TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 3: Ataques de red comunes

Los atacantes conocen muy bien los detalles de los protocolos de internet y han creado diversas estrategias localizadas a nivel de la red de datos. Es importante recordar que, a diferencia de los paquetes en el correo postal, en donde un paquete enviado en un elemento único que no puede ser reemplazado, en internet los paquetes de datos son copiados muchas veces. Cada equipo encargado de enrutar los datos crea una copia, añade o retira información de enrutamiento y redirige el paquete al siguiente enrutador.

Teniendo en cuenta esos detalles, algunos de los ataques a nivel de red más comunes son:

IP Spoofing (suplantación de IP)

Este ataque consiste en falsificar la dirección IP de origen en los paquetes de datos, haciéndolos parecer que provienen de una fuente confiable. Los atacantes pueden usar este método para eludir filtros de seguridad o interceptar datos. Una vez se interceptan los datos, se pueden enviar respuestas falsificadas al usuario, quien puede ingresar información confidencial (nombres de usuario, contraseñas, datos privados).Para prevenir ese tipo de ataques se deben validar los certificados que el sitio remoto envía (con la clave pública y el certificado) de esta forma se determina si la ip remota es real o ha sido suplantada antes de enviar información confidencial.
También se pueden prevenir empleando datos cifrados con claves simétricas o asimétricas.

SYN Flood

Este ataque consiste en el envío de muchas solicitudes de conexión incompletas a nivel de protocolo TCP. Esto hace que el servidor consuma recursos de CPU decodificando las solicitudes, a tal punto que no queda capacidad de procesamiento para que las solicitudes legítimas puedan ser atendidas.

Man in the middle

Este ataque consiste en que un atacante intercepta y manipula las comunicaciones, haciéndole creer al cliente y al servidor que estos hablan entre sí. Usualmente sucede en redes públicas donde los datos están siendo enviados sin cifrar. Para evitar estos ataques hay que mandar la información cifrada y verificar que la clave pública pertenezca al servidor. También se puede evitar cifrando las conexiones con el uso de redes privadas virtualizadas (VPN).

Packet Sniffing.

El sniffing ocurre cuando un atacante utiliza herramientas para capturar y analizar paquetes de datos que viajan por la red. Esto puede revelar información sensible como contraseñas, datos de sesión o mensajes no cifrados. Se puede prevenir usando cifrado en la comunicación. También es posible evitarlo separando el tráfico en subredes virtuales.

Denial of Service (DoS) y Distributed Denial of Service (DDoS):

En estos ataques, el atacante sobrecarga un servidor o red con tráfico excesivo, haciendo que los servicios sean inaccesibles para los usuarios legítimos. Los ataques DDoS se realizan desde múltiples dispositivos comprometidos.

Esta categoría de ataques requiere de cierta infraestructura que permita bloquear direcciones IP que se identifiquen como atacantes y sistemas que realicen el balanceo de la carga.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

DNS Spoofing (Cache Poisoning)

En este ataque, el atacante altera las respuestas DNS para redirigir a los usuarios hacia sitios maliciosos, a pesar de que ingresaron una URL legítima. Esto puede comprometer datos sensibles como contraseñas o información financiera.

Se pueden prevenir utilizando certificados en los dominios, también se puede emplear DNSSEC para autenticar las respuestas DNS.
Otras alternativas consisten en configurar tiempos de vida (TTL) bajos en las respuestas DNS para limitar la duración del envenenamiento y monitorear y validar las configuraciones de los servidores DNS.

Ataques inalámbricos comunes

Las redes inalámbricas permiten que nuestros dispositivos se conecten fácilmente a redes de todas partes. En su casa, la red inalámbrica permite que su smartphone y sus dispositivos IoT siempre activos se conecten a Internet. La amplia disponibilidad de estas redes las convierte en el objetivo perfecto para los ciberdelincuentes. Hay muchas maneras diferentes de atacar una red inalámbrica:

- Wardriving: este término se popularizó en un par de películas de los 80. El atacante, que normalmente trabaja desde un vehículo, busca redes inalámbricas no seguras que tengan vulnerabilidades. La mayoría de los ataques de "wardriving" buscan usar la red para actividades delictivas, como la piratería de otros equipos y el robo de información personal.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira | faceIT

- Suplantación de zonas Wi-Fi: es parecido a un ataque de tipo "Man in the middle". El atacante usa su portátil o un dispositivo conectado a él para ofrecer un punto de acceso de red que imita un punto de acceso original. Por ejemplo, si está en una cafetería y quiere acceder a Internet mediante su Wi-Fi de invitado, es posible que vea un par de puntos de acceso que tienen el nombre de la cafetería. Pero puede ocurrir que uno de ellos proceda de un actor malintencionado. Una vez que se haya conectado al punto de acceso falso, todo lo que haga a través de la red se puede interceptar. También permite que el ciberdelincuente les dirija a sitios web poco seguros o capture sus datos privados.

Uso de software antivirus:

Los virus son programas maliciosos. Existen todo tipo de virus tanto para dispositivos móviles como para servidores. Con el uso de software antivirus, los servidores y los ordenadores clientes pueden validar qué cambios están haciendo los programas en su interior (en segundo plano) y bloquear aquellos que tengan comportamientos sospechosos, como el envío de grandes cantidades de datos a otros servidores, copia o manipulación no autorizada de datos, entre otros.

- Medidas de control de acceso a la red: Si bien se puede bloquear tráfico desde el firewall, se puede mejorar la seguridad bloqueando directamente a los dispositivos que no están autorizados a estar en la red. Estas soluciones también suelen controlar qué se puede hacer en las redes, por ejemplo, forzar a que el ingreso a la red sea con doble factor de autenticación, impedir la conexión con sitios en una lista de sitios inseguros, entre otras medidas que mejoran la seguridad.

- División de la red en partes: Una forma efectiva de controlar el tráfico y los ataques a una red consiste en la división de una red física en redes virtuales con numeración independiente. Este tipo de soluciones permiten restringir el acceso a cada segmento de red y evitar que dispositivos no permitidos se conecten a una subred privada o con niveles de confidencialidad más altos. Si un atacante ingresa de forma maliciosa a una subred, no podrá desplazarse horizontalmente a las otras redes para buscar incrementar el daño.

- Uso de redes privadas virtuales: Las redes virtuales privadas o VPN son una solución que cifra todos los datos a través de internet incrementando sustancialmente la seguridad en el tráfico por internet. Las redes VPN cifran cada paquete de datos y los ocultan, haciendo imposible que en internet se sepa cuál es la identidad del dispositivo remitente de los datos.
- Estas soluciones hacen que a los atacantes les sea altamente complicado falsificar paquetes, colocar ataques del tipo man in the middle y robar información. Por este motivo se recomienda que al usar redes WiFi-públicas se haga uso de VPNs.