  - ¿Qué algoritmos de cifrado/hash están siendo utilizados?
- Verificar quién tiene acceso a los hashes
- Verificar cómo es realizada la autenticación a lo largo de la red

AAA (Autenticación, Autorización y Responsabilidad)

- Asegurar que la actividad de los usuarios está siendo auditada
- ¿Qué debería ser auditado?
  - Revisar la política
  - Como mínimo:
    - Acceso al sistema - Exitoso y Fallido
    - Actividad administrativa
    - Auditar las fallas
    - Auditar los cambios a la configuración

Firewalls

Asegurando el Perímetro ¿Dónde está el fin del Perímetro?

- Hay una gran cantidad de potenciales puntos de acceso hacia nuestras redes:
  - VPNs / Modems (B2B)
  - Wireless
  - Router de Borde
  - Firewall de Perímetro

Defensa en Profundidad (DiD)

- Las “Capas” deben ser incorporadas en la seguridad
  - Firewalls de Perímetro
  - Firewalls internos
  - Sistemas de Detección de Intrusiones (IDS)
  - Routers de Borde
  - Routers Internos
  - Políticas y Procedimientos
  - Auditorías
- Múltiples controles deben estar presentes y ser evaluados

¿Por qué realizar Auditoría de Perímetro?

- Reglas de Filtrado Complejas
- Muchos cocineros echan a perder la sopa
- Errores en el código del fabricante
    - La Auditoría es una capa de Defensa en Profundidad

Filtros de Firewall vs Filtros de Router

- Los conceptos son los mismos
  - Difieren en base a las expectativas de la política
- Deben complementarse entre ellos
  - No necesariamente tener reglas iguales
- Aprovechar las fortalezas de cada uno
- Múltiples filtros en servicios críticos
- Prueba de Salud
  - ¿Tienen sentido las reglas para el entorno?

Conceptos Claves de Auditoría de Firewall

- Política de Seguridad
  - Debería ser un documento escrito
- Permitido por Defecto vs Rechazado por Defecto
- Grupos
  - Equipos, redes o servicios similares
- Zonas de Seguridad
  - Grupos de equipos y/o redes
  - Criticidad similar y requerimientos de acceso

Temas Fundacionales de Firewall (1/2)

- Filtrado de Paquetes
  - Rápido, baja seguridad
- Inspección Con Estado
  - Rendimiento medio, Seguridad media
- Proxy o Gateway de Aplicaciones
  - Lento, Seguridad más alta
- Inspección Profunda de Paquetes
  - Combina la Inspección Con Estado y la tecnología IDS o el Protocolo de Detección de Anomalías

Temas Fundacionales de Firewall (2/2)

- NAT (Network Address Translation)
  - Permite el uso de direcciones privadas en la Intranet (RFC1918)
  - Variaciones
    - Reenvío o Redirección de Puertos
    - Muchos a Uno (NAT oculto)
    - Uno a Uno (NAT estático)
    - Pool de Direcciones NAT

Preparación de la Auditoría

Política

- Antes de comenzar la Auditoría, debe definirse el propósito del firewall
  - ¿Qué se espera que haga el firewall?
  - Debe estar basado en la Política de Seguridad
- Si no hay Política de Seguridad, debe iniciarse una conversación con la Dirección
  - Un gran comienzo puede ser comenzar a escribir las reglas en el lenguaje del firewall

Cuestiones a Definir

- ¿Qué Información está protegiendo el Firewall?
- ¿Cuáles son las expectativas del Firewall?
- ¿Qué riesgos está dispuesta a aceptar la organización?
- ¿Qué acciones son autorizadas?

Procedimientos

- Control de Cambios
- Copias de Seguridad
- Administración de Usuarios
- Política de Contraseñas
- Actualizaciones de Parches
- Construcciones seguras y estandarizadas de plataformas de Firewall

Arquitectura de Firewall

Arquitectura de Firewall

- Revisar la Arquitectura de Firewall
  - ¿La Política de Seguridad es soportada por la arquitectura?
  - ¿Hubs?
  - ¿Switches?
- Definir cómo la información debería fluir
  - ¿Qué flujo de datos está y no está autorizado?
- Diseñadores de Firewall y Perímetro tienden a usar diagramas físicos
  - El auditor deber ser capaz de deducir el flujo de información y posiblemente un diagrama lógico desde un diagrama físico

Diagrama Lógico

- El propósito de un Diagrama Lógico es mostrar el flujo de información
  - Permite definir qué información puede fluir hacia donde
  - La Política de Seguridad define qué y qué no está autorizado
- El propósito del firewall es controlar el flujo de información
- Ejemplo: Arquitectura de un Sitio de E-commerce
  - Necesita una red dedicada separada para el comercio B2B
  - Sin embargo, el sitio de E-commerce debe ser capaz de comunicarse con lo corporativo (bases de datos)

Preguntas de Arquitectura

- ¿El Firewall segmenta la información correctamente?
  - ¿Agregar o quitar un firewall?
  - ¿Agregar o quitar una interfaz de red?
  - ¿Se están siguiendo los procedimientos de arquitectura?
- La Arquitectura debe soportar la Política de Seguridad
  - Si la arquitectura del firewall está mal hecha, es poco lo que la base de reglas del firewall podrá hacer

Firewall de Aplicaciones Web (WAF)

- Diseñado para proteger los sitios web de ataques
- Aplican un conjunto de reglas a una conversación HTTP
- Controlan la ejecución de la información, no solo el flujo de datos
- Sitio Principal de WAFs de OWASP
- Criterio de Evaluación de WAFs de OWASP

Arquitectura y Entornos B2B

- Se confía también en los controles del otro negocio
- Se debe mantener la documentación adecuada
- Ver su Política de Seguridad
- Se debe firmar un Acuerdo
- Política de Acceso y Controles de Autenticación
- Aplicaciones Propietarias: Métodos y Requerimientos de Seguridad, Controles de Autorización, Cifrado, Logging.
- Planes de Respuesta ante Incidentes
- Arquitectura
- Cifrado punto a punto

Probando el Firewall

Plataforma - ¿Dispositivo (Appliance) o Sistema Operativo?

- Dispositivo (Appliance)
  - Ventajas
    - Normalmente viene completamente asegurada
    - Diseñadas desde cero como dispositivos firewall
  - Desventajas
    - Muchas son cerradas y propietarias
    - Se debe confiar la seguridad al vendedor
- Sistema Operativo
  - Ventajas
    - Mayor control sobre el aseguramiento del sistema
    - Muchos proveen el código fuente
  - Desventajas
    - Se debe tener mayor control sobre el aseguramiento del sistema
    - Grandes oportunidades de cometer errores

Específico de la Plataforma de Firewall

- Considerar el Firewall específico que se está auditando
  - ¿Hay opciones de configuración que se desvían de la base de reglas?
  - ¿Hay características de seguridad que son específicas a la plataforma que se está auditando?
- Recursos
  - Revisar la documentación del fabricante

Probando la Base de Reglas del Firewall

Validación Manual de la Base de Reglas

- Comenzar revisando la base de reglas manualmente
  - Eliminar cualquier regla innecesaria
    - Armar equipo con el Gerente de Seguridad, Administrador de Firewall y Arquitecto de Redes
  - Combinar las repetitivas
  - Identificar cualquier regla no autorizada
  - Finalizar con la menor cantidad de reglas posible

Consejos sobre la Base de Reglas

- El ordenamiento de las reglas debe ser mantenido tan simple como sea posible
- Verificar reglas pasadas por alto o implícitas
- Verificar qué reglas tienen el logging habilitado
  - Sólo debe loguearse lo que es necesario
- Todas las reglas deberían estar documentadas
  - Para qué existe, quién la autorizó y cuando fue cambiada

Auditar Reglas de Filtrado

- ¿Cumplen las reglas de filtrado la política y/o mejores prácticas?
- ¿Están autorizadas y optimizadas?
- Recomendar cambios como sea necesario
  - Siempre explicar:
    - Razón para el cambio
    - Beneficio del cambio

Recomendaciones de Reglas de Base de Firewall

- Debería existir una política de “Rechazado por Defecto”
- Las reglas:
  - Deberían ser específicas
  - No deben superponerse o duplicarse entre sí
  - No deberían contradecir a otras reglas
  - Deberían ser utilizadas (aplicadas)
- Los servicios deberían estar configurados de manera segura
- El Logging debería ocurrir para las reglas donde sea necesario
- Todas las reglas deberían tener una justificación de negocio

Validación Técnica de la Base de Reglas

- Validar la base de reglas del firewall desde el nivel de red a través del escaneo
  - Escanear a través del firewall
  - Determinar que paquetes el firewall permite que pasen
- Escanear cada red desde cada interfaz
  - Una laptop puede reemplazar sistemas en la red de servicio y escanear la red interna para simular un compromiso

¿Qué herramientas utilizar?

- Cualquier conjunto de herramientas debería, como mínimo, proveer las siguientes tres capacidades:
  - Herramientas de Mapeo de Red
    - Hping, nemesis, nmap
  - Análisis de Vulnerabilidades Pasivo
    - Wireshark, tcpdump, windump
  - Análisis de Vulnerabilidades Activo
    - Nessus, OpenVAS

Permiso de Ejecución

- La diferencia entre un hacker malicioso y un analista de seguridad es el Permiso de Ejecución
  - ¡Siempre se necesita!
  - ¡Por escrito!
  - De individuos autorizados

Alertas y Logging

Revisión de Logs

- Durante la ejecución de la Auditoría, se produjo mucho “ruido” ¿Fue detectado?
  - ¿Fueron detectadas estas exploraciones?
  - ¿Fue alertada la gente apropiada?
  - ¿Se está registrando información adecuada?
  - ¿Se están perdiendo entradas en los logs?
  - ¿Se revisan con frecuencia las entradas en los logs?
- Estudiar y aprender las firmas (signatures) en los logs

NAC,
Detección de Intrusiones y
Prevención de Intrusiones

Sobre NAC (Network Access Control)

- Controla los endpoints
  - Toma decisiones antes de permitir a los sistemas conectarse a la red
  - Las políticas controlan el acceso
- Centraliza la administración de tecnologías como antivirus, prevención de intrusiones de equipos, autenticación, etc.
- El objetivo de NAC es:
  - Controlar los ataques “Zero-day”
  - Permitir a los administradores la definición de políticas
  - Autenticar identidades de usuario

Pasos de Verificación de Detección/Prevención de Intrusiones (NIDS/NIPS)

- Usar nmap para verificar la detección de escaneo de puertos
  - Probar múltiples velocidades
- Usar un Analizador de Vulnerabilidades como Nessus para verificar la detección de Payloads
- Usar fragrouter para probar la fragmentación de paquetes
- Combinar con un Sniffer para verificar precisión

Auditoría de IDS/IPS

- ¿Cuál es la Arquitectura?
  - Basados en Red versus basados en Host
- ¿Detectó el IDS/IPS la mayoría de los ataques?
  - ¿Está la base de firmas actualizada?
- ¿Es utilizable el sistema de alertas?
  - ¿Envía mensajes o agrega registros a un archivo que nadie lee?
- ¿Tiene sentido su ubicación en la red?
  - ¿Está conectado al puerto de un switch?

¿Preguntas?

¡Muchas Gracias!