TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

Seguridad y Virtualización

Investigación practica 5

Integrantes del Equipo:

Rael Gabriel Bautista

Sandra Gabriela Velasco Guzmán

Amilkar Vladimir Reyes Reyes

Arnol Jesus Cruz Ortiz

Docente:

Ing. Edward Osorio Salinas

Carrera:

Ingeniera en Sistemas Computacionales

Grupo: 7US

Semestre: Agosto – diciembre 2024

10/ Octubre /2024

Índice

Introducción

En la actualidad, la seguridad informática se ha convertido en un aspecto crucial para la integridad y la disponibilidad de los sistemas, servicios y datos. Las ciberamenazas evolucionan constantemente, con atacantes que buscan explotar vulnerabilidades y comprometer la estabilidad de las infraestructuras tecnológicas. Entre los métodos más utilizados para perturbar servicios y sistemas se encuentran los ataques de denegación de servicio (DoS) y sus variantes. Estos ataques están diseñados para sobrecargar o interrumpir la disponibilidad de un servicio, afectando tanto a pequeñas empresas como a grandes corporaciones.

Uno de los tipos más conocidos de ataques es el ataque de fuerza bruta, el cual se basa en intentar repetidamente acceder a un sistema mediante el ensayo y error de contraseñas o claves de acceso. Si bien su objetivo es eludir mecanismos de seguridad, su impacto puede derivar en la sobrecarga de los recursos del sistema.

Por otro lado, los ataques de denegación de servicio (DoS) buscan incapacitar un servicio, ya sea saturando el ancho de banda, agotando los recursos del servidor o interfiriendo con su funcionamiento. Dentro de este ámbito, surgen variantes como el ataque de denegación de servicio distribuido (DDoS), en el cual múltiples dispositivos, a menudo comprometidos mediante redes de bots, se utilizan para lanzar un ataque coordinado que incrementa la magnitud del impacto.

Otra variante es el ataque de denegación de servicio económico (EDoS), que, aunque menos conocido, afecta financieramente a las víctimas al consumir recursos de forma continua, incrementando los costos operativos sin necesariamente colapsar el sistema.

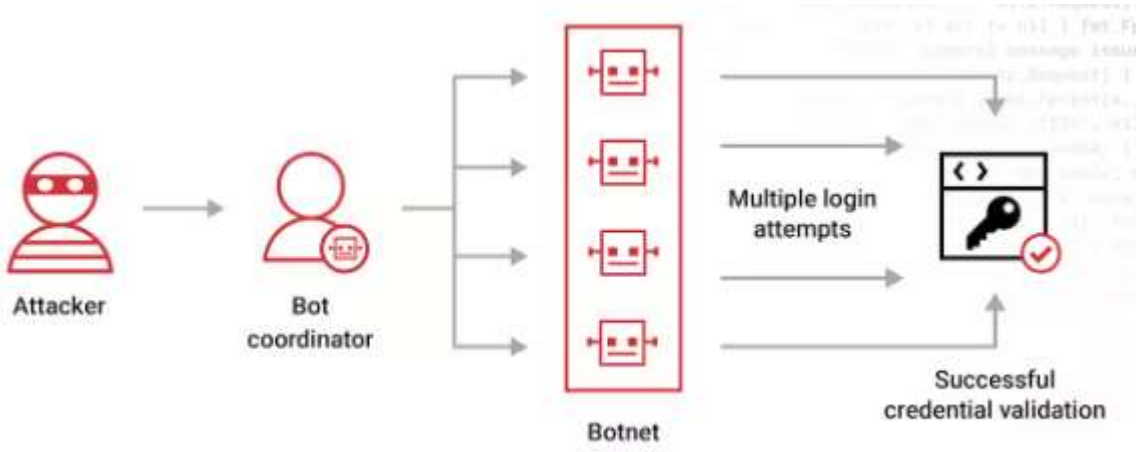
A lo largo de esta investigación se analizarán los diferentes tipos de ataques de denegación de servicio, sus características y las estrategias que se utilizan para agotamiento de recursos y saturación de ancho de banda. El objetivo es ofrecer una comprensión profunda de estas amenazas y proponer medidas preventivas y de mitigación que ayuden a mejorar la ciberseguridad de las organizaciones.

Ataque de fuerza bruta

Un ataque de fuerza bruta es un intento repetitivo y sistemático de descifrar una contraseña, clave o credencial al probar todas las combinaciones posibles hasta encontrar la correcta. Se trata de ciberataques que no requieren de una estrategia compleja, sino la aplicación del método de prueba y error, aplicando diferentes combinaciones de caracteres.

Debido a que deben realizar un gran número de intentos antes de dar con la contraseña correcta, los ciberdelincuentes usualmente crean bots o botnets para probar con una cantidad enorme de posibles contraseñas a la vez, disminuyendo así el tiempo que tardarían en lograr acceder a los datos personales o confidenciales de la víctima.

Este método de ataque usualmente es utilizado para descifrar nombre de usuario, contraseñas, claves de cifrado, claves API (siglas de Application Programming Interfaces) e inicios de sesión de SSH (siglas de Secure SHell, un programa que permite acceso remoto a un servidor por un canal seguro).



Tipos de ataques de fuerza Bruta

Credential stuffing

El credential stuffing o relleno de credenciales consiste en aprovecharse de filtraciones de contraseñas (que pueden ser compradas en la Dark Web) para rellenar los campos de acceso en múltiples plataformas hasta conseguir uno que coincida.

Este método es sumamente efectivo, incluso si el usuario utiliza una contraseña compleja, pues muchas personas utilizan la misma contraseña (que podría haber sido filtrada previamente) en múltiples cuentas a pesar de saber que esto implica una vulnerabilidad informática.

Ataques de fuerza bruta simples

Los ataques de fuerza bruta simples utilizan el método de prueba y error descrito anteriormente. Prueban combinaciones de caracteres al azar hasta descifrar las credenciales de la víctima. Suelen tener éxito si el usuario utiliza contraseñas cortas, con combinaciones de números y/o palabras fáciles de adivinar (como «12345678» o la fecha de cumpleaños de la víctima, por ejemplo).

Ataque de fuerza bruta inversa

En lugar de crear las credenciales al azar para conseguir la correcta, en este caso los ciberdelincuentes se aprovechan de bases de datos con recopilaciones de contraseñas ampliamente utilizadas que están disponibles en línea, y prueban estas contraseñas en múltiples sitios web hasta tener una coincidencia.

Ataques de fuerza bruta híbridos

Los ataques híbridos son llevados a cabo con un programa informático que utiliza lógica externa para determinar qué combinaciones de caracteres tienen más probabilidades de ser la contraseña correcta, y posteriormente prueban todas las variaciones de ese conjunto de caracteres.

Ataque de diccionario

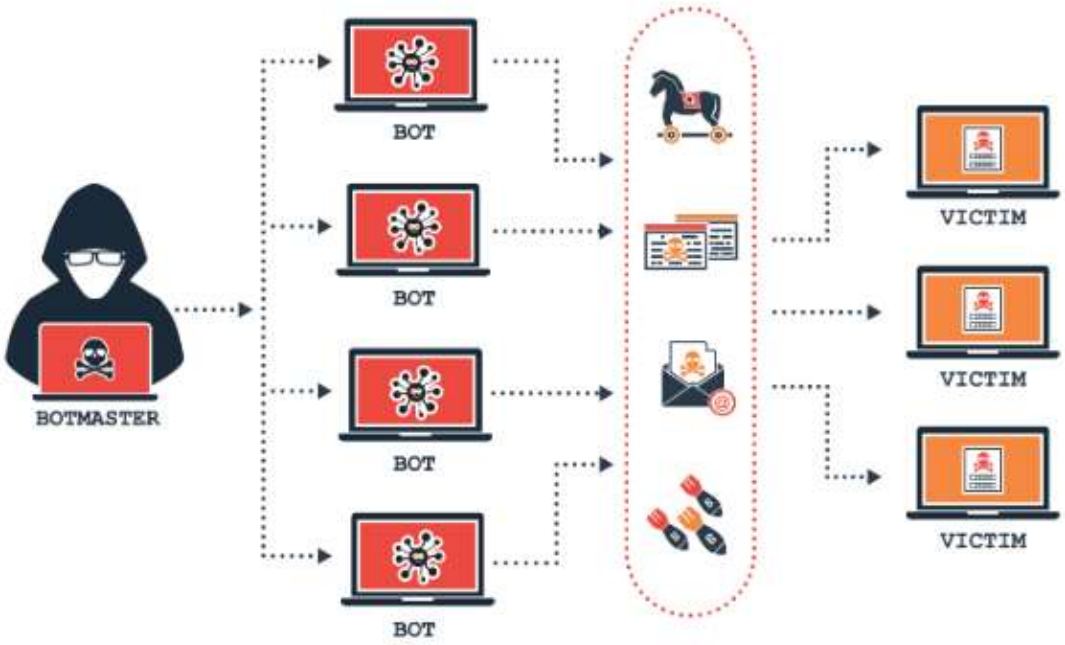
Los ataques de diccionario utilizan palabras comunes, extraídas del diccionario, y modifican algunas letras por caracteres especiales o números para el descifrado de contraseñas. Por ello, no es recomendable utilizar palabras o frases sencillas que podrían estar en un diccionario como contraseñas.

Rociado de contraseñas

Los ataques de rociado de contraseñas consisten en elegir un pequeño grupo de contraseñas comunes y llevar a cabo varios intentos de inicio de sesión en distintas cuentas de usuarios

Ataque de denegación de servicio (DoS)

Un ataque de denegación de servicio (DoS) es un ciberataque en el que los ciberdelincuentes interrumpen el servicio de un host conectado a Internet a sus usuarios previstos. Para esto envían a la red o servidor de destino una avalancha constante de tráfico, como solicitudes fraudulentas, que sobrecargan el sistema y evitan que procese el tráfico legítimo.



Tipos de ataques DoS

Existen cuatro tipos principales de ataques DoS que tienen como objetivo aprovechar o extorsionar sistemas y datos:

Redirección del navegador: Un usuario solicita que se cargue una página, pero un hacker redirige al usuario a otra página maliciosa.

Cierre de conexión: Un malintencionado cierra un puerto abierto, negando a un usuario el acceso a una base de datos.

Destrucción de datos: Un hacker elimina archivos, lo que lleva a un error de "recurso no encontrado" cuando alguien solicita ese archivo, o, si una aplicación contiene una vulnerabilidad que la deja expuesta a ataques de inyección, el malintencionado puede denegar el servicio eliminando la tabla de la base de datos.

Agotamiento de recursos: Un malintencionado solicitará repetidamente el acceso a un recurso en particular, sobrecargando la aplicación web para que se ralentice o se bloquee al volver a cargar repetidamente la página.

Prevención de ataques DoS

Los ataques DoS o DDoS pueden ocurrir en cualquier momento, pero con las mejores prácticas adecuadas, puede asegurarse de que su organización tenga todas las herramientas y protocolos necesarios para una defensa sólida.

He aquí cinco maneras de prevenir un ataque DoS:

Cree un plan de respuesta para DoS. Revise su sistema e identifique posibles fallas de seguridad, vulnerabilidades o deficiencias en la postura. Diseñe un plan de respuesta en caso de un ataque.

Proteja su infraestructura. Un firewall eficaz basado en la nube, la supervisión del tráfico y las soluciones de inteligencia de amenazas, como la detección o prevención de intrusiones, aumentan en gran medida sus posibilidades de defenderse de los ataques DoS.

Conozca las señales de advertencia. Busque un rendimiento lento de la red, tiempo de inactividad del sitio web, una interrupción o un aumento repentino del spam. Todo esto requiere de una acción inmediata.

Adopte servicios basados en la nube. Los recursos en la nube le brindan más ancho de banda que los locales, y debido a que sus servidores no están todos en las mismas ubicaciones, los atacantes tendrán más dificultades para atacarlo.

Supervise la actividad inusual. Esto permitirá a su equipo de seguridad detectar y mitigar un ataque DoS o DDoS en tiempo real. En la siguiente sección, veremos algunas formas de reducir el riesgo de ataques DoS y DDoS por completo.

Ataque economico de denegación de servicio (EDoS)

El ataque económico de denegación de servicio (EDoS) se enfoca no tanto en interrumpir el funcionamiento de un servicio, sino en generar un impacto financiero al aumentar los costos operativos de la víctima. Esto ocurre principalmente en sistemas en la nube, donde los servicios están sujetos a escalabilidad automática basada en la demanda de recursos. Los atacantes envían grandes cantidades de tráfico no legítimo, lo que obliga al proveedor de servicios a asignar más recursos (como servidores o ancho de banda) y, como resultado, incrementa los costos para el propietario del servicio.

Características principales:

- Se dirige a servicios escalables, como la computación en la nube.
- No necesariamente bloquea el servicio, sino que incrementa los costos financieros.
- Utiliza grandes cantidades de tráfico o peticiones de servicio.

Ataque de denegación de servicio distribuido (DDoS)

Un ataque DDoS tiene como objetivo deshabilitar o derribar un sitio web, aplicación web, servicio en la nube u otro recurso en línea saturándolo con solicitudes de conexión sin sentido, paquetes falsos u otro tráfico malicioso.

Un ataque DDoS (ataque de denegación distribuida del servicio) inunda sitios web con tráfico malicioso, lo que hace que las aplicaciones y otros servicios no estén disponibles para los usuarios legítimos. Incapaz de manejar el volumen de tráfico ilegítimo, el objetivo se ralentiza o falla por completo, lo que lo hace no disponible para los usuarios legítimos.

Características principales:

- Uso de múltiples dispositivos infectados (bots) para realizar el ataque.
- Saturación de los recursos de red o computacionales del servidor objetivo.
- Tráfico legítimo y malicioso pueden ser difíciles de diferenciar

Ataque de denegación de servicio por agotamiento de recursos

Este tipo de ataque se dirige a agotar recursos específicos del servidor o sistema objetivo, como la memoria, la CPU, los archivos de registro, o cualquier otro recurso esencial para su funcionamiento. A través de solicitudes repetitivas y de alto consumo de recursos, el atacante logra hacer que el servidor o dispositivo no pueda procesar más peticiones legítimas, colapsando así el servicio.

Características principales:

- Se enfoca en agotar los recursos del sistema (CPU, RAM, almacenamiento, etc.).
- Puede implicar tráfico limitado pero especialmente diseñado para consumir recursos.
- Afecta tanto la capacidad de respuesta del servidor como su estabilidad general.

Ataque de denegación de servicio por saturación de ancho de banda

Este tipo de ataque se enfoca en saturar el ancho de banda disponible de la red que conecta el sistema objetivo. El atacante inunda el enlace con más tráfico del que puede manejar, haciendo que el servidor sea inaccesible para los usuarios legítimos. A diferencia de otros ataques, que se centran en agotar los recursos del sistema, este ataque afecta directamente la capacidad de la red para manejar tráfico, bloqueando efectivamente las comunicaciones hacia y desde el servidor.

Características principales:

- El objetivo es saturar la capacidad de la red (ancho de banda) del sistema.
- Afecta tanto el servidor como la infraestructura de red (routers, switches).
- Se utiliza tráfico excesivo que supera la capacidad de procesamiento de la red.

Conclusión

Con toda la información se comprendió sobre las amenazas a las que se enfrentan los sistemas y redes en el ámbito digital actual. Desde el ataque DDoS tradicional, que utiliza múltiples dispositivos comprometidos para saturar los recursos de un sistema, hasta variantes más recientes como el EDoS, cuyo objetivo es generar un impacto financiero, los atacantes han desarrollado estrategias más elaboradas para interrumpir y colapsar los servicios.

El ataque de fuerza bruta el cual se analizó en este reporte es un método no muy complejo, pero también a vulnerado muchos sistemas informáticos por lo cual es de gran importancia el saber cómo evitarlos ya que en la actualidad se sigue usando con frueciencia por los ciberdelicuentes para descifrar contraseñas.

Cada tipo de ataque explota diferentes puntos débiles de los sistemas, ya sea agotando recursos computacionales, saturando el ancho de banda o manipulando la escalabilidad de los servicios en la nube. Esto resalta la necesidad de diseñar medidas de defensa especializadas que aborden cada tipo de amenaza de manera efectiva, como el uso de sistemas de detección de anomalías, balanceadores de carga, y redes de distribución de contenido (CDN).

Asimismo, la tendencia hacia ataques que no solo buscan derribar sistemas, sino también generar consecuencias económicas, como en el caso de los EDoS, muestra que las empresas no solo deben preocuparse por la disponibilidad de sus servicios, sino también por la eficiencia en el uso de recursos y el control de costos en entornos escalables.

La complejidad y variabilidad de los ataques DoS subraya la importancia de una estrategia de ciberseguridad integral y adaptativa, que no solo proteja los recursos tecnológicos de las organizaciones, sino que también minimice su vulnerabilidad financiera frente a estas amenazas cada vez más sofisticadas.

Referencias

Juan Santos. (2024, mayo, 6). ¿Qué es un ataque de fuerza bruta en ciberseguridad?. Delta. https://www.deltaprotect.com/blog/ataque-de-fuerza-bruta-en-ciberseguridad

IBM. ¿Qué es un ataque DDoS?. IBM Security. https://www.ibm.com/mx-es/topics/ddos

Douligeris, C., & Mitrokotsa, A. (2004). "DDoS attacks and defense mechanisms: classification and state-of-the-art". Computer Networks, 44(5), 643-666.