17. Evadiendo IDS, Firewalls y Honeypots

Julio Javier Iglesias Pérez

Sistema de Detección de Intrusos

Un Sistema de Detección de Intrusos (IDS) obtiene información de entre un equipo o una red, para identificarlas violaciones posibles de la política de seguridad, incluyendo acceso no autorizado, así como su mal uso. Un IDS es también referido como un "packet-sniffer" que intercepta paquetes viajando a lo largo de varios medios de comunicación y protocolos, generalmente TCP/IP. Los paquetes son analizados luego de que son capturados. Un IDS evalúa una sospecha de intrusión una vez que toma lugar y señala una alarma.

Maneras de detectar una intrusión

Existen tres maneras de detectar una intrusión:

- Reconocimiento de firma: También conocido como detección de mal uso. Intenta identificar eventos que usen mal un sistema.
- Detección de anomalía: Detecta la intrusión basada en características de comportamiento fijas de los usuarios y componentes en un sistema de cómputo.
- Detección de anomalía de protocolo: En este tipo de detección, los modelos son construidos en protocolos TCP/IP utilizando sus especificaciones.

Tipos de IDS

- Basado en Red: Mecanismos que típicamente consiste en una caja negra que es colocada en una red en modo promiscuo, escuchando patrones indicativos de una intrusión.
- Basado en host: Usualmente incluye auditoría para eventos que ocurren en un host específico. No son tan comunes, debido a la sobrecarga que incurren al tener que monitorear cada evento del sistema.

Tipos de IDS

- Monitoreando archivos de registro (Log): Estos mecanismos son programas que típicamente analizan archivos de registro luego de que un evento ha ocurrido, como intento de inicios de sesión fallidos.
- Revisión de integridad de archivo: Estos mecanismos revisan caballos de troya, o archivos que han sido modificados de otra manera, indicando que un intruso ya estuvo ahí. Ejemplo: Tripwire

Sistemas Verificadores de Integridad (SIV)

Tripwire es un SIV que monitorea archivos del sistema y detecta cambios realizados por un intruso.

Indicadores Generales de Intrusiones

- Intrusiones de Sistema de Archivos: La presencia de nuevos, archivos no familiares o programas. Cambio de extensión de los archivos. Cambios inexplicados en el tamaño de los archivos. Archivos pícaros en el sistema que no corresponden a la lista maestra de archivos firmados. Nombres de archivos no familiares en los directorios. Archivos perdidos.

Indicadores Generales de Intrusiones

- Intrusiones de red: Sondas repetidas de servicios disponibles en los equipos. Conexiones desde localidades poco usuales. Registros repetidos de intentos desde hosts remotos. Dato arbitrario en los archivos de registro, indicando un intento de crear un DoS o bloquear los servicios.

Indicaciones Generales de Intrusiones al sistema

- Modificaciones al software del sistema y archivos de configuración.
- Lagunas en las cuentas del sistema.
- Rendimiento lento poco usual en el sistema.
- Bloqueo del sistema o reinicio.
- Logs incompletos o cortos.
- Registros perdidos o con permisos incorrectos.
- Procesos no familiares.
- Gráficos o mensajes de texto inusuales.

Firewall

Software o hardware o una combinación de ambos diseñado para impedir acceso no autorizado a la red privada. Es colocado en un punto de unión o puerta de enlace entre dos redes, que usualmente es una red privada y una pública (internet).Examina todos los mensajes que entran o salen de la intranet y bloquea aquellos que no cumplen criterios específicos de seguridad. Pueden ser afectados por el tipo de tráfico o por la fuente o direcciones destino y puertos.

Arquitectura del Firewall

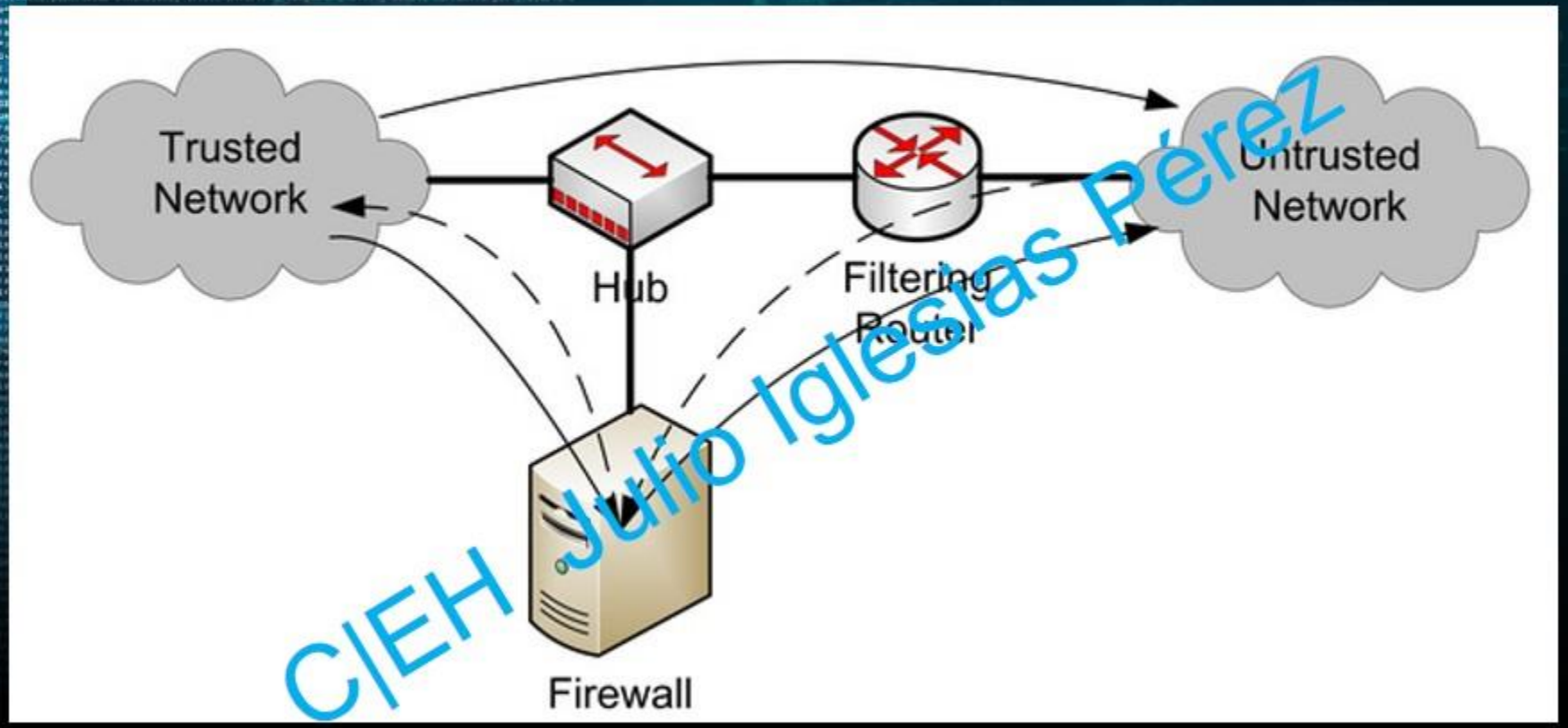
Host Bastión: Es un sistema de cómputo diseñado para proteger los recursos de la red de un ataque.

El tráfico de entrada o salida de la red, pasa por el firewall.

Tiene dos interfaces:

- Interfaz privada, conectada directamente a Internet
- Interfaz pública, conectada a la intranet.

Arquitectura del Firewall



Screened subnet

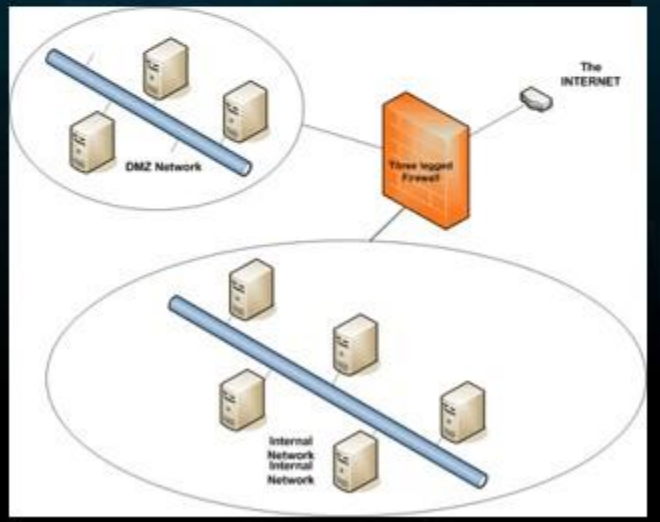
O DMZ contiene hosts que ofrecen servicios públicos.

La zona pública está conectada directamente a Internet y no tiene hosts controlador por la organización.

La zona privada tiene sistemas que los usuarios de internet no tienen acceso de negocio.

Zona desmilitarizada

- Es una red que sirve como buffer (regulador) entre la red interna segura y la insegura Internet.
- Es creada utilizando firewall entre tres o más interfaces de red asignada con roles específicos como Red Interna confiada, red DMZ y la red externa.



Tipos de firewall

- Filtro de paquetes.
- Firewall de inspección de estado multicapa.
- Puertas de enlaces a nivel de aplicación.
- Puertas de enlaces a nivel de circuito.

Filtrado de paquetes Firewall

Trabaja en la capa red del modelo OSI (o capa IP de TCP/IP), usualmente son parte de un router.

Cada paquete es comparado con un conjunto de criterios antes de ser renviado.

Dependiendo del paquete y del criterio, el firewall puede:

- Dropear el paquete.
- Renviarlo, o enviar un mensaje al que lo originó.

Las reglas pueden incluir la dirección IP fuente y destino, el número de puerto fuente y destino, y el protocolo utilizado.

Firewall de puerta de enlace a nivel de circuito

- Trabajan en la capa de sesión del modelo OSI o en la capa TCP de TCP/IP.
- Monitorean el handshaking TCP entre paquetes para determinar si la sesión solicitada es legítima.
- La información es pasada a un equipo remoto a través de una puerta de enlace a nivel de circuito.
- Estos gateways esconden la información acerca de las redes que ellos protegen, pero no filtran paquetes individuales.

Firewall a nivel de aplicación

O proxis, pueden filtrar paquetes en la capa aplicación del modelo OSI.

Los paquetes de entrada o salida no pueden acceder a servicios si es que no hay proxy.

Un gateway configurado para ser proxy no permitirá ningún tráfico FTP, gopher, telnet o cualquier otro.

Como esta aplicación examina paquetes en la capa aplicación, puede filtrar comandos de aplicación específicos como http:post y get.

Firewall de inspección multicapa Stateful

- Combina los aspectos de los otros tres tipos de firewall.
- Filtran los paquetes en la capa red para determinar si los paquetes de la sesión son legítimos y evalúan el contenido de los paquetes en la capa de aplicación.

El tráfico es filtrado en tres capas basado en el rango de una aplicación específica, sesión y reglas de filtrado de paquetes.

Identificación de Firewall: Escaneo de puertos

- Ayuda al atacante a encontrar que puertos están disponibles, consiste en enviar mensajes a cada puerto, uno por vez.
- Algunos firewalls serán identificados únicamente utilizando un simple escaneo de puertos.
- El tipo de respuesta recibida indican si el puerto está en uso y por ende puede probar fortaleza o debilidad.

Identificación de Firewall: Firewalking

- Es una técnica de pruebas de vulnerabilidad de un firewall y mapeo de routers de una red que se encuentra detrás del firewall.
- Si el paquete pasa por el gateway, es renviado al próximo salto donde el TTL iguala a cero y elige un mensaje TTL "excedido en tránsito", en este punto el paquete es descartado.

Identificación de Firewall: Firewalking

- Firewalking es similar al tracerounting y trabaja enviando paquetes TCP y UDP dentro del firewall que tienen un TTL configurado en un salto más grande que el firewall apuntado.
- Utilizando este método, el acceso a la información en el firewall puede ser determinado si paquetes de sondeo sucesivos son enviados.

Identificación de Firewall: Banner Grabbing

Los banners son mensajes enviados por los servicios de red mientras están conectado al servicio que anuncian la ejecución de un servicio en el sistema.

Banner grabbing es un método simple de detección de S.O. que ayuda a detectar servicios ejecutados por firewall.

Los tres servicios principales enviados son FTP, telnet y Servidores Web.

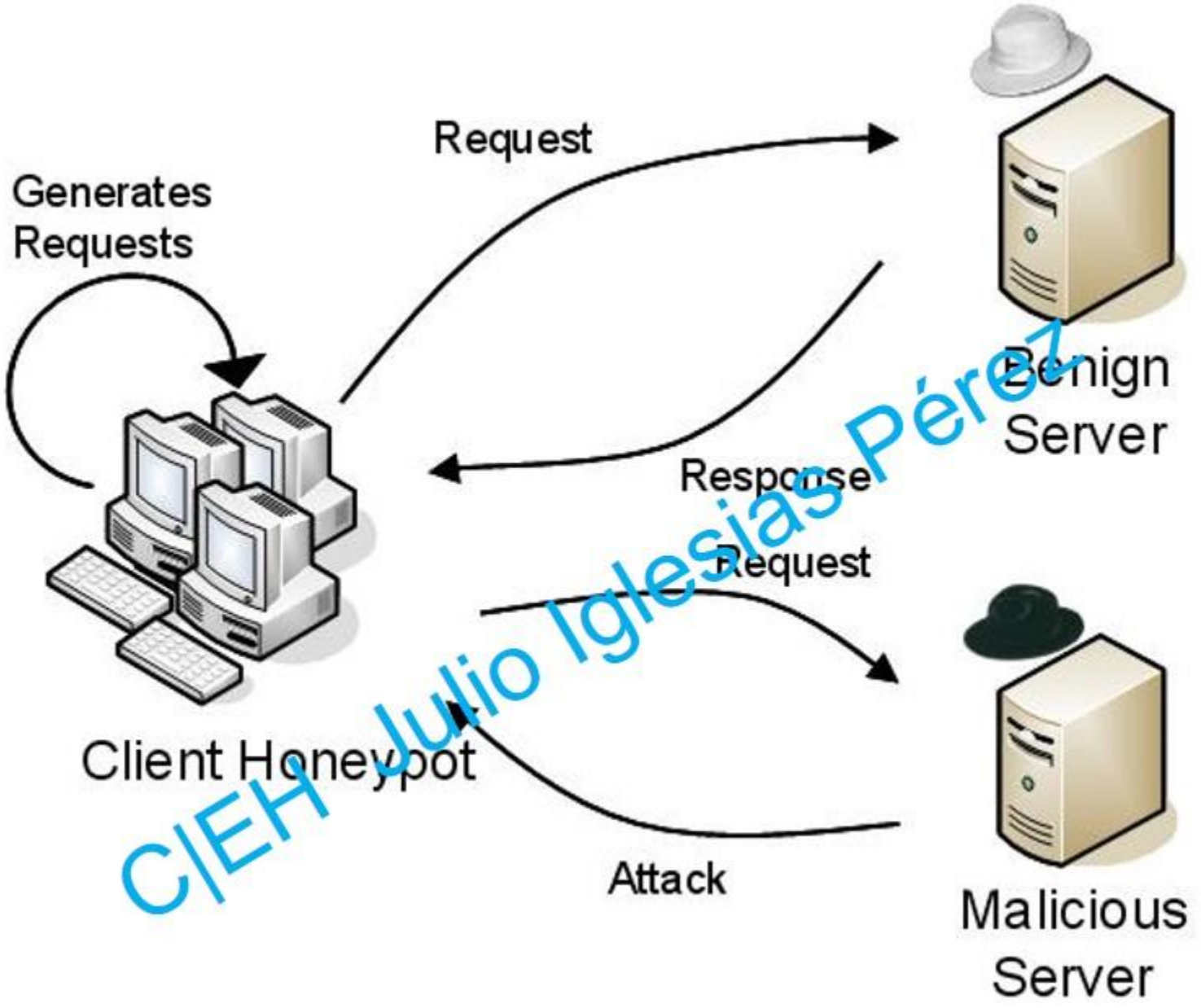
Un ejemplo de banner grabbing SMTP es: telnet mail.gargetcompany.org 25

Honeypot

Es una información de un recurso del sistema que está expresamente configurado para atraer y atrapar personas que intentan penetrar la red de una organización.

No tiene actividad autorizada, no tiene ningún valor de producción y es como un sondeo, ataque o compromiso.

Puede ser utilizado para registrar intentos de acceso a aquellos puertos incluyendo los keystrokes del atacante. Puede enviar mensajes de advertencia tempranos.



Tipos de honeypots

Honeypot de poca interacción

- Trabajan emulando servicios y programas que pueden ser encontrados en un sistema individual.
- Si el atacante hace algo que la emulación no espera, el honeypot simplemente generará un mensaje de error.
- Captura cantidades limitadas de información, principalmente datos transaccionales y alguna interacción limitada.

Ej: Specter, Honeyd, KFSensor

Tipos de honeypots

Honeypot de elevada interacción

- Sistemas, redes o equipos enteros, para tener controlada un área donde los atacantes pueden interactuar con aplicaciones y programas reales.
- Se basan en dispositivos de borde para controlar el tráfico para que los atacantes puedan ingresar, pero la actividad de afuera es estrechamente controlada.- Captura mucha más información, incluyendo nuevas herramientas, comunicaciones y keystrokes de los atacantes.

Ej: Symantec Decoy Server y Honeynets

¿Cómo configurar un Honeypot?

- Descargar o comprar un software honeypot.
- Para Linux algunos son: Tini Honeypot, LaBrea, Honeyd.
- KFSensor para Windows.
- Iniciar sesión como administrador al equipo para instalarlo.
- Instalar el software en su equipo, elegir full versión.

IDS, Firewall y Sistema Honeyspot

Herramienta IDS Snort: OpenSource, en tiempo real analiza el tráfico y loggin de paquetes en las redes IP. Realiza análisis de protocolo y contenido. Detecta varios ataques y sondeos.

¿Cómo funciona Snort?

- Decodificador: Guarda los paquetes capturados dentro de una pila, identifica los protocolos de nivel de vínculo y decodifica el IP.
- Motor de detección: Compara paquetes con reglas previamente cargadas en la memoria.
- Plugins de salida: Estos módulos formatean las notificaciones para el usuario para que acceda de distintas maneras (consola, archivos externos, bases de datos, etc.)

Reglas Snort

- El motor de reglas de Snort escribe sus propias reglas.
- Ayudan a diferenciar entre actividades de internet normales y maliciosas.
- Deben estar contenidas en una línea, el analizador de regla no admite reglas en múltiples líneas.

Regla de acciones y protocolos IP

- Regla de acciones: El encabezado de la regla almacena información completa sobre un paquete y determina la acción que aplicará.
- Alerta a Snort cuando encuentra un paquete con una regla determinada.
- Hay tres acciones:
  - Alerta.
  - Registra.
  - Ignora.

Reglas Snort: El Operador de dirección y direcciones IP

Operador de dirección: Indica la dirección del tráfico. Puede ser uni o bidireccional -> <>Ejemplo:

log !192.168.1.0/24 any <> 192.168.1.0/24 23

Direcciones IP

- Información de direcciones IP y puertos.
- Utilizar la palabra "any" para definir cualquier dirección IP.

Ejemplo:

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg: "external mountd access";)

Reglas Snort: Números de puertos

- Ejemplo:

log tcp any any -> 192.168.1.0/24 !6000:6010

log udp any any -> 98.168.1.0/24:1024. Registra el tráfico UDP q venga de cualquier puerto y ´puerto destino desde 1 a 1024.

Reglas Snort: Números de puertos

log tcp any any -> 192.168.1.0/24:5000.
Registra tráfico TCP desde cualquier puerto a puertos menores o iguales a 5000

log tcp any :1024-> 192.168.1.0/24 400:
Registra tráfico desde puertos privilegiados menores o iguales a 1024 yendo a puertos mayores o iguale a 400.

Herramienta IDS: Tipping Point

- Es insertado sin problemas y transparente dentro de la red, es un dispositivo in-line.
- Cada paquete es inspeccionado a fondo para determinar si son maliciosos o legítimos.
- Provee protección de rendimiento, aplicación e infraestructura a velocidades gigabit de inspección de paquetes.

Herramienta IDS: Tipping Point

Firewall: Subnet Personal Firewall.

Herramienta Honeypot: KFSensor

Características:

- Consola de administración GUI.
- Administración remota.
- Compatibilidad con el motor de firmas de Snort.
- Emulaciones para protocolos de red de Windows.
- Exporta registros en formatos múltiples.
- Protección contra ataques DoS.

Herramienta Honeypot: SPECTER

- Es un IDS inteligente que ofrece servicios de Internet comunes como SMTP, FTP, POP3, HTTP Y TELNET.
- Provee varias cantidades de señuelos como imágenes, mp3, mensajes de correo, archivos de contraseñas, documentos y todo tipo de software.

Evasión de IDS

Ataque de inserción

1. Un IDS confía y acepta un paquete que un sistema final ha rechazado.
2. Un atacante explota esta condición e inserta datos dentro del IDS.
3. Este ataque ocurre cuando el NIDS es menos restrictivo en los paquetes de procesamiento.
4. Un atacante utiliza estos paquetes para vencer al análisis de firma y solicitudes de envío.
5. El IDS obtiene más paquetes que el destino.

Evasión

1. En esta técnica de evasión, un sistema final acepta el paquete que el IDS rechazó.
2. Utilizando esta técnica, un atacante explota el host.
3. El atacante envía porciones de solicitudes en paquetes que el IDS rechaza por error, permitiendo remover las partes de la corriente desde la vista del ID del sistema.
4. Ejemplo, si la secuencia maliciosa es enviada byte por byte y un byte es rechazado por el IDS, el IDS no puede detectar el ataque.
5. Aquí el IDS recibe menos paquetes que el destino.

Ataque DoS

- Muchos IDS emplean servidores de loggin centrales que son utilizados exclusivamente para almacenar registros de alerta IDS.
- Si los atacantes saben la IP del servidor de logs central, ellos pueden alentarlo o incluso bloquearlo con un ataque DoS.

Ofuscar

- Un IDS puede ser evadido ofuscando o codificando el payload del ataque.
- Un atacante manipula la ruta referenciada en una firma.
- Codificar paquetes de ataque que el IDS no reconoce, pero el IIS los decodificará y será atacado.
- Ataques a protocolos encriptados como HTTPS.
- Código polimórfico.

Generación de Falso Positivo

- Otro ataque similar al método DoS es generando una gran cantidad de datos de alerta que deben ser registrados.
- Generar número largo de reportes falsos.- Mezclar ataques reales con falsos.
- Puede llegar a ser muy difícil diferenciar entre ataques legítimos y falsos positivos.- Generar falsos positivos específicos.

Empalme de sesión

1. Es una técnica de evasión que explota algunos IDS no solicitan sesión de reconstrucción antes de realizar patrones parecidos en los datos.
2. La idea es empalmar datos entre varios paquetes, asegurando que los paquetes no muestren patrones en la firma IDS.
3. Si los atacantes saben qué IDS se está utilizando, se puede agregar retrasos entre paquetes para omitir la comprobación de montaje.

Empalme de sesión

4. Muchos IDS re ensamblan las comunicaciones, así que si el paquete no fue recibido en un tiempo razonable, puede ser que el IDS haya detenido.
5. Si la aplicación bajo ataque mantiene una sesión activa más larga que el tiempo que el IDS tardará, el IDS se detendrá.
6. Como resultado, una sesión luego de que el IDS detenga el re ensamblaje, la sesión será susceptible a datos maliciosos.

Técnica de Evasión Unicode

Representación de carácter que da a cada carácter un identificador único. Esto dificulta a los IDS porque es posible tener múltiples representaciones de un simple carácter. Por ejemplo el "\" puede ser representado como 5C, C19C y E0819C

Ataques Time-To-Live

En este tipo de ataques, el atacante debe tener conocimiento sobre la topología de la red de la víctima. Esta información se puede obtener utilizando traceroute la cual da información sobre el número de routers entre el atacante y la víctima.

Paquetes RST Inválidos

1. El protocolo TCP utiliza las sumas de comprobación para asegurarse que la comunicación es posible.
2. Una lista de comprobación es agregada a cada segmento transmitido y es chequeado en el extremo receptor Cuando una suma de comprobación difiere de la suma de comprobación esperada por el host de recepción, el paquete es dropeado en el extremo receptor.
3. El protocolo TCP también utiliza un paquete RST para terminar una comunicación two-way.

Paquetes RST Inválidos

4. Los atacantes pueden utilizar esta característica para eludir la dirección enviando paquetes RST con una suma de comprobación inválida, que causa que el IDS detenga el procesamiento del flujo porque el IDS cree que la comunicación ha terminado.

5. Sin embargo, el receptor final ve el paquete y verifica el valor de la suma de comprobación, luego dropea el paquete si es inválido

.6. Algunos sistemas IDS pueden interpretar este paquete con una terminación real de la comunicación y detiene el re ensamblaje de la comunicación.

Paquetes RST Inválidos

7. Algunas instancias permiten a los atacantes continuar la comunicación con el receptor final confundiendo al IDS porque el receptor final acepta los paquetes que siguen al paquete RST con una suma de comprobación inválida.

Bandera de emergencia

Es utilizada dentro del protocolo TCP para marcar los datos como urgentes. Utiliza un puntero que apunta al principio de la bandera de urgencia dentro del paquete. Cuando la bandera se establece, todos los datos antes del puntero son ignorados, y los datos a los cuales seña el puntero son procesados.

Bandera de emergencia

Algunos IDS no toman en cuenta la característica de urgencia de TCP, lo que puede permitir a los atacantes evadir IDS. Los atacantes pueden colocar datos basura en el puntero de urgencia, y el IDS lee los datos sin consideración por de el flag de urgencia del host. Esto quiere decir que el IDS tiene más datos de los que el host puede procesar.

Código shell polimórfico

1. Muchos IDS contienen firmas para las cadenas comúnmente utilizadas dentro del shellcode.
2. Esto es fácilmente saltado utilizando código shell codificado conteniendo un talón (stub) que codifica el shellcode que sigue.3. Esto significa que el shellcode puede ser completamente distinto cada vez que es enviado.
4. El Shellcode polimórfico permite a los atacante esconder su shellcode cifrándolo.

Código Shell Polimórfico

5. Es difícil para los IDs identificar esto como shellcode.
6. Este método también esconde las cadenas comúnmente utilizadas dentro del shellcode, haciendo de las firmas de shellcode inservibles.

Ataques en la capa Aplicación

1. Muchas aplicaciones que trabajan con Medía como imágenes, videos y audio emplean algunos manera de comprensión para enviar a un formulario mas pequeño que el original lo cual incrementa la velocidad de transferencia de datos.

2. Cuando una falla es encontrada en estas aplicaciones, el ataque completo puede ocurrir dentro de los datos compresos y la IDS no tendrá manera de revisar el formato del archivo compreso.

Ataques en la capa Aplicación

3. Muchos IDS buscan por condiciones específicas. Sin embargo, hay momentos en que el ataque puede tomar distintas formas.
4. Por ejemplo, vulnerabilidades de overflow enteras pueden ser explotadas utilizando valores de integridad distintos.
5. Este hecho combinado con datos compresos hace la detección de formas extremadamente difícil.

Desincronización: Pre Conexión SYN

- Este ataque a "bind" para que el kernel asigne un puerto local al socket antes de llamar a "connect".
- enviar un SYN inicial antes de la conexión real con una suma de comprobación TCP inválida.
- Si el sniffer ignora subsecuentemente la conexión SYN, y no revisa la suma de comprobación TCP, entonces el ataque sincronizará el sniffer/IDS a una secuencia de números falsa antes de que la conexión real ocurra.

Desincronización: Post Conexión SYN

1. Para esta técnica se intenta desincronizar el IDS de la actual secuencia de números que el kernel está cumpliendo.
2. enviar un paquete luego dela conexión SYN en el flujo de datos, tendrá una secuencia de números divergente, pero por lo demás cumple todos los criterios necesarios para ser aceptado en el host objetivo.
3. Sin embargo, el host objetivo ignorará este paquete SYN, como se hace referencia a una conexión establecida.

Desincronización: Post Conexión SYN

4. El intento de este ataque es producir una desincronización del IDS de su noción de la secuencia de números de un nuevo paquete SYN.
5. A continuación se ignorarán todos los paquetes legítimos del flujo original, porque estará esperando una secuencia de números distinta.
6. Una vez realizada la desincronización entre el IDS y el paquete SYN, se enviará un paquete RST con una nueva secuencia, esto cerrará la noción de la conexión.

Otros tipos de evasión

- Encriptación: Si el atacante establece una sesión cifrada con la víctima, esto resultará el ataque de evasión más efectivo.
- Flooding: El atacante envía cargas de tráfico innecesario produciendo "ruido" y el IDS no analizará este tráfico ruido, el verdadero ataque puede no ser detectado.

Evadiendo Firewalls

Falsificación de dirección IP

- Utilizando esta técnica, el atacante obtiene acceso no autorizado a un equipo o red, haciendo parecer que el mensaje viene de un equipo verdadero. Para saltar el firewall, el atacante modifica la dirección de información en el encabezado del paquete IP y el campo de dirección fuente.

Evadiendo Firewalls

Ataque con mecanismo de generación de Tokens

- Utilizando esta técnica, el que envía el paquete designa la ruta que el paquete debe tomar a través de la red. Cuando estos paquetes viajan por los nodos de la red, cada router revisará la IP destino y renviarán los paquetes al próximo nodo. En el router fuente, el atacante hace parte o todas estas decisiones.

Evadiendo Firewalls

- Pequeños fragmentos.
- – El atacante utiliza la técnica de fragmentación IP para crear fragmentos extremadamente pequeños y forzar a la información del encabezado TCP ir en el próximo fragmento. Esto puede resultar en el caso de que el campo de flags de TCP sean forzadas en un segundo fragmento, los filtros no podrán revisar estas flags en el primer octeto, por lo que ignorará los fragmentos subsecuentes (cont.)

Evadiendo Firewalls

Los atacantes esperan que solo el primer fragmento se examinado por el primer router de filtrado y los restantes son pasados. Este ataque es utilizado para impedir las reglas de filtrado definidas por el usuario y trabaja cuando el firewall revisa solo la información de encabezado TCP.

Evadiendo Firewalls

Se puede saltar los sitios bloqueados utilizando la IP en vez de la URL.

Evadiendo Firewalls

Saltando Sitios bloqueados utilizando Navegación de sitios anónima.

Algunos sitios permite la opción de cifrar las URLs de los sitios. Estos sitios proxy esconden la dirección IP actual y muestran otra, esto ayuda a prevenir los sitios bloqueados.

Ejemplos:

- http://www.anonymizer.com
- http://www.anonymouse.org
- http://www.proxify.com
- http://www.bumsk.com
- http://www.dailybestlinks.com

Evadiendo Firewalls

Saltando el Firewall a través del método ICMP Tunneling.

- Permite hacer un túnel de shell backdoor en la porción de datos de los paquetes ICMP echo. Esta porción payload es arbitraria y no es examinada por la mayoría de firewalls. Asumiendo que ICMP está permitido en el firewall, utilizar Loki ICMP tunneling para ejecutar comandos de elección haciéndolos un túnel dentro del payload de los paquetes ICMP echo.

Evadiendo Firewalls

Saltando el Firewall a través del método ACK Tunneling.

- Permite hacer un túnel de aplicación backdoor con paquetes TCP con el bit ACK. Este BIT es utilizado para reconocer el recipiente de un paquete. Algunos firewalls no revisan estos paquetes. Utilizar herramientas como AckCMD (http://ntsecurity.nu).

Evadiendo Firewalls

- Saltando el Firewall a través del método HTTP Tunneling
  - Este método puede ser implementado si la compañía objetivo tiene un Servidor Web público con el puerto 80 para el tráfico HTTP. Muchos firewalls no examinan el payload del paquete HTTP para confirmar si el tráfico HTTP es legítimo. Herramientas como HTTPTunnel (www.nocrew.org) utiliza esta técnica para hacer túnel a través del puerto 80. Subir (upload) el servidor en el sistema objetivo e indicarle qué puerto será redirigido a través del puerto TCP 80.

Evadiendo Firewalls

Saltando el Firewall a través de sistemas externos.

1. Un usuario legítimo trabaja con algún sistema externo para acceder a la red corporativa.
2. El atacante olfatea el tráfico del usuario, roba la sesión ID y las cookies.
3. El atacante accede a la red corporativa saltando el firewall y obteniendo la ID de Windows y ejecutando Netscape 4.x/Mozilla en el sistema del usuario.

Evadiendo Firewalls

4. El atacante luego emite un comando "openURL()" en la ventana encontrada.
5. El navegador del usuario se conecta con el servidor WWW del atacante.
6. El atacante inserta un payload malicioso dentro de la página Web solicitada (applet de Java) y por lo tanto el código del atacante se ejecuta en el equipo del usuario.

Evadiendo Firewalls

Saltando el firewall con un ataque MITM

1. El atacante realiza un DNS Server Poisoning.
2. El usuario A solicita un sitio (ej: www.juggyboy.com) al DNS Server corporativo.
3. El servidor DNS envía la IP (ej: 127.22.16.64) del atacante.
4. El usuario A accede al servidor Web malicioso.
5. El atacante se conecta con el host real y hace un túnel del tráfico HTTP del usuario.
6. El atacante inserta un payload malicioso dentro del sitio web solicitado (applet de Java) y por lo tanto el código del atacante se ejecuta en el equipo del usuario.

Evadiendo Firewalls

Detectando Honeypots: Los atacantes pueden determinar la presencia de honeypots probando los servicios en ejecución del sistema. El atacante elabora un paquete de sonda maliciosa para escanear servicios como HTTP sobre SSL (HTTPS), SMTP sobre SSL (SMTPS) e IMAP sobre SSL (IMAPS).

Evadiendo Firewalls

Algunas herramientas utilizadas son:

- Send-safe Honeypot.
- Hunter.
- Nessus.
- Hping. Los puertos que muestran un servicio particular en ejecución pero deniegan la three handshare connection indica la presencia de un honeypot.

Herramienta de detección de Honeypot

Send-Safe Honeypot Hunter- Revisa la lista de proxis HTTPS, SOCKS4, SOCKSS con cualquier puerto. Revisa listas proxy remotas o locales. Puede subir archivos "Valid proxis" y "All except honeypots" a un FTP.

Herramientas de evasíón de Firewall

- Traffic IQ Professional: Permite a los profesionales de seguridad auditar y validar el comportamiento de dispositivos de seguridad generando tráfico de aplicación estándar o tráfico de ataque entre dos equipos virtuales. Puede ser utilizado para evaluar, auditar y probar las características de comportamiento de cualquier dispositivo no proxy y filtrado de paquetes incluyendo:
  - Firewall de la capa Aplicación.
  - IDS.
  - Sistemas de prevención de Intrusión.
  - Routers y switches.

Herramientas de evasión de Firewall

- tcp-over-dns: Contiene servidores DNS especiales y clientes dns especiales. El cliente y el servidor trabajan en un tandem para proveer un túnel TCP (y UDP) a través del protocolo estándar de DNS.

Contramedidas

- Administrativamente apagar una interfaz de puerto de switch asociada a un sistema desde el cual sus ataques han sido realizados.
- Buscar que el código de operación no sea otro que 0x90 para defenderse contra problemas de shellcode polimórfico.
- Realizar un análisis bifurcado, en donde el monitor trata el tráfico ambiguo.
- Mantener los parches de vulnerabilidades actualizado.

Contramedidas

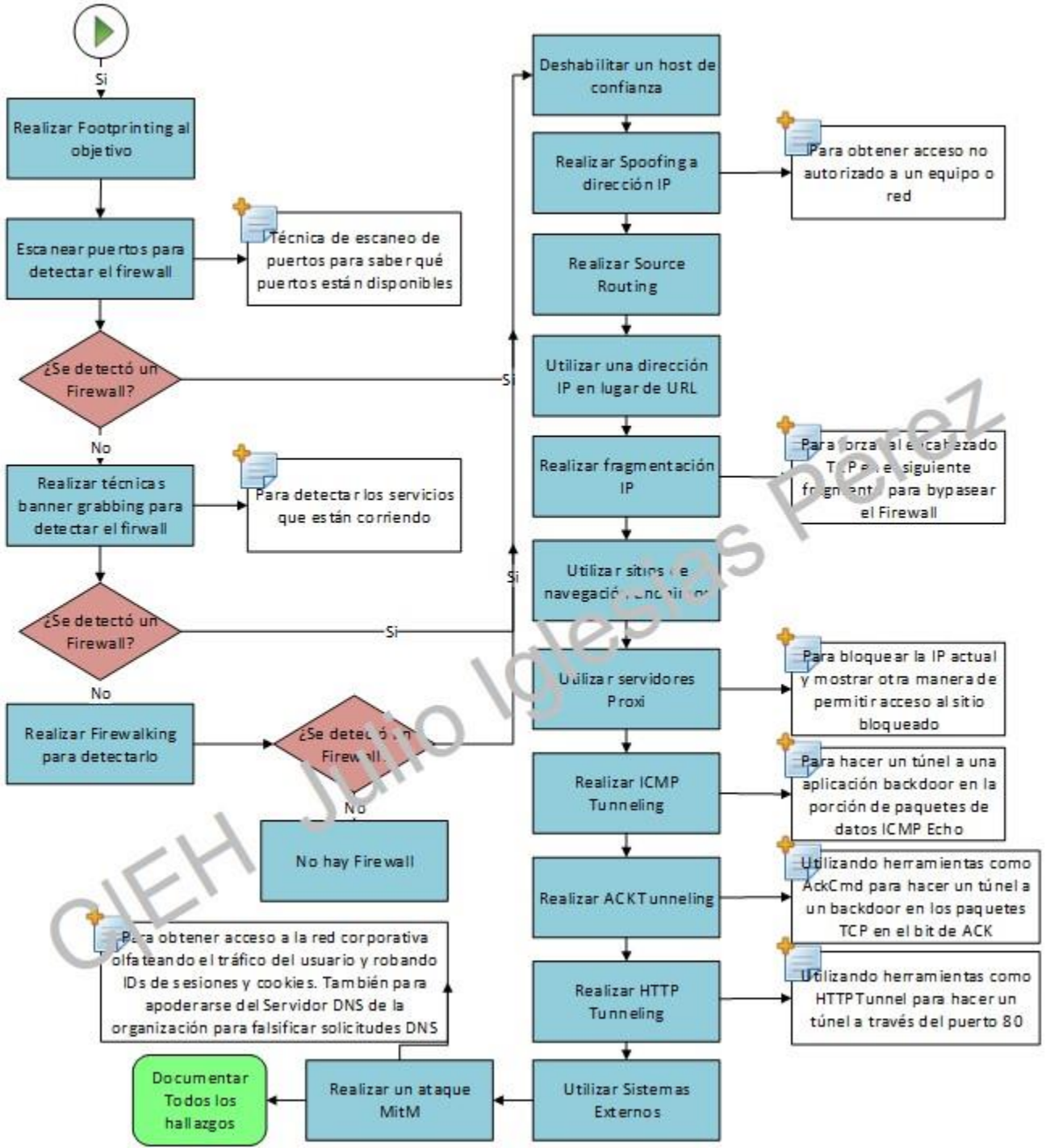
- Generar paquetes TCP RST para quitar las sesiones TCP maliciosas.
- Interactuar con un firewall externo o router para agregar una regla general para bloquear comunicaciones desde direcciones IP individuales o redes enteras.
- Implementar un normalizador de tráfico, una red de renvío de elementos que intentan eliminar tráfico de red ambiguo.

Contramedidas

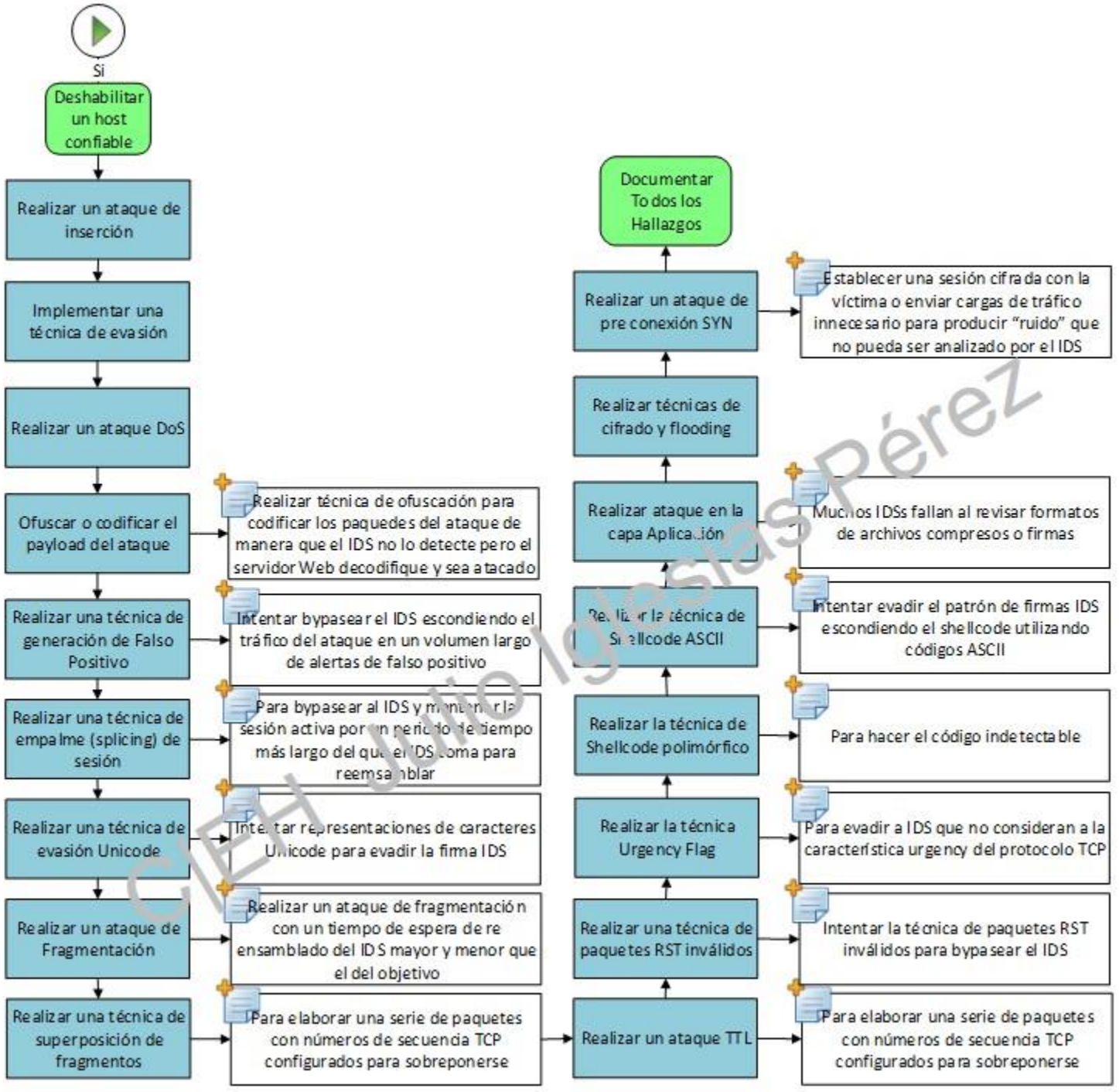
- Asegurarse de normalizar los paquetes fragmentados.
- Mantener actualizado el IDS.
- Mantener actualizaciones

Test de Intrusión

Es para evaluar las vulnerabilidades de entrada y de salida y las reglas apropiadas de la red.




Test de intrusión al IDS




¡Muchas Gracias!
C|EH Julio Iglesias Perez