**EXPLOIT**

Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en un aplicación o sistema, de forma que un atacante podría usarla en su beneficio.

Existen 2 tipos:

**Conocidos:** son aquellos de lo que se tiene constancia y se deben tomar medidas para evitar nuestros sistemas

**Desconocidos (0-day):** estos se utilizan sobre vulnerabilidades que un no han sido reportadas al público en general y por esto, representa una amenaza grave, especialmente si se utilizan en empresas o gobierno.

Herramienta descargar (DVWA)

**Negación de servicio (DoS)**

Una negación de servicio (DoS) es un servicio como resultado de la falta de disponibilidad del sistema impactando a la triada CID y la consistencia.

Impide que cualquier parte de un sistema de

Esto incluye cualquier acción que cause degradación internacional, modificación o retraso del servicio.

**Objetivo:**

Un ataque de denegación de servicio (DoS) ocurre cuando los usuarios legítimos no pueden acceder a los sistemas de información, dispositivos u otros recursos de la red debido a las acciones de un actor malicioso de ciber amenazas.

**Técnicas**

Existen 2 técnicas de este tipo de ataques:

**Denegación de servicio o DoS:** se generan una cantidad masiva de peticiones al servicio desde un cliente, maquina o dirección IP, consumiendo así los recursos que ofrece el servidor hasta que llega a un momento en el que no se tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

**Denegación de servicio distribuido o DDoS:**  ocurre cuando se realizan peticiones empleando un gran número de ordenadores o direcciones IP que generan peticiones que se realizan todas al mismo tiempo y hacia el mismo servidor como objeto de ataque. Un ataque DDoS es más difícil de detectar ya que un numero de peticiones proviene desde diferentes IP’s y el administrador no puede bloquear la IP que está realizando las peticiones, como si ocurriera el ataque DoS.

**Métodos para un ataque DoS**

Existen muchos métodos de ataque para llevar a acabo un ataque DoS como un ataque más común ocurre cuando un atacante inunda la red de tráfico. En este tipo de ataque DoS, el atacante envía varias IP de destino, sobrecargándola con tráfico. Estas solicitudes… y tienen direcciones de retorno fabricadas…

**Tipos básicos de ataques DoS**

Saturación: su objetivo es agotar o saturar alguno de los recursos del sistema en los que se incluyen el tiempo de CPU, memoria, ancho de banda, discos externos, espacio en disco o alimentación de los sistemas.

Modificación de la configuración: su objetivo es altera toda la configuración del sistema o alguno de los elementos clave del sistema, típicamente servicio…

Destrucción: el resultado del ataque es la destrucción o sabotaje de todos los componentes del sistema.

Disruptivo: consisten en la interrupción de la comunicación en el sistema y el sistema de la información, haciendo inviable la transferencia de datos.

Obstrucción: este tipo de técnicas de impedir la comunicación es impidiendo que la victima se pueda comunicar de forma directa con el sistema.

**Falsificación IP (IP Spoofing)**

Se falsifica una dirección de origen en el ataque IP.

Dado que los enrutadores de red utilizan la dirección IP como parte para enrutar los paquetes en l red, el host de destino solicita la dirección IP de origen para responder al host de origen. Por lo tanto, la dirección IP de origen hace que las respuestas se desvíen. Muchos ataques a la red son el resultado de la suplantación de dirección IP.

**Inundación SYN (syn flooding)**

Se produce una inundación SYN cuando un atacante envía solicitud para conectarse al servidor de destino pero no completa la autenticación, por lo que se conoce como un protocolo de enlace de tres vías.

**UDP Flood (Saturación UDP)**

Este ataque DDoS aprovecha el protocolo UDP, un protocolo de red que no necesita una sesión iniciada o un equipo remoto. Este tipo de ataque inunda puertos aleatorios dicho host envía peligrosos paquetes UDP, causando que el equipo victima compruebe la aprobación a cada puerto, si hay alguna aplicación escuchando en destino responde como un paquete ICMP.

**ICMP Flood (Saturación por ping)**

similar al ataque de inundacion UDP, este ataque satura el recurso de destino con solicitud de paquetes “eco” ICM (conocido como ping)…

**Ataque Smurf (Smurf Attack)**

el atacante envía paquetes de difusión del protocolo de mensajes de control de internet (ICMP) a varios hosts con una dirección de protocolo de internet (IP) de origen falso que pertenece a la maquina de destino. Los destinatarios de estos paquetes falsificados responderán y el host objetivo se… esas respuestas.

**Desbordamiento de búfer (Buffer Overflow)**

Es un ataque en el que el atacante inunda un elemento de red, como un campo de dirección con más caracteres de los que se puede contener. Estos caracteres excesivos en casos maliciosos son en realidad código ejecutable, que el atacante puede ejecutar para causar estragos en el sistema, lo que efectivamente le de al atacante el control del sistema. Debido a que cualquier persona con poco conocimiento del sistema puede usar este tipo de ataque, el desbordamiento de buffer se ha convertido en una de las clases mas graves de amenazas de seguridad.

**Ping de la muerte (Ping of Death)**

Un atacante del sistema envía paquetes IP que son mas grandes que los 65.536 bytes permitidos por el protocolo IP. Muchos sistemas operativos, incluidos los sistemas operativos de red, no pueden manejar estos paquetes de gran tamaño, entonces se congelan y eventualmente se estrellan.

**Ataque Land (Land Attack)**

Es un ataque DoS land, el atacante envía un paquete falsificado TCP SYN donde las IP de origen están configurados para ser idénticos, esto hace que la maquina objetivo interno intenta responder, entra en un bucle y repetidamente envía respuestas a sí misma, lo que eventualmente hace que la maquina víctima se bloquee.

**Detección de números de secuencia**

Detección de números de secuencia, en este ataque el atacante aprovecha la previsibilidad de los números de secuencia. El atacante luego usa los números de la secuencia siguiente para establecer legitimidad.

**Botnets**

Las botnets, formadas por dispositivos comprometidos, también pueden alquilarse a otros posibles atacantes. A menudo, la botnet está disponible para servicios de ataque por alquiler, que permiten a los usuarios no calificados lanzar ataques DDoS.

DDoS permite enviar exponencialmente mas solicitudes al objetivo, por lo que aumenta el poder de ataque. También aumenta la dificultad de atribución, ya que la verdadera fuente del ataque es más difícil de identificar.

Acunetix: escáner de ataques.