ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN - 2024

GRUPO 8

SNIFFERS Y ESCANEO DE PUERTOS

Ministerio de Educación
Universidad Tecnológica Nacional
Facultad Regional Mendoza

INTEGRANTES:

- Cucharelli Santiago
- Galdeano Huilen
- Ledesma Jennifer
- Leon Quispe Mario Cesar
- Malgioglio Lucio
- Maya Facundo
- Vaieretti Roberto

1. Introducción

El avance de la tecnología ha traído consigo herramientas que permiten analizar y supervisar el tráfico en redes informáticas. Dos de estas herramientas son los sniffers y el escaneo de puertos. El uso de estas tecnologías puede ser útil para tareas legítimas como el diagnóstico de redes, pero también pueden ser utilizadas con fines maliciosos. Este informe aborda qué son los sniffers y el escaneo de puertos, su uso, así como su legalidad en Argentina.

2. ¿Qué es un Sniffer?

Un sniffer es una herramienta que permite capturar y analizar el tráfico de una red. Su funcionamiento se basa en interceptar los paquetes de datos que circulan por la red, lo que permite al usuario visualizar el contenido de estos paquetes (Avast, n.d.). Esta tecnología es frecuentemente utilizada para monitorear y diagnosticar redes, pero en manos equivocadas puede ser utilizada para interceptar información privada, como contraseñas o datos bancarios (UNIR, n.d.).

3. Tipos de Sniffers

Existen diferentes tipos de sniffers que se pueden clasificar de acuerdo a su comportamiento y la forma en que interceptan el tráfico de la red:

3.1. Sniffers pasivos

Se limitan a capturar datos sin alterar el tráfico de la red. Funcionan en redes con conmutadores (switches) o concentradores (hubs) y son difíciles de detectar porque solo están "escuchando".

3.2. Sniffers activos

No solo escuchan, sino que también pueden enviar paquetes a la red para generar respuestas o alterar el tráfico, lo que los hace más detectables pero también más peligrosos en manos malintencionadas.

3.3. Sniffers basados en hardware

Son dispositivos físicos conectados a la red que interceptan y capturan el tráfico sin necesidad de software adicional.

3.4. Sniffers basados en software

Aplicaciones que se instalan en un sistema para capturar el tráfico de la red. Ejemplos incluyen Wireshark y tcpdump, que pueden ser utilizados para análisis de redes legítimas o con fines maliciosos (UNIR, n.d.).

4. Cómo protegerse de un ataque de Sniffer

Para protegerse de un ataque de sniffer, es importante adoptar medidas de seguridad que aseguren el tráfico en la red:

4.1. Cifrado de datos

Utilizar protocolos de cifrado, como HTTPS, SSL o TLS, para proteger la información transmitida en la red. El cifrado hace que, aunque un atacante capture los datos, no pueda leerlos sin la clave de descifrado.

4.2. Redes privadas virtuales (VPN)

Una VPN cifra todo el tráfico de internet y oculta la dirección IP, lo que reduce la probabilidad de que un atacante intercepte comunicaciones sensibles.

4.3. Seguridad de las contraseñas

Usar contraseñas fuertes y únicas para cada cuenta, además de habilitar la autenticación de dos factores (2FA), lo que añade una capa extra de seguridad en caso de que un atacante obtenga acceso a la red.

4.4. Monitoreo de redes

Implementar herramientas de monitoreo para detectar cualquier tráfico inusual o actividad sospechosa en la red, lo que puede indicar la presencia de un sniffer (Avast, n.d.).

4.5. Evitar el uso de redes desconocidas o no seguras

Utilizar una red pública o desconocida significa exponer el tráfico que realizamos en Internet o hacia otros dispositivos, si hay un sniffer en la red que esté recolectando información. En la actualidad, el caso más común sería conectarse a una red WiFi “gratuita”, cuyo administrador puede estar utilizando para monitorear el tráfico de red (Innovación Digital, n.d.).

5. Herramientas Comunes

5.1. Wireshark

Una de las herramientas de análisis de paquetes más populares.

5.2. Tcpdump

Herramienta de línea de comandos para capturar y analizar tráfico.

6. ¿Cómo detectar un Sniffer?

Detectar un sniffer en una red puede ser complicado, especialmente si es pasivo. Sin embargo, existen algunas técnicas para identificar su presencia:

6.1. Enviar paquetes "trampa"

Algunos sniffers responden a paquetes especialmente diseñados que no deberían generar una respuesta en condiciones normales. Si se recibe una respuesta, es una señal de que hay un sniffer activo en la red.

6.2. Inspección del uso de la interfaz de red

Los sniffers suelen cambiar la configuración de la interfaz de red a "modo promiscuo", lo que permite capturar todo el tráfico de red, no sólo el destinado al dispositivo. Algunas herramientas de red pueden detectar si una interfaz está en modo promiscuo, lo que indica la posible presencia de un sniffer.

6.3. Herramientas de detección de sniffers

Existen aplicaciones como AntiSniff que pueden ayudar a detectar sniffers en la red, monitoreando los cambios en las interfaces y el tráfico de red inusual (UNIR, n.d.).

7. Escaneo de Puertos

El escaneo de puertos es una técnica utilizada para identificar los puertos abiertos y disponibles en un sistema. Los puertos representan puntos de acceso a servicios específicos, como web o correo electrónico, y al ser abiertos pueden convertirse en puntos vulnerables. El escaneo de puertos ayuda a determinar qué servicios están activos en un servidor o dispositivo, y si esos servicios pueden representar un riesgo para la seguridad (Avast, n.d.).

8. Tipos de escaneo de puertos

Existen varios métodos de escaneo de puertos que varían en complejidad y eficacia:

8.1. Escaneo de puertos TCP

Este es el tipo más común y efectivo. Intenta establecer una conexión completa con cada puerto en el sistema objetivo, permitiendo al atacante o administrador saber si el puerto está abierto.

8.2. Escaneo de puertos SYN

También conocido como escaneo furtivo, este método envía paquetes SYN sin completar la conexión. Es más rápido y menos detectable que el escaneo TCP tradicional.

8.3. Escaneo de puertos UDP

Busca puertos abiertos en los servicios que utilizan el protocolo UDP. A menudo es más lento y complicado, ya que UDP no ofrece confirmación de paquetes como lo hace TCP.

8.4. Escaneo de puertos ACK

Esta técnica se utiliza para determinar si un puerto está filtrado (por un firewall, por ejemplo) y puede ayudar a mapear las reglas de un cortafuegos.

9. Herramientas Comunes

9.1. Nmap

Una herramienta popular y poderosa para el escaneo de puertos y mapeo de red.

9.2. Netcat

Utilizada para explorar redes y gestionar conexiones.

10. Relación entre Sniffers y Escaneo de Puertos

El escaneo de puertos y los sniffers pueden estar relacionados en un ataque de red. Mientras que el escaneo de puertos permite a un atacante identificar qué puertos están abiertos y qué servicios están en funcionamiento, un sniffer puede interceptar y analizar el tráfico que pasa a través de esos puertos. En conjunto, estas herramientas pueden ser utilizadas para detectar vulnerabilidades y extraer información confidencial.

Por ejemplo, un atacante puede usar un escáner de puertos para encontrar un puerto abierto en el que esté corriendo un servicio inseguro. Luego, podría usar un sniffer para capturar los datos que viajan a través de ese puerto y obtener información sensible, como contraseñas o credenciales de inicio de sesión (Avast, n.d.).

El escaneo de puertos también puede alertar a un administrador sobre posibles intentos de ataque, ya que una gran cantidad de escaneos no solicitados pueden ser un indicio de que un atacante está buscando vulnerabilidades. Esto permite a los administradores tomar medidas preventivas antes de que un sniffer sea instalado o utilizado para capturar datos.

11. Cómo protegerse de un escaneo de puertos

11.1. Configurar un firewall

Un firewall correctamente configurado puede bloquear el tráfico de escaneo no autorizado y filtrar paquetes entrantes y salientes.

11.2. Cerrar puertos innecesarios

Asegurarse de que solo los puertos esenciales estén abiertos, minimizando los puntos de entrada que un atacante podría utilizar.

11.3. Usar herramientas de detección de intrusiones (IDS)

Estas herramientas pueden detectar patrones de escaneo de puertos y alertar a los administradores de red sobre actividades sospechosas.

12. Legalidad en Argentina

En Argentina, el uso de sniffers y el escaneo de puertos está regulado por la Ley 25.326 de Protección de Datos Personales y otras normativas relacionadas con delitos informáticos. El uso de estas tecnologías sin consentimiento está prohibido y puede considerarse una violación de la privacidad o un intento de acceso no autorizado. Sin embargo, su uso es legal si se realiza en redes bajo control del administrador y con el consentimiento de los usuarios, como parte de las políticas de ciberseguridad (UNIR, n.d.).

Un caso destacado en Argentina en 2016 involucró la condena de un individuo por el uso de un sniffer para interceptar comunicaciones de terceros sin autorización, sentando un precedente sobre la ilegalidad de esta práctica en el país.

13. Casos de ataques utilizando Sniffers y Escaneo de puertos

13.1. Equifax

El 12 de mayo de 2017, la empresa Equifax fue víctima de un ataque que involucró sniffers: los atacantes obtuvieron acceso no autorizado a la red de la empresa (aprovechándose de una vulnerabilidad causada por una actualización del software Apache Struts) y emplearon sniffers para obtener información sensible. Si bien los desarrolladores de Apache Struts rápidamente lanzaron un parche para corregir la vulnerabilidad, Equifax no actualizó el software hasta mucho después.

Estas actividades continuaron durante 76 días hasta ser descubiertas. Además de la vulnerabilidad de Apache Struts y la lentitud en actualizar el software al próximo parche, expertos han reportado que la red interna de Equifax exhibía múltiples puntos débiles, entre los que se encontraban técnicas insuficientes de encriptación, y la ausencia de mecanismos de detección de infiltraciones.

Se estima que la información filtrada corresponde a 143 millones de ciudadanos de los Estados Unidos, que incluía: nombres, números de seguridad social, datos de tarjetas de crédito, e incluso licencias de conducir. (Wikipedia, Equifax Data Breach).

13.2. Mirai

En 2016, un malware llamado “Mirai” comenzó a expandirse por internet. Este malware en particular atacaba a dispositivos IoT (Internet of Things) como cámaras, routers, etc., con el propósito de formar una botnet: una red de dispositivos que se sincronizan para lograr un objetivo, que en el contexto de malware, suele ser un ataque de ciberseguridad. Mirai infectó aquellos dispositivos cuyas contraseñas nunca fueron cambiadas de las que vienen por defecto, y aquellos con software viejo y sin actualizar. Para detectar estos dispositivos e infectarlos, se utilizó escaneo de puertos.

La característica que destacó a Mirai fue que, una vez infectado el dispositivo, podía autorreplicarse: mientras más dispositivos infectaba, más rápido se expandía. Esta botnet se utilizó para llevar a cabo un ataque DoS (Denial of Service), que entre otras cosas, atacó a Dyn, uno de los proveedores más grandes del sistema DNS, interrumpiendo el acceso a GitHub, Twitter, Netflix, Amazon, entre otros. (Medium, Case Study on Mirai Botnet Attack).

14. Conclusión

Tanto los sniffers como el escaneo de puertos son herramientas poderosas en el campo de la administración de redes y la ciberseguridad. Su uso debe estar enmarcado en la legalidad, ya que pueden ser utilizados con fines maliciosos para interceptar comunicaciones y explotar vulnerabilidades. La detección de sniffers y la protección contra el escaneo de puertos son elementos clave en la protección de redes y sistemas. En Argentina, el uso no autorizado de estas tecnologías puede acarrear sanciones legales, subrayando la importancia de utilizarlas con el consentimiento adecuado y fines legítimos.

15. Referencias

Avast. (n.d.). ¿Qué es un sniffer de red? Cómo funcionan y cómo protegerse. Recuperado de https://www.avast.com/es-es/c-sniffer

UNIR. (n.d.). ¿Qué es un sniffer? Definición, usos y riesgos. Recuperado de https://ecuador.unir.net/actualidad-unir/que-es-sniffer-red/

Mogull, R. (2009). Understanding Port Scanning Techniques. SANS Institute InfoSec Reading Room. Recuperado de https://www.sans.org/reading-room/whitepapers/auditing/understanding-port-scanning-techniques-42

NMAP. (n.d.). Scanning Techniques. Nmap Network Scanning. Recuperado de https://nmap.org/book/man-port-scanning-techniques.html

Innovación Digital (n.d.). Ataques sniffer, qué son y cómo protegerse. Recuperado de https://www.innovaciondigital360.com/cyber-security/ataques-sniffer-que-son-y-como-protegerse/

Wikipedia. (n.d.). 2017 Equifax data breach. Recuperado de https://en.wikipedia.org/wiki/2017_Equifax_data_breach

Medium. (n.d.). A case study on Mirai Botnet Attack of 2016. Recuperado de https://medium.com/@d21dcs151/a-case-study-on-mirai-botnet-attack-of-2016-4b66630e6508