Explotación de vulnerabilidades

Indice

1. Introducción a las vulnerabilidades en routers y puertas de enlace:
2. Clasificación de vulnerabilidades
3. Identificación y explotación de vulnerabilidades
4. Medidas de mitigación y protección

Objetivos

- Comprender los conceptos básicos de las vulnerabilidades en routers y puertas de enlace.
- Identificar y clasificar diferentes tipos de vulnerabilidades comunes en estos dispositivos.
- Conocer las técnicas utilizadas por los hackers para explotar las vulnerabilidades y obtener acceso no autorizado.
- Aprender sobre los ataques de denegación de servicio (DoS) y cómo se pueden dirigir a routers y puertas de enlace.
- Aplicar medidas de mitigación y protección para prevenir y defenderse de las vulnerabilidades y ataques en routers y puertas de enlace.

Introducción

Vulnerbailidades: debilidades o fallos en el diseño, implementación o configuración de un sistema o dispositivo que pueden ser aprovechados por personas malintencionadas para comprometer la seguridad y obtener acceso no autorizado o realizar acciones no deseadas. En el contexto de los dispositivos de red, como los routers y las puertas de enlace, las vulnerabilidades representan **riesgos significativos para la integridad, confidencialidad y disponibilidad de la red**.

Introducción

Relevancia del reconocimiento de vulnerabilidades

1. **Exposición de la infraestructura de red**: Las vulnerabilidades en routers y puertas de enlace pueden proporcionar una puerta de entrada a la red, permitiendo a los atacantes ingresar y comprometer otros sistemas y datos sensibles.
2. **Pérdida de confidencialidad**: Las vulnerabilidades pueden permitir la **interceptación** de datos confidenciales que se transmiten a través del dispositivo de red, como contraseñas, información personal o datos comerciales sensibles.

Introducción

3. **Alteración de la integridad de la red**: Los atacantes pueden explotar vulnerabilidades para modificar o manipular el tráfico de red, redirigirlo hacia destinos maliciosos o modificar la configuración del dispositivo, lo que compromete la integridad y confiabilidad de la red.

4. **Interrupción de la disponibilidad**: Los ataques basados en vulnerabilidades pueden causar una interrupción completa o parcial de los servicios de red al agotar los recursos del dispositivo o sobrecargarlo con tráfico malicioso, lo que resulta en una falta de disponibilidad de los servicios para los usuarios legítimos.

Introducción

6. **Riesgos para la privacidad y cumplimiento normativo**: Las vulnerabilidades pueden permitir el acceso no autorizado a información confidencial, lo que puede violar la privacidad de los usuarios y poner en riesgo el cumplimiento de regulaciones y normativas de protección de datos.

Tipos de vulnerabilidades

Vulnerabilidades de seguridad y configuración

Vulnerabilidad	Descripción
Falta de actualizaciones y parches	No aplicar las actualizaciones de firmware o parches de seguridad proporcionados por el fabricante.
Configuraciones por defecto inseguras	Utilizar configuraciones predeterminadas inseguras que no ofrecen suficiente protección o restricciones.
Fallos en cifrado y autenticación	Errores en los algoritmos de cifrado o en los mecanismos de autenticación utilizados, lo que facilita el acceso no autorizado.
Puertos y servicios innecesarios expuestos	Tener puertos y servicios abiertos y expuestos innecesariamente, lo que aumenta el riesgo de ataques y compromisos.

Tipos de vulnerabilidades

Vulnerabilidades de autenticación y gestión de acceso

Vulnerabilidad	Descripción
Autenticación débil o predeterminada	Uso de contraseñas débiles o predeterminadas que pueden ser fácilmente adivinadas o explotadas.
Falta de bloqueo de cuenta tras intentos fallidos	No bloquear o restringir el acceso a una cuenta después de un número determinado de intentos fallidos de inicio de sesión.
Uso de protocolos no seguros	Utilización de protocolos de autenticación o gestión de acceso no seguros, como Telnet o HTTP en lugar de SSH o HTTPS.
Insuficiente gestión de permisos	Falta de una gestión adecuada de los permisos de usuario y privilegios, lo que permite el acceso no autorizado a funciones críticas.

Tipos de vulnerabilidades (otros)

1. **Vulnerabilidades de inyección de comandos**: Estas vulnerabilidades ocurren cuando los routers y las puertas de enlace no validan o filtran adecuadamente las entradas de los usuarios. Los atacantes pueden aprovechar esto para insertar comandos maliciosos en los campos de entrada, lo que les permite ejecutar comandos arbitrarios en el dispositivo y obtener acceso no autorizado.
2. **Vulnerabilidades de desbordamiento de búfer**: Estas vulnerabilidades ocurren cuando un router o una puerta de enlace no maneja adecuadamente la entrada de datos y permite que se escriba más información de la esperada en una ubicación de memoria, lo que puede llevar a la ejecución de código malicioso o a la denegación de servicio.

Tipos de vulnerabilidades (otros)

3. **Vulnerabilidades de enrutamiento malicioso**: Estas vulnerabilidades permiten a los atacantes manipular las tablas de enrutamiento del dispositivo, redirigiendo el tráfico hacia destinos maliciosos o interceptando el tráfico legítimo. Esto puede afectar la disponibilidad, integridad y confidencialidad de las comunicaciones en la red.

Métodos para identificar vulnerabilidades

- **Escaneo de puertos**: Se utiliza para identificar los puertos abiertos en un router o una puerta de enlace. Al identificar los puertos abiertos, se puede determinar qué servicios o protocolos están disponibles y, en consecuencia, analizar su seguridad y posibles vulnerabilidades asociadas.
- **Análisis de configuración**: Implica examinar la configuración del router o la puerta de enlace para identificar errores o configuraciones inseguras. Esto puede incluir la revisión de contraseñas débiles, configuraciones de autenticación inadecuadas, servicios innecesarios habilitados y configuraciones de firewall incorrectas.

Métodos para identificar vulnerabilidades

- **Análisis de tráfico de red**: Se utiliza para monitorear y analizar el tráfico de red que pasa a través del router o la puerta de enlace. Esto puede revelar actividades sospechosas o anómalas que podrían indicar la existencia de una posible vulnerabilidad o un intento de explotación.
- **Revisión de seguridad de firmware y actualizaciones**: Implica verificar y evaluar las actualizaciones de firmware y parches de seguridad proporcionados por el fabricante del router o la puerta de enlace. Al mantener el firmware actualizado y aplicar los parches de seguridad, se pueden corregir vulnerabilidades conocidas y mejorar la seguridad del dispositivo.

Métodos para identificar vulnerabilidades

- **Análisis de vulnerabilidades conocidas**: Se utilizan herramientas automatizadas, como Nessus o OpenVAS, para realizar escaneos de vulnerabilidades en routers y puertas de enlace. Estas herramientas comparan las versiones del firmware o del sistema operativo utilizadas por el dispositivo con una base de datos de vulnerabilidades conocidas, identificando así las posibles vulnerabilidades presentes en el dispositivo.

Practica

Actividad: Enumera las vulnerabilidades de un router usando herramientas privadas (OpenVAS) y herramientas open source (nuclei)

- **Objetivos**
- Reconocer las ventajas y desventajas del uso de herramientas para analizar vulnerabilidades
- Aprender a utilizar herramientas para enumerar vulnerabilidades de un router o puerta de enlace
- Conocer el procedimiento para realizar una auditoría de seguridad relacionada con la evaluación de vulnerabilidades:

Métodos para explotar vulnerabilidades

Técnica	Descripción
Inyección de comandos	Aprovechar las vulnerabilidades para inyectar comandos maliciosos en campos de entrada y ejecutar acciones no autorizadas.
Ataques de denegación de servicio (DoS)	Sobrecargar el router con tráfico o solicitudes masivas, agotando sus recursos y causando una interrupción de servicios.
Explotación de vulnerabilidades conocidas	Aprovechar las vulnerabilidades previamente identificadas y documentadas en el router para obtener acceso no autorizado o control sobre el dispositivo.
Ataques de enrutamiento malicioso	Manipular las tablas de enrutamiento para redirigir el tráfico hacia destinos maliciosos o interceptar la comunicación legítima.
Ataques de fuerza bruta	Realizar intentos repetitivos de adivinar contraseñas hasta encontrar la correcta y obtener acceso no autorizado al router.
Explotación de debilidades en protocolos de enrutamiento	Aprovechar vulnerabilidades en los protocolos de enrutamiento utilizados por el router para manipular el enrutamiento y obtener acceso no autorizado.

Practica

Actividad: Simula ataques sobre routers y puertas de enlace

Objetivos:

- Conocer el proceso para desarrollar una auditoria de seguridad sobre routers y puertas de enlace
- Distinguir los diferentes aspectos involucrados en los ataques a routers y puertas de enlace
- Conocer herramientas para la realización de auditorias de seguridad en routers y puertas de enlace

Practica

1. Code injection
2. DDoS
3. Envenenamiento de ARP o ARP spoofing

Medidas de mitigación y protección

Code Injection

Medida	Descripción
Validación y filtrado de entrada de datos	Realizar una validación estricta de todos los datos de entrada, verificando su tipo, longitud y formato adecuados.
Utilizar parámetros preparados o consultas parametrizadas	Emplear consultas SQL parametrizadas en lugar de concatenar directamente datos de entrada en las consultas SQL.
Escapado o sanitización de salida	Escapar o sanitizar adecuadamente los datos de salida que se muestran en el navegador o en otros sistemas, evitando la ejecución de código malicioso.
Actualizaciones y parches	Mantener actualizados los sistemas y aplicaciones con los últimos parches y actualizaciones de seguridad proporcionados por los proveedores y fabricantes.
Pruebas de seguridad y revisión de código	Realizar pruebas de seguridad y revisiones de código para identificar y corregir posibles vulnerabilidades de inyección de código.

Mitigación: DDoS

Medida	Descripción
Implementación de firewalls	Utilizar firewalls para filtrar y bloquear el tráfico malicioso o sospechoso antes de que llegue al servidor o a la red, limitando el impacto de los ataques DoS.
Configuración de límites y políticas de tráfico	Establecer límites y políticas de tráfico para limitar la cantidad de solicitudes y conexiones que un cliente puede hacer en un determinado período de tiempo.
Implementación de sistemas de detección y prevención de intrusiones (IDS/IPS)	Utilizar sistemas de detección y prevención de intrusiones para identificar y bloquear patrones y comportamientos de tráfico maliciosos relacionados con ataques DoS.
Balanceo de carga y redundancia	Implementar soluciones de balanceo de carga y tener sistemas redundantes para distribuir el tráfico y mitigar los impactos de los ataques DoS.
Uso de servicios de mitigación de DDoS	Contratar servicios de mitigación de ataques de denegación de servicio distribuido (DDoS) que puedan detectar y mitigar automáticamente los ataques.
Configuración de límites de recursos	Establecer límites de recursos, como ancho de banda, número de conexiones o uso de CPU, para limitar el impacto de los ataques DoS y proteger los recursos del sistema.
Monitoreo y análisis de tráfico	Implementar herramientas de monitoreo y análisis de tráfico para identificar patrones de ataque, anomalías y comportamientos maliciosos relacionados con ataques DoS.
Plan de respuesta a incidentes	Tener un plan de respuesta a incidentes que contemple acciones específicas para mitigar y manejar los ataques de denegación de servicio.

Medidas de mitigación y protección contra ARP spoofing

Medida	Descripción
Seguridad física y control de acceso	Mantener un control estricto sobre el acceso físico a los dispositivos de red para evitar ataques de envenenamiento de ARP realizados desde dentro de la red.
Implementación de VLANs	Utilizar VLANs (Virtual LANs) para segmentar la red en dominios de difusión más pequeños y evitar que un atacante pueda realizar envenenamiento de ARP en toda la red.
Configuración de tablas ARP estáticas	Configurar tablas ARP estáticas en los dispositivos de red para establecer manualmente las correspondencias entre direcciones IP y MAC, evitando así el envenenamiento de ARP.
Uso de DHCP Snooping y ARP Inspection	Implementar funcionalidades como DHCP Snooping y ARP Inspection en los switches para monitorear y filtrar el tráfico ARP, previniendo así ataques de envenenamiento.
Implementación de autenticación de dispositivos	Utilizar técnicas de autenticación, como IEEE 802.1X, para asegurarse de que solo los dispositivos autorizados puedan conectarse y comunicarse en la red.
Uso de ARP Spoofing Detection Tools	Utilizar herramientas especializadas de detección de ARP Spoofing que monitoreen continuamente el tráfico ARP en busca de posibles ataques y generen alertas en caso de detección.
Configuración de detección y prevención de ARP Spoofing en firewalls	Configurar reglas en los firewalls para detectar y bloquear el tráfico de envenenamiento de ARP, evitando así que los paquetes ARP maliciosos lleguen a los dispositivos.
Monitoreo y análisis de tráfico	Implementar soluciones de monitoreo y análisis de tráfico para identificar patrones de envenenamiento de ARP, anomalías y comportamientos sospechosos en la red.
Mantener el software actualizado y parcheado	Mantener actualizados los sistemas operativos, firmware y aplicaciones de red, instalando los últimos parches de seguridad disponibles para protegerse contra las vulnerabilidades conocidas de envenenamiento de ARP.