TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

INVESTIGACIÓN 5.

SEGURIDAD Y VIRTUALIZACION

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

GRUPO: 7US

PRESENTA:

ROSA SALAZAR DOROTEO - 18620216

RUFINO MENDOZA VAZQUEZ - 21620198

ANA MICHEL LEÓN LEÓN - 21620112

FERNANDA RUIZ HERAS - 21520151

DOCENTE

ING. EDWARD OSORIO SALINA

Tlaxiaco, Oax., 09 de octubre del 2024.

"Educación, ciencia y tecnología, progreso día con día" ®

INTRODUCCION

En el mundo digital actual, los ciberataques se han vuelto cada vez más sofisticados, afectando tanto a individuos como a organizaciones. Los ataques de fuerza bruta y los ataques de denegación de servicio (DoS y DDoS) son dos de las técnicas más comunes empleadas por los atacantes para comprometer la seguridad de los sistemas. Un ataque de fuerza bruta se basa en la repetición de intentos para descifrar contraseñas o claves, mientras que los ataques de denegación de servicio buscan sobrecargar un sistema o red, haciéndolos inaccesibles para los usuarios legítimos. Estas técnicas varían en complejidad y pueden causar graves daños financieros y operativos. Para combatir estos ataques, es vital que las organizaciones implementen medidas de seguridad avanzadas, como el uso de cifrado, la autenticación de dos factores (2FA) y la protección contra DDoS.

INVESTIGA Y DESCRIBE LOS SIGUIENTES CONCEPTOS:

ATAQUE DE FUERZA BRUTA

Un ataque de fuerza bruta es un método de piratería informática que implica enviar una gran cantidad de contraseñas o combinaciones de credenciales de inicio de sesión para descubrir la contraseña correcta de una cuenta o sistemas. El objetivo es probar todas las posibles combinaciones de carácter, números y símbolos hasta encontrar la contraseña valida.

Tipos de ataques de fuerza bruta

Existen varios tipos de ataques de fuerza bruta, incluyendo;

- ✓ Credential stuffing: El atacante utiliza una lista de credenciales robados o compradas para intentar acceder a varias cuentas.
- ✓ Ataques de diccionario: El atacante utiliza un diccionario de palabras y frases para intentar descubrir la contraseña.
- ✓ Ataques de fuerza bruta inverso: El atacante comienza con una contraseña conocida y luego intenta encontrar la contraseña original.

- ✓ Ataque de password spraying: El atacante utiliza una contraseña conocida y la intenta en varias cuentas para ver si alguno de ellos es válido.

- ✓ Ataques híbridos de fuerza bruta: Los hackers mezclan medios externos con sus conjeturas lógicas para intentar una intrusión. Un ataque hibrido suele mezclar ataques de diccionario y de fuerza bruta.

Relleno de credenciales

Si un hacker tiene una combinación de nombre de usuario y contraseña que funciona en un sitio web, la probará también en muchos otros.

Dado que se sabe que los usuarios reutilizan la información de inicio de sesión en muchos sitios web, son el objetivo exclusivo de un ataque de este tipo. La combinación de la CPU y la unidad de procesamiento gráfico (GPU) acelera la potencia de cálculo. Al añadir los miles de núcleos de cálculo de la GPU para el procesamiento, el sistema puede gestionar varias tareas a la vez. El procesamiento en la GPU se utiliza para análisis, ingeniería y otras aplicaciones de cálculo intensivo. Los hackers que utilizan este método pueden descifrar contraseñas unas 250 veces más rápido que una CPU sola.

Protección pasiva de backend para contraseñas

- ✓ Tasas de cifrado elevadas: para dificultar el éxito de los ataques de fuerza bruta, los administradores de sistemas deben asegurarse de que las contraseñas de sus sistemas estén cifradas con las tasas de cifrado más elevadas posibles, como el cifrado de 256 bits. Cuanto mayor sea el número de bits en el esquema de cifrado, más difícil será descifrar la contraseña.
- ✓ Salar el hash: los administradores también deben aleatorizar los hashes de las contraseñas añadiendo una cadena aleatoria de letras y números (llamada salt) a la propia contraseña.
- ✓ Autenticación de dos factores (2FA): además, los administradores pueden exigir la autenticación en dos pasos e instalar un sistema de detección de intrusos que detecte los ataques de fuerza bruta.
- ✓ Limitar el número de reintentos de inicio de sesión: limitar el número de intentos también reduce la susceptibilidad a los ataques de fuerza bruta. Si solo se permiten, por ejemplo, tres intentos para introducir la contraseña correcta antes de bloquear al usuario durante varios minutos, se pueden causar retrasos significativos, lo que haría que los hackers apuntaran hacia un blanco más fácil.

ATAQUE DE DENEGACIÓN DE SERVICIO (DOS)

Es un tipo de ciberataque que tiene como objetivo hacer que un sitio web, aplicación web, servicio en la nube u otro recurso en línea no esté disponible para los usuarios legítimos. Los atacantes utilizan una red de sistemas comprometidos (botnet) para inundar el objetivo con tráfico malicioso, lo que consume grandes cantidades de ancho de banda de la red o inutiliza otros recursos del sistema.

CARACTERÍSTICAS

- ✓ Un ataque DDoS se caracteriza por la sobrecarga del sistema objetivo con tráfico malicioso, lo que impide que los usuarios legítimos accedan al servicio.
- ✓ Los atacantes utilizan una red de sistemas comprometidos (botnet) para generar el tráfico malicioso.

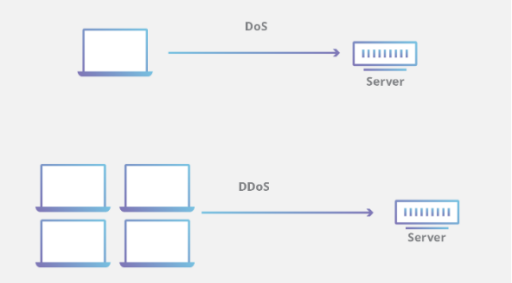
- ✓ Los objetivos comunes de un ataque DDoS incluyen sitios web, aplicaciones web, servicios en la nube y otros recursos en línea.

TECNICAS

- ✓ Inundación de tráfico HTTP o DNS: los atacantes envían una gran cantidad de solicitudes HTTP o consultas DNS al sistema objetivo, lo que consume ancho de banda y recursos del sistema.
- ✓ Paquetes falsos: los atacantes envían paquetes de red falsos al sistema objetivo, lo que consume recursos del sistema y hace que sea difícil para los usuarios legítimos acceder al servicio.
- ✓ Uso de protocolos de red: los atacantes utilizan protocolos de red como TCP o UDP para generar tráfico malicioso y sobrecargar el sistema objetivo.

EJEMPLOS

- ✓ HTTP inundations: los atacantes envían una gran cantidad de solicitudes HTTP al sistema objetivo, lo que consume ancho de banda y recursos del sistema.
- ✓ DNS consultas: los atacantes envían una gran cantidad de consultas DNS al sistema objetivo, lo que consume ancho de banda y recursos del sistema.
- ✓ Sincronización de inundaciones: los atacantes sincronizan sus ataques para generar un pico de tráfico malicioso que sobrecarga el sistema objetivo.



ATAQUE ECONOMICO DE DENEGACIÓN DE SERVICIO (EDOS)

Un ataque económico de denegación de servicio (EDos) es una variante de los ataques de denegación de servicio (Dos/DDos) que se enfoca en generar un costo económico a la víctima, en lugar de simplemente saturar la red o el sistema. En este

tipo de ataque, el objetivo es generar una gran cantidad de trafico no deseado, pero legítimo, que consuma recursos y genere costos para la víctima.

CARACTERISTICAS

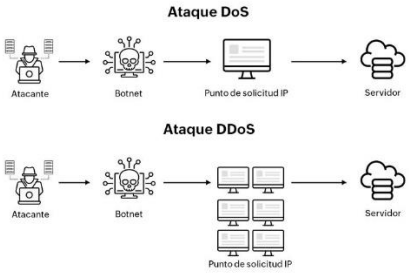
- ✓ El atacante utiliza direcciones io falsa o comprometidas para generar peticiones de servicios legitimas, pero no deseadas, hacia la víctima.
- ✓ Estas peticiones pueden ser de cualquier tipo, como consultas a base de datos, descargas de archivos o envíos de correos electrónicos.
- ✓ El objetivo es generar un volumen de trafico que sea lo suficiente alto para generar costos significativos para la víctima, como sobrecarga de servidores, aumento del ancho de banda y consumo de recursos computacionales.

EFECTOS

- ✓ La victima enfrenta un aumento sustancial en sus costos operativos, lo que puede afectar su capacidad para ofrecer servicios y generar ingresos.
- ✓ La saturación de recursos puede llevar a la perdida de conectividad, lentitud en la respuesta o incluso la paralización del servicio.
- ✓ La victima puede requerir recursos adicionales para mitigar el ataque, como servidores adicionales o capacidad de ancho de banda aumentada.

DIFERENCIA ENTRE ATAQUES Dos/DDoS

- ✓ Mientras que ataques Dos/DDoS se enfocan en saturar la rede o el sistema con trafico no deseado, un ataque económico de generación de servicio se centra en generar un costo económico a la víctima.
- ✓ Los ataques Dos/DDos suelen ser más visibles y fáciles de detectar, mientras que un Edos puede ser más difícil de detectar ya que las peticiones de servicio legitimas puede ser difíciles de distinguir de las normales.

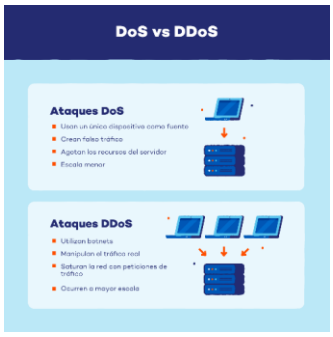


ATAQUE DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS)

Un ataque de denegación de servicios distribuidos es un tipo de ciberataque en el que un atacante utiliza múltiples fuentes de vulnerabilidad o fuentes controladas para generar un gran flujo de trafico malicioso hacia un objetivo único, como un sitio web, un servidor o un recurso de red.

CARACTERISTICAS

- ✓ Utiliza múltiples fuentes de vulnerabilidad o fuentes controladas (botnet) para generar el ataque.
- ✓ Genera un gran flujo de tráfico malicioso hacia el objetivo.
- ✓ El ataque se dirige a un punto de destino único, como un sitio web, un servidor o un recurso de red.
- ✓ El objetivo es sobrecargar el sistema objetivo, lo que impide que los usuarios legítimos accedan a los recursos o servicios.



ESTRATEGIAS DE ATAQUES

- ✓ Inundación de paquetes: El atacante envía un gran volumen de paquetes de datos hacia el objetivo, lo que consume la capacidad de procesamiento del sistema y lo hace inaccesible.
- ✓ Inundación de solicitudes: El atacante envía un gran número de solicitudes hacia el objetivo, como peticiones HTTP o consultas DNS, lo que sobrecarga el sistema y lo hace inaccesible.
- ✓ Abuso de protocolos: El atacante explota vulnerabilidades en protocolos de comunicación, como el protocolo de transferencia de hipertexto (HTTP) o el protocolo de dominio de nombre (DNS), para generar tráfico malicioso.

MEDIDAS DE PROTECCION

- ✓ Implementar soluciones de seguridad avanzadas, como cortafuegos y sistemas de detección de intrusiones.
- ✓ Utilizar servicios de protección contra DDoS, como firewall de acceso web (WAF) y redes de entrega de contenido (CDN).
- ✓ Monitorear constantemente el tráfico y las solicitudes hacia el sistema objetivo.
- ✓ Implementar técnicas de mitigación, como la reducción del tráfico y la reconfiguración de la red.
- ✓ Colaborar con proveedores de servicios y autoridades de seguridad para compartir información y coordinar esfuerzos.

TIPOS DE ATAQUES DDoS

Existen tres tipos de ataques DDos son;

- ✓ Ataques a la capa de aplicación: Los ataques a la capa de aplicación también se conocen como ataques de capa 7 porque se dirigen a la séptima capa del modelo OSI.
- ✓ Ataques a nivel de protocolo o de red: Los ataques de protocolo, también llamados ataques de capa de red, suelen tener como objetivo los niveles tres y cuatro del sistema de comunicación de una red.
- ✓ Ataques volumétricos: Los ataques volumétricos intentan saturar una red y su conexión a Internet. Los atacantes amplificarán los datos y otras peticiones de comunicación hasta un punto en el que el sistema sea incapaz de funcionar.

ATAQUE DE DENEGACIÓN DE SERVICIO POR AGOTAMIENTO DE RECURSOS

Un ataque de denegación de servicio por agotamiento de recursos (DoS) es un tipo de ataque cibernético que busca colapsar o agotar los recursos de un sistema, servicio o red, impidiendo su normal funcionamiento. El objetivo es sobrecargar el sistema objetivo con una cantidad excesiva de solicitudes o tráfico, lo que agota sus recursos y lo hace inoperante o muy lento.

TECNICAS UTILIZADAS

Entre las técnicas utilizadas para llevar a cabo este tipo de ataque se encuentran:

- ✓ Inundación: El atacante envía un gran volumen de paquetes o solicitudes al sistema objetivo, lo que lo sobrecarga y lo hace inoperante.
- ✓ Amplificación: El atacante utiliza un sistema de amplificación, como un servidor comprometido, para multiplicar el tráfico y aumentar la carga sobre el sistema objetivo.
- ✓ Agotamiento de recursos: El atacante solicita repetidamente acceso a un recurso en particular, como una base de datos o un archivo, lo que agota la capacidad del sistema para manejar solicitudes y hace que se bloquee o se ralentice.

Los ataques de denegación de servicio por agotamiento de recursos pueden tener efectos devastadores en la disponibilidad y la integridad de los sistemas y servicios afectados.

- ✓ Dificultad para acceder a los servicios: Los usuarios legítimos no pueden acceder a los servicios debido a la sobrecarga del sistema.
- ✓ Ralentización del sistema: El sistema se vuelve lento y responde con lentitud o errores.
- ✓ Error de “recurso no encontrado”: Los archivos o recursos solicitados no se encuentran disponibles debido a la sobrecarga del sistema.

ATAQUE DE DENEGACIÓN DE SERVICIO POR SATURACIÓN DE ANCHO DE BANDA

Un ataque de saturación de ancho de banda (bandwidth saturation attack) es un tipo de ataque de denegación de servicio (DDoS) en el que un atacante intenta agotar toda la capacidad de ancho de banda de una red o servidor con una cantidad masiva de tráfico malicioso. El objetivo del atacante es sobrecargar la red o el servidor, lo que impide que los usuarios legítimos puedan acceder a los servicios o recursos alojados en el mismo.

Este tipo de ataque se puede llevar a cabo de varias maneras, como por ejemplo mediante el envío de paquetes de datos de gran tamaño, el uso de paquetes mal formados o el envío masivo de peticiones HTTP. Estos ataques pueden ser difíciles de mitigar ya que el tráfico malicioso es similar al tráfico legítimo, lo que dificulta su detección y bloqueo.

Para protegerse contra los ataques de saturación de ancho de banda, se pueden implementar medidas como el uso de sistemas de detección y mitigación de DDoS, el balanceo de carga de la red, la limitación del ancho de banda para usuarios

desconocidos y la segmentación de la red para evitar que el tráfico malicioso se propague por toda la red.

CONCLUSION

Los ataques de fuerza bruta y de denegación de servicio presentan desafíos significativos para la seguridad cibernética, tanto en términos de comprometer la integridad de las credenciales como de interrumpir los servicios en línea. A medida que los atacantes se vuelven más sofisticados en sus métodos, también lo deben hacer las estrategias de protección. La combinación de soluciones técnicas, como el cifrado robusto y la mitigación de tráfico, junto con una vigilancia constante y la colaboración entre las organizaciones de seguridad, es esencial para minimizar el impacto de estos ataques. Si bien ningún sistema es completamente inmune, un enfoque proactivo y multifacético puede reducir significativamente los riesgos asociados con estos ciberataques.

BIBLIOGRAFIA

https://www.kaspersky.es/resource-center/definitions/brute-force-attack

https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

https://www.akamai.com/es/glossary/what-is-ddos

https://www.manageengine.com/latam/netflow/que-es-el-ataque-de-denegacion-de-servicios.html

https://mineryreport.com/ciberseguridad/glosario/tipos-de-amenazas/termino/ataque-saturacion-ancho-banda/