Seguridad informática: principios y Práctica

Capítulo 7: Ataques de denegación de servicio

EECS710: Seguridad de la información

Profesor Hossein Saiedian

Otoño 2014

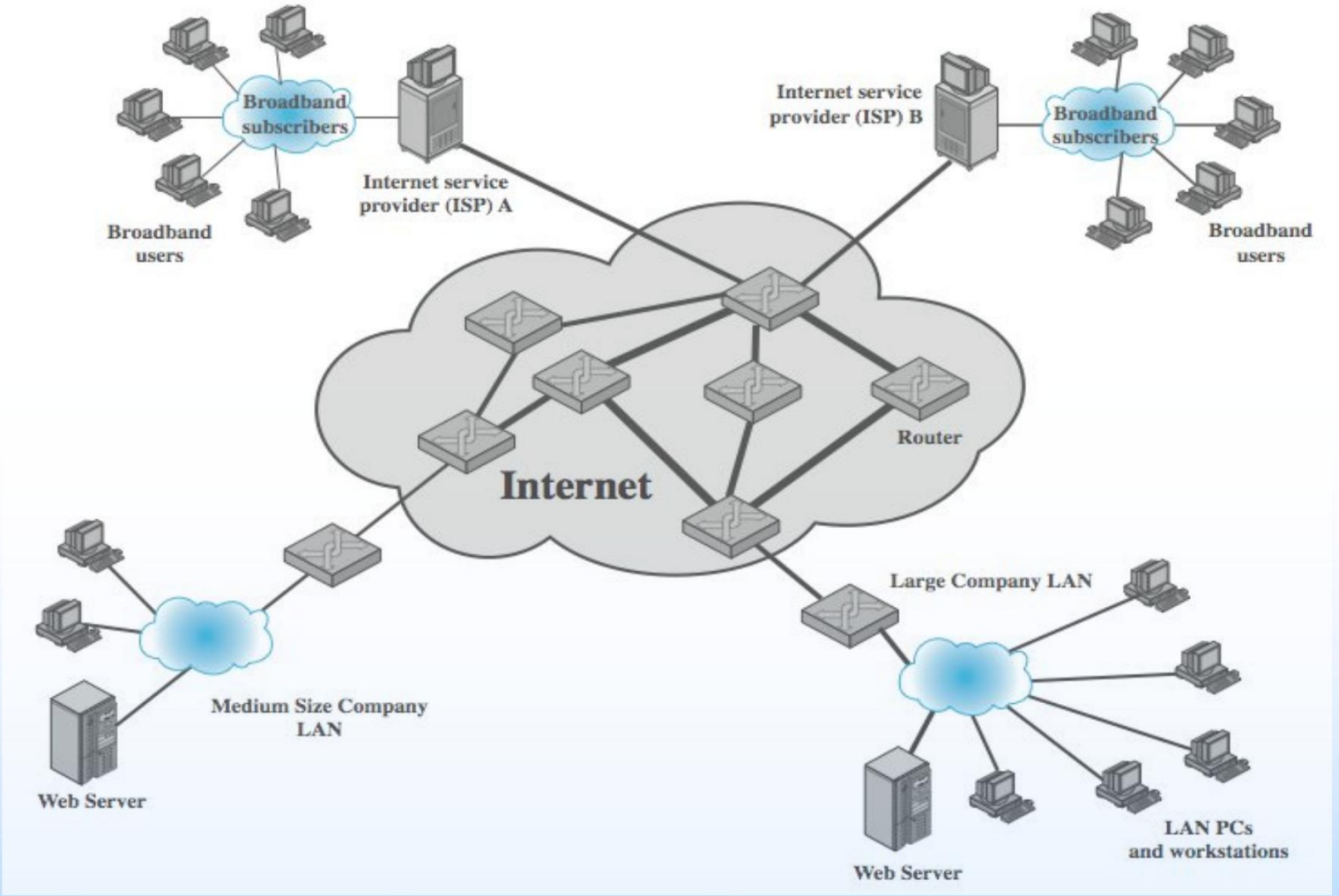
Denegación de servicio

- Denegación de servicio (DoS): una acción que impide o perjudica el uso autorizado de redes, sistemas o aplicaciones al agotar recursos como unidades centrales de procesamiento (CPU), memoria, ancho de banda y espacio en disco.
- Ataques (sobrecarga o solicitud no válida de servicios que consumen recursos significativos)
  - ancho de banda de la red
  - recursos del sistema
  - recursos de la aplicación
- Han sido un problema durante algún tiempo (25% de los encuestados Encuesta del FBI)

Ataques DoS clásicos

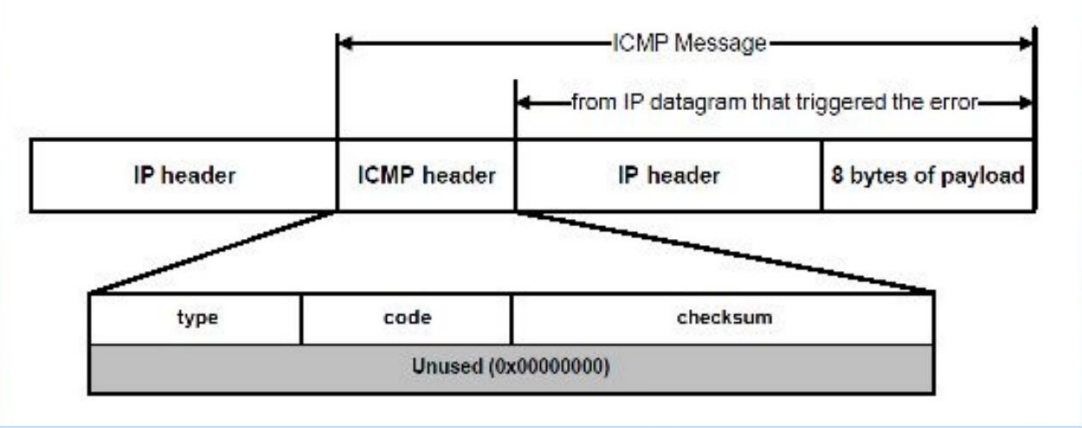
- Comando ping de inundación
  - El objetivo de este ataque es sobrepasar la capacidad de la conexión de red con la organización objetivo.
  - El tráfico puede ser manejado por enlaces de mayor capacidad en la ruta, pero los paquetes se descartan a medida que disminuye la capacidad.
- La fuente del ataque está claramente identificada a menos que se utilice una dirección falsificada
- El rendimiento de la red se ve afectado notablemente.

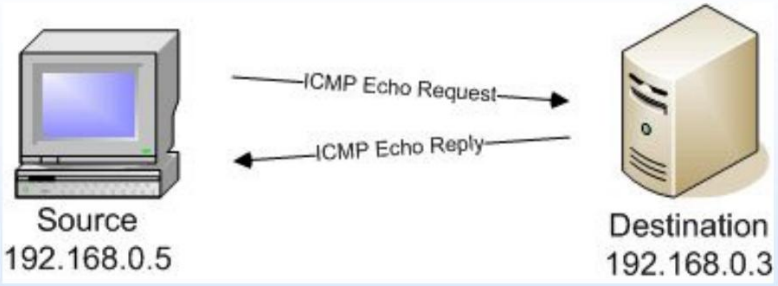
Ataques DoS clásicos



Protocolo de mensajes de control de Internet (ICMP)

- El Protocolo de mensajes de control de Internet (ICMP) es uno de los principales protocolos IP; lo utilizan los dispositivos de red, como los enrutadores, para enviar mensajes de error que indican (por ejemplo, un servicio solicitado no está disponible o no se pudo acceder a un host o enrutador)





El host debe responder a todas las solicitudes de eco con un Respuesta de eco que contiene los datos exactos recibidos en el mensaje de solicitud

Falsificación de la dirección de origen

- Utilizar direcciones de origen falsificadas
  - Generalmente a través de la interfaz de socket sin procesar en los sistemas operativos
  - Hace que los sistemas atacantes sean más difíciles de identificar
- El atacante genera grandes volúmenes de paquetes que tienen como dirección de destino el sistema de destino.
- La congestión provocaría que el enrutador conectado a El enlace final, de menor capacidad
- Tráfico de retrodispersión
  - Publicitar rutas a direcciones IP no utilizadas para monitorear ataques tráfico

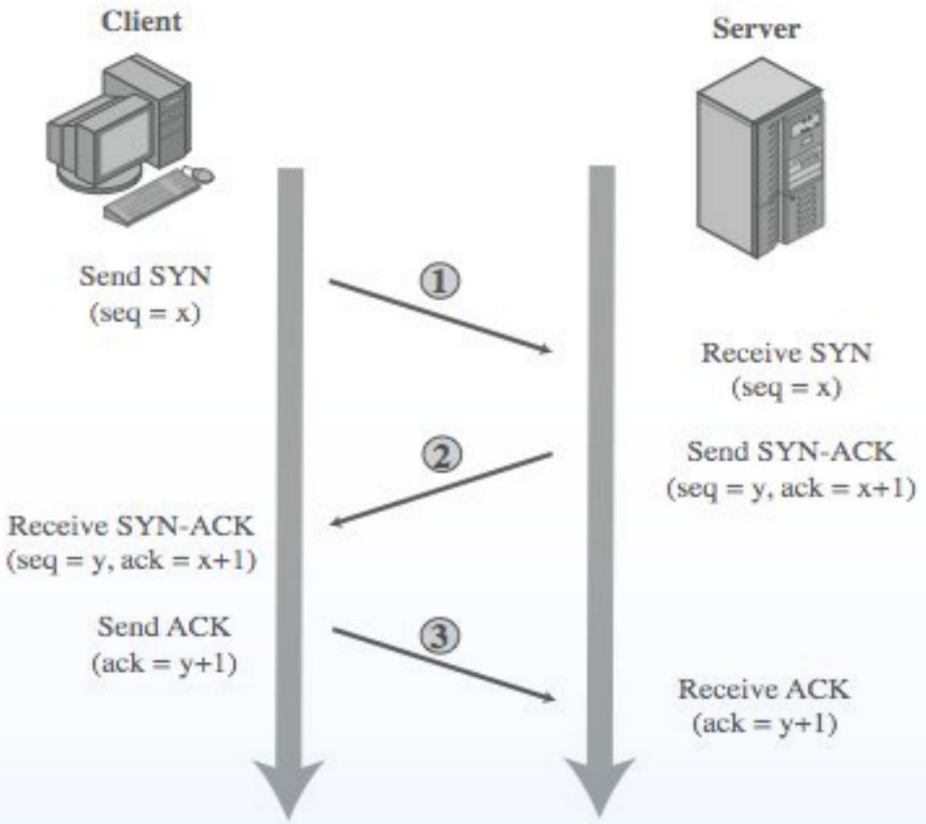
Tráfico de retrodispersión

- Los investigadores de seguridad (Proyecto Honeypot) publicitan bloques de direcciones IP no utilizadas (sin usos reales/legítimos)
- Si se realiza una solicitud ICMP/conexión, lo más probable es que provenga de atacantes
- El monitoreo proporciona información valiosa sobre el tipo y la escala del ataque.

Falsificación de SYN

- Ataque DoS común
- Ataca la capacidad de un servidor para responder a futuras solicitudes de conexión al desbordar las tablas utilizadas para administrarlas.
- De esta manera, a los usuarios legítimos se les niega el acceso a la servidor
- Por lo tanto, un ataque a los recursos del sistema, específicamente al código de manejo de red en el sistema operativo.

Protocolo de enlace de conexión TCP

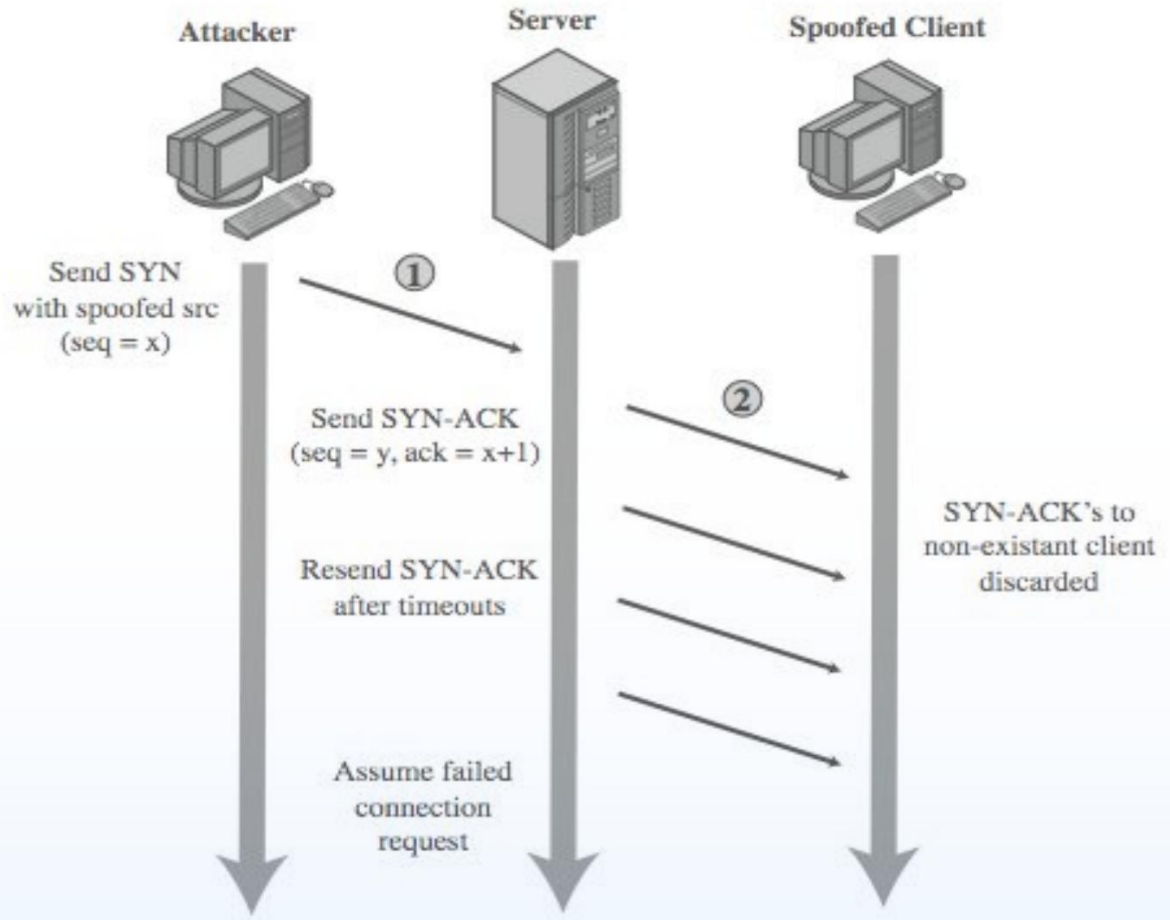


paquetes syn/ack y= n.°

de secuencia del servidor x=

n.° de secuencia del cliente

Ataque de suplantación de identidad SYN



Suposición: la mayoría de las conexiones tienen éxito y, por lo tanto, la tabla se borra rápidamente

Ataque de suplantación de identidad SYN: fuente del atacante

- El atacante a menudo utiliza direcciones

  de origen aleatorias (direcciones que pueden no existir) o las de un servidor sobrecargado (que puede no enviar un RST) para bloquear el retorno de (la mayoría de) los paquetes de reinicio.

- Tiene un volumen de tráfico mucho menor

  – el atacante puede estar en un enlace de capacidad

mucho menor • Objetivo: utiliza direcciones que no responderán al SYN-ACK con un RST

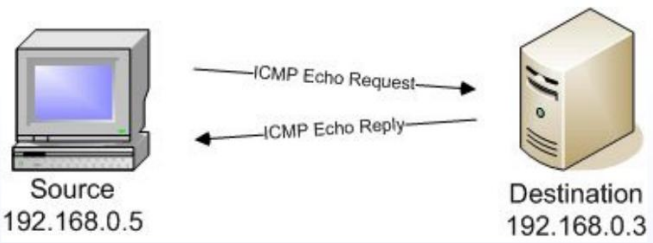
Tipos de ataques de inundaciones

• Clasificado según el protocolo de red utilizado • Objetivo: sobrecargar

la capacidad de red en algún enlace a un servidor • Se puede utilizar prácticamente cualquier tipo de

paquete de red • Inundación ICMP

– Utiliza paquetes ICMP, por ejemplo, solicitud de ping (eco)
– Generalmente se permite el paso, algunos son necesarios



• Inundación UDP

– La alternativa utiliza paquetes UDP a puertos aleatorios (incluso si no hay servicio disponible, el atacante logra su objetivo)

• Inundación SYN de TCP (suplantación SYN frente a inundación SYN)

– Envía paquetes TCP SYN (solicitud de conexión)
– Pero para el ataque de volumen

Paquete UDP

- El Protocolo de datagramas de usuario (UDP) es un componente del conjunto IP y permite que las aplicaciones informáticas envíen mensajes
- Un UDP puede dirigirse prácticamente a cualquier servicio (puerto); si el servicio no está disponible, el paquete se descarta pero se logra el objetivo del atacante.

Offset (bits)	Field
0	Source Port Number
16	Destination Port Number
32	Length
48	Checksum
64+	Data ⋮

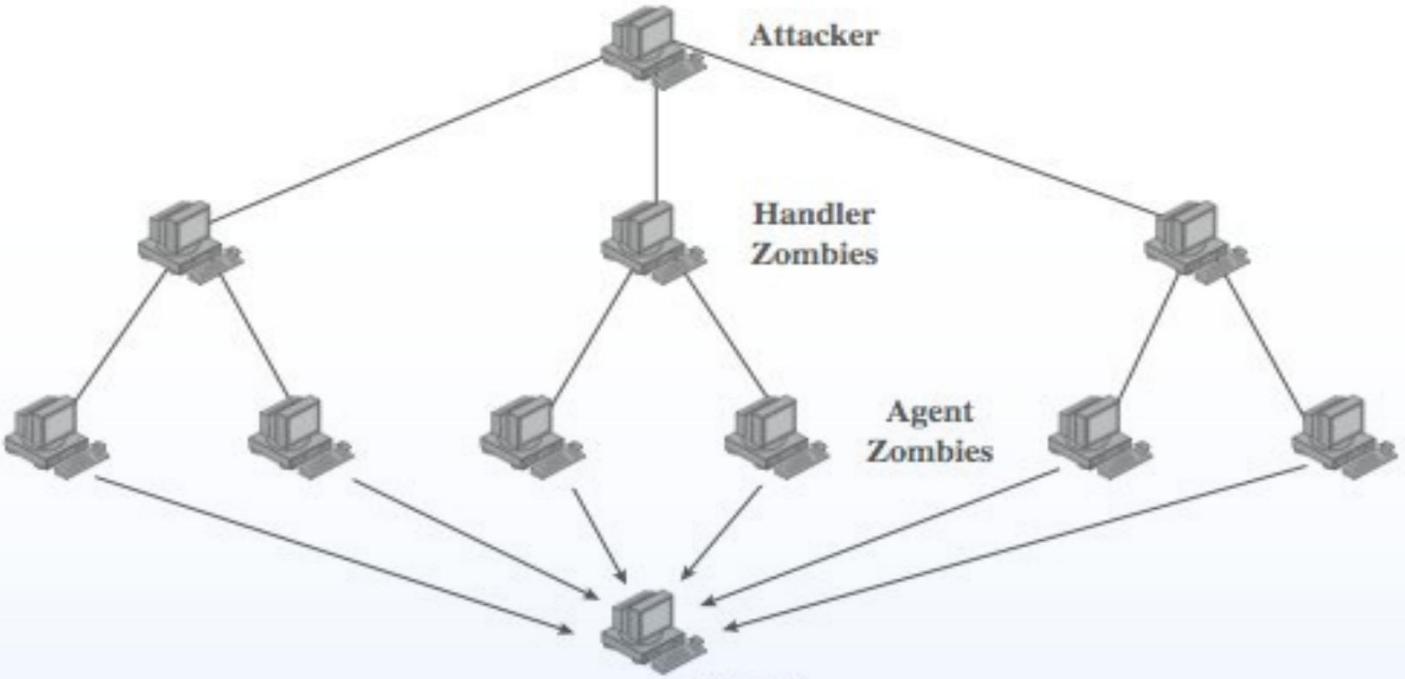
Ataques DoS distribuidos

- Tienen un volumen limitado si se utiliza una sola fuente
- Múltiples sistemas permiten que volúmenes de tráfico mucho mayores formen un ataque DoS distribuido (DDoS)
- PC/estaciones de trabajo a menudo comprometidas
  - Zombies con programas de puerta trasera instalados
  - Formación de una

botnet • Ejemplo: Tribe Flood Network (TFN), TFN2K – realizó inundaciones ICMP, SYN, UDPF e ICMP

Jerarquía de control de DDoS

El atacante envía un comando al controlador de zombies; el controlador lo reenvía a otros controladores, agentes.

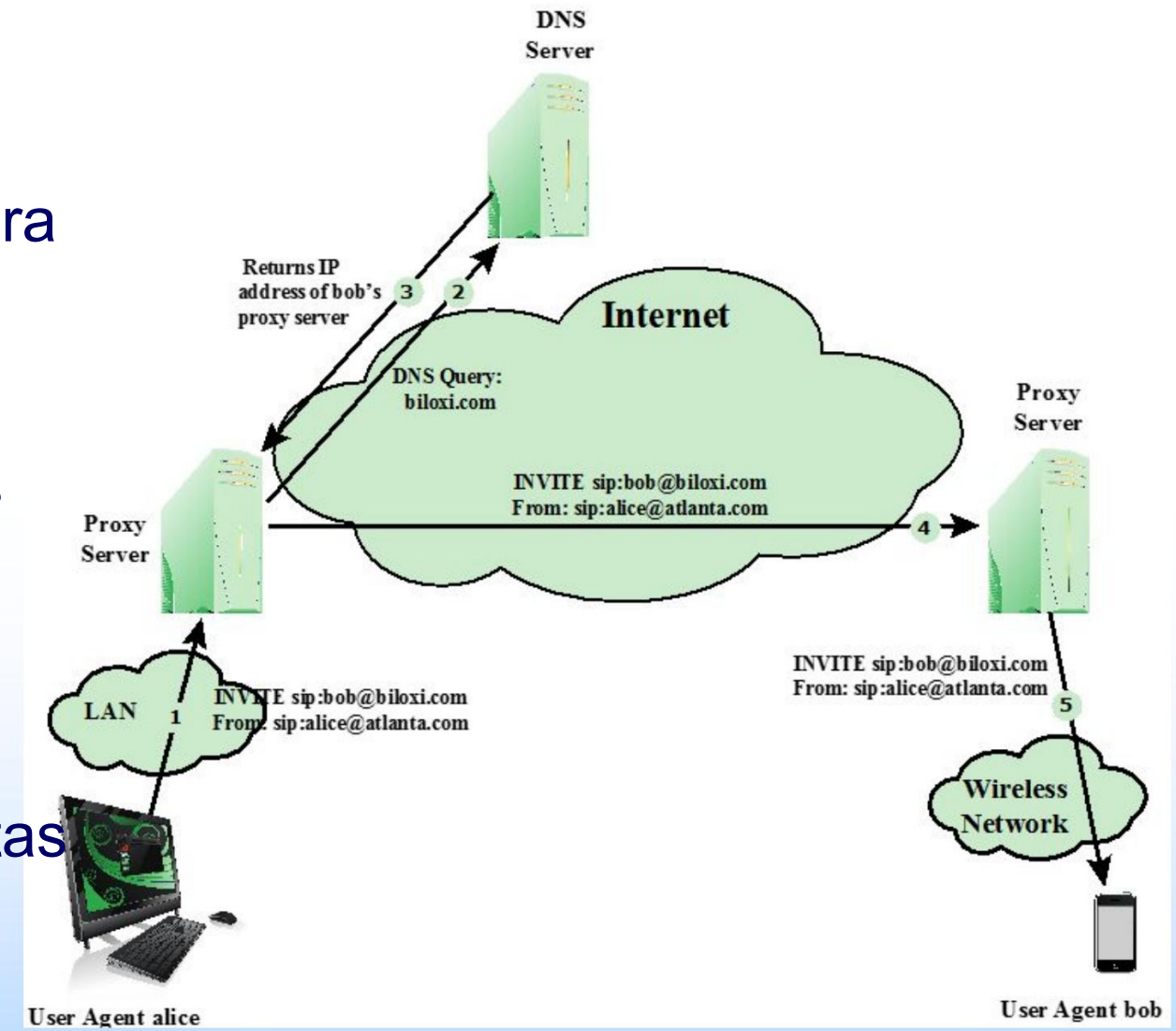


Ataques de ancho de banda basados en aplicaciones

- Obligar al sistema víctima a ejecutar operaciones que consumen recursos (por ejemplo, búsquedas, consultas complejas a bases de datos)
- Inundación del Protocolo de inicio de sesión de VoIP (SIP) (ver Figura 7.5): el atacante envía muchas solicitudes INVITE; gran carga para los servidores proxy
  - los recursos del servidor se agotaron mientras se procesaban las solicitudes
  - se consume la capacidad de ancho de banda

Invitación SIP guión

- Protocolo estándar para Telefonía VoIP
- Protocolo basado en texto con una sintaxis similar a la de HTTP
- Dos tipos de mensajes SIP: solicitudes y respuestas



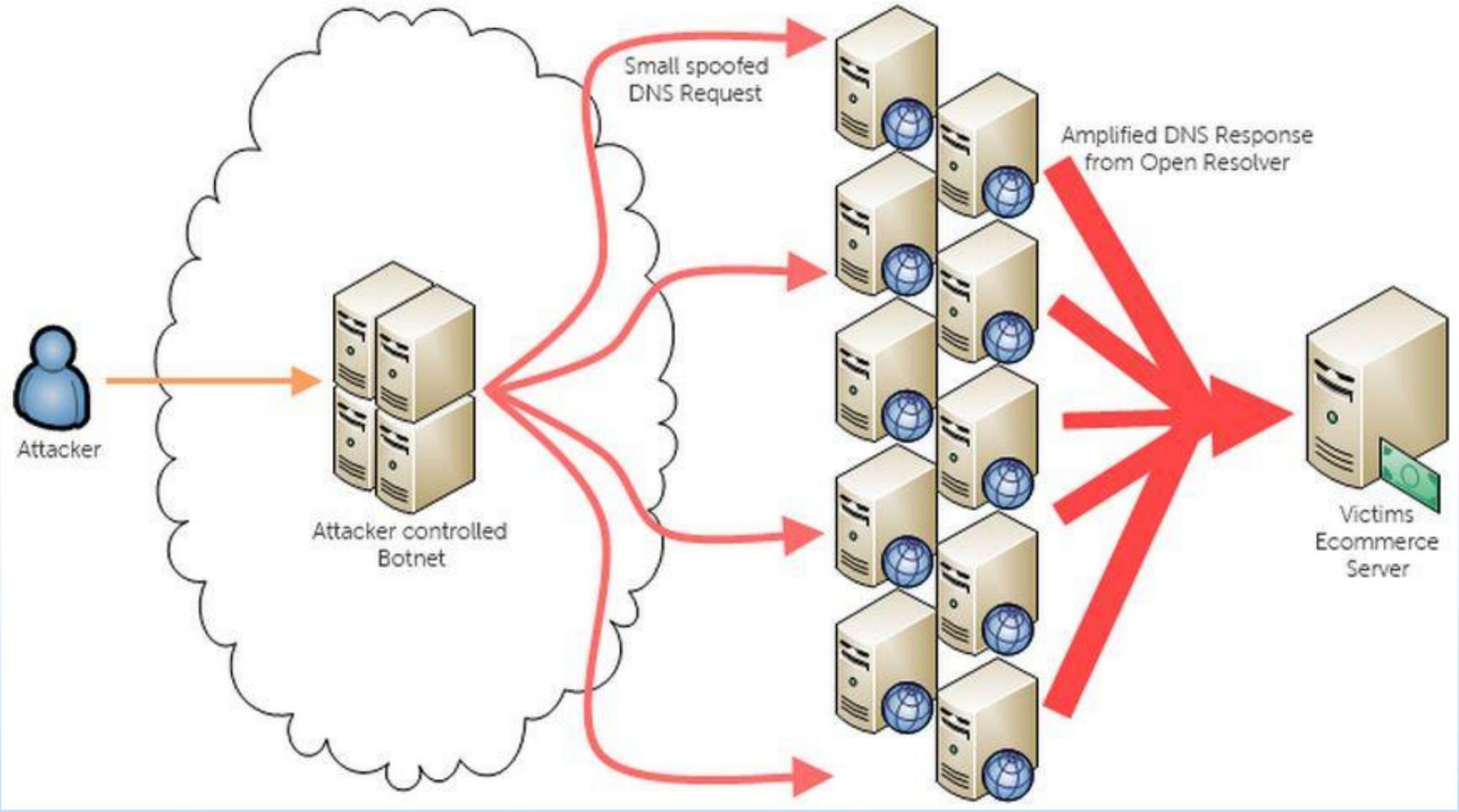
Ataques basados en HTTP

- Intentos de monopolio mediante el envío de solicitudes HTTP que nunca se completan
- Eventualmente consume la capacidad de conexión del servidor web.
- Utiliza tráfico HTTP legítimo
- Spidering: Bots que parten de un enlace HTTP determinado y siguen todos los enlaces en el sitio web proporcionado de forma recursiva
- Soluciones existentes de detección y prevención de intrusiones que dependen de firmas para detectar ataques generalmente no reconocerán Slowloris

Ataques de reflexión

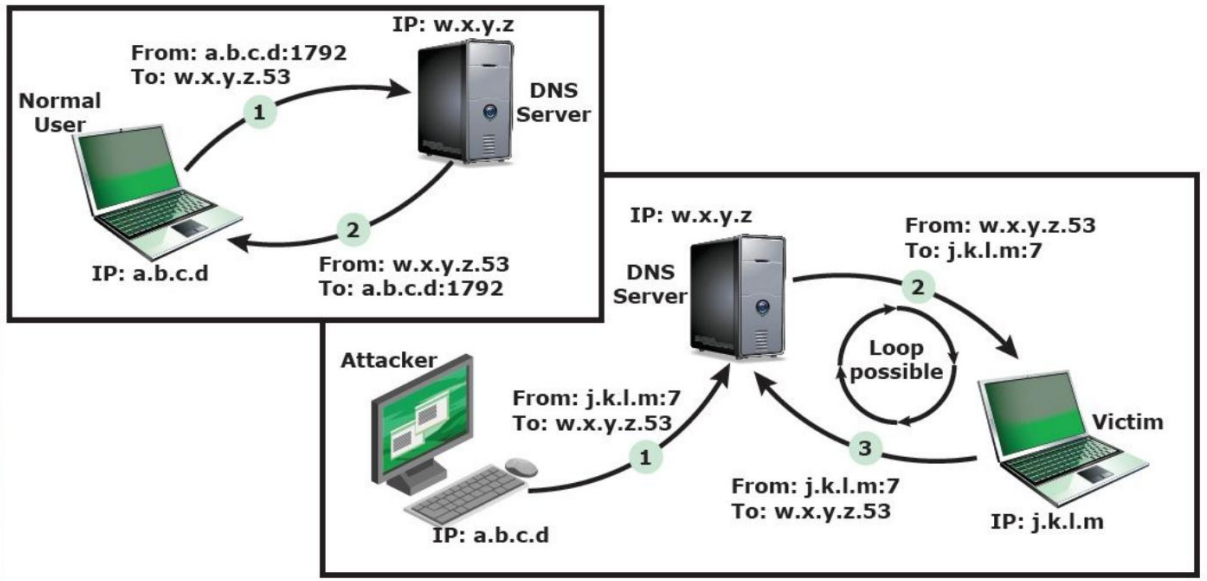
- El atacante envía paquetes a un servicio conocido en el intermediario con una dirección de origen falsificada del sistema de destino real.
- Cuando el intermediario responde, la respuesta se envía al objetivo
- "Refleja" el ataque del intermediario (reflector)
- El objetivo es generar suficientes volúmenes de paquetes para inundar el enlace al sistema de destino sin alertar al intermediario.
- La defensa básica contra estos ataques es bloquear los paquetes de origen falsificado.

Ataques de reflexión

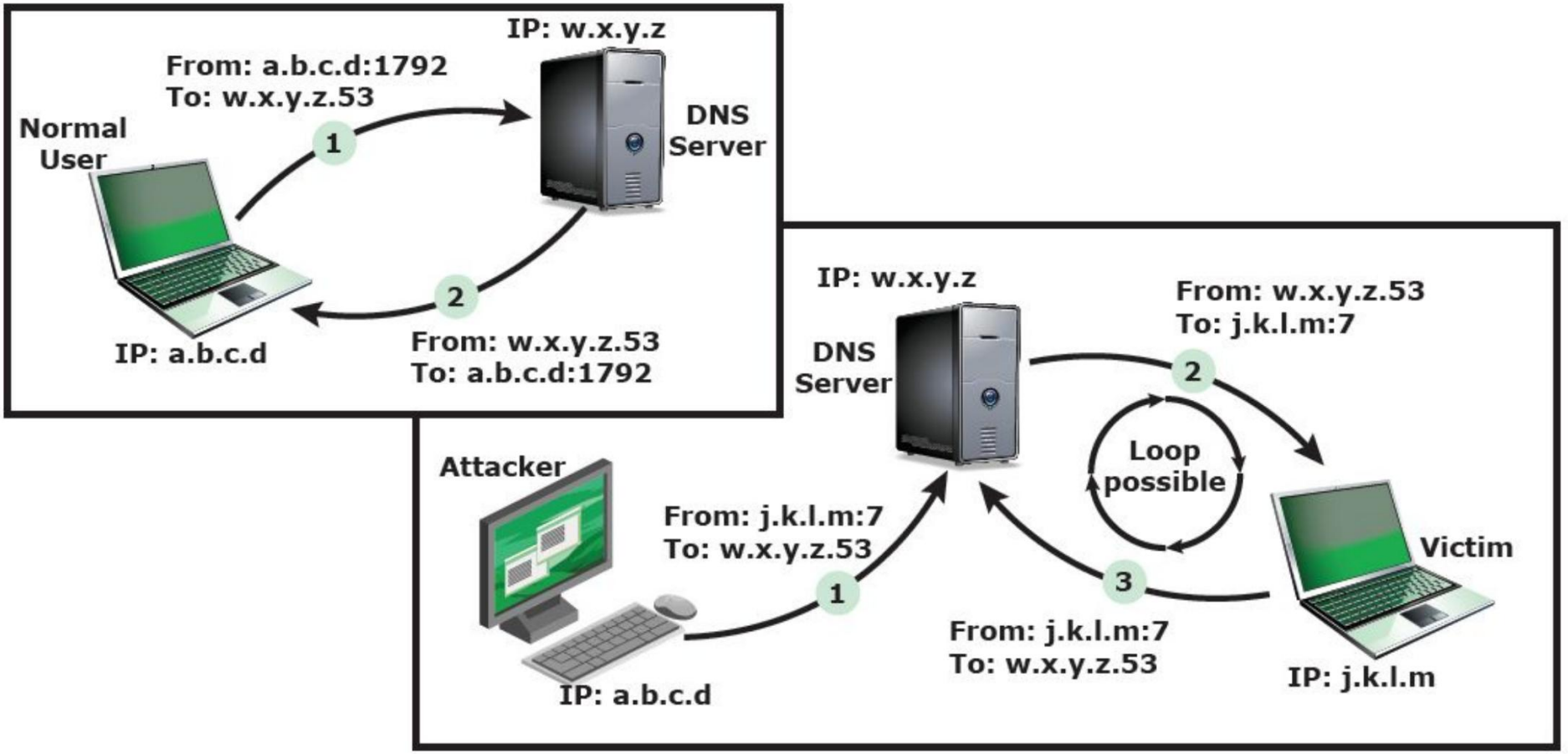


Ataques de reflexión

- Una mayor variación crea un bucle autónomo. entre el intermediario y el objetivo (el atacante falsifica el puerto 7 y requiere ecos)
- Bastante fácil de filtrar y bloquear.



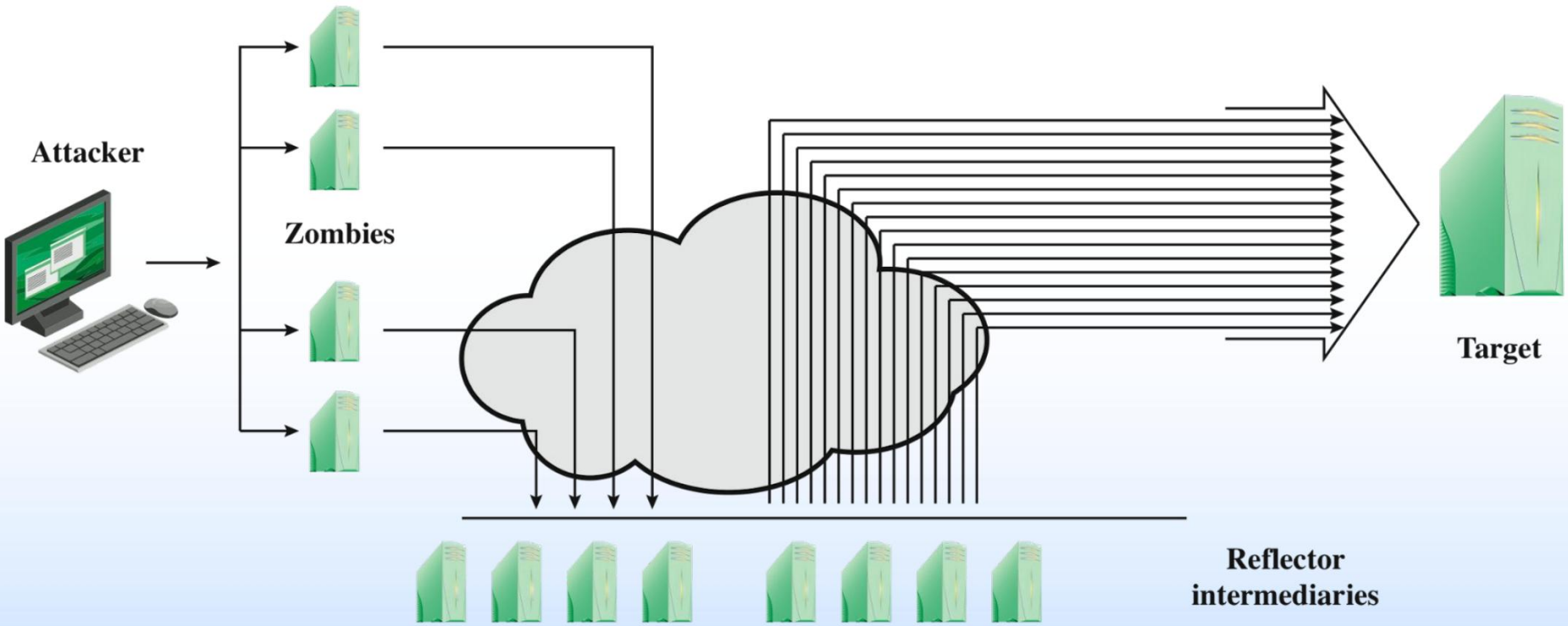
Ataques de reflexión de DNS



Ataques de amplificación de DNS

- Utilizar paquetes dirigidos a un servidor DNS legítimo como sistema intermediario
- El atacante crea una serie de solicitudes DNS que contienen la dirección de origen falsificada del sistema de destino.
- Aprovechar el comportamiento de DNS para convertir una pequeña solicitud en una Respuesta mucho mayor (amplificación)
- El objetivo está inundado de respuestas.
- La defensa básica contra este ataque es evitar el uso de direcciones de origen falsificadas.

Ataques de amplificación



Puede aprovechar la dirección de transmisión de alguna red

Cuatro líneas de defensa contra ataques DDoS

- Prevención y preeminencia de ataques (antes del ataque)
- Detección y filtrado de ataques (durante el ataque)
- Rastreo e identificación de la fuente del ataque (durante y después del ataque)
- Reacción al ataque (después del ataque)

Prevención de ataques DoS

- Bloquear direcciones de origen falsificadas
  - En enrutadores lo más cercanos posible a la fuente
- Se pueden utilizar filtros para garantizar la ruta de regreso al destino reclamado.
  La dirección de origen es la que utiliza el paquete actual.
  - Se deben aplicar filtros al tráfico antes de que salga de la red del ISP o en el punto de entrada a su red
- Utilice código de manejo de conexión TCP modificado
  - Codificar criptográficamente información crítica en una cookie que se envía como número de secuencia inicial del servidor
  - El cliente legítimo responde con un paquete ACK que contiene la cookie con el número de secuencia incrementado
  - Eliminar una entrada para una conexión incompleta de la tabla de conexiones TCP cuando se desborda

Prevención de ataques

- Controles de tarifas en redes de distribución ascendentes
  - En tipos de paquetes específicos, por ejemplo, algunos ICMP, algunos UDP, TCP/Sincronización
  - Imponer límites
- Utilizar un manejo de conexión TCP modificado
  - El servidor envía cookies SYN cuando la tabla está llena (reconstruye los datos de la tabla a partir de la cookie de los clientes legítimos)
  - Sr. Eliminación selectiva o aleatoria cuando la tabla está llena

Prevención de ataques

- Bloquear transmisiones dirigidas por IP
- Bloquear servicios y combinaciones sospechosas
- Gestionar ataques a aplicaciones con una especie de rompecabezas gráfico (captcha) para distinguir solicitudes humanas legítimas
- Utilice servidores reflejados y replicados cuando
  Se requiere alto rendimiento y confiabilidad

Respondiendo a los ataques

- Buen plan de respuesta a incidencias
  - Detalles sobre cómo contactar al personal técnico del ISP
  - Necesario imponer filtrado de tráfico en sentido ascendente
  - Detalles de cómo responder al ataque
- Implementar filtros anti-spoofing, de transmisión dirigida y de limitación de velocidad.
- Lo ideal es contar con monitores de red e IDS para detectar y notificar patrones de tráfico anormales.

Respondiendo a los ataques

- Identificar el tipo de ataque
  - Capturar y analizar paquetes
  - Diseñar filtros para bloquear el tráfico de ataques ascendentes
  - O identificar y corregir errores del sistema/aplicación •

Hacer que el ISP rastree el flujo de paquetes hasta la fuente

  - Puede ser difícil y llevar mucho tiempo.
  - Necesario si se planea emprender acciones legales

- Implementar plan de contingencia
  - Cambiar a servidores de respaldo alternativos
  - Poner en servicio nuevos servidores en un nuevo sitio con nuevas direcciones

- Actualizar el plan de respuesta a incidentes

Resumen

• Ataques de denegación de servicio (DoS) introducidos • Ataques clásicos de inundación y suplantación de SYN • Inundaciones de SYN ICMP, UDP y TCP • Ataques de denegación de servicio distribuido (DDoS) • Ataques de reflexión y amplificación

• Defensas contra ataques DoS • Respuesta a ataques DoS