**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | *Hacking* ético en sistemas y redes |
| --- | --- |

| COMPETENCIA | 220501111. Controlar sistema de seguridad de la información de acuerdo con los procedimientos y normativa técnica. | RESULTADOS DE APRENDIZAJE | 220501111-3. Emplear herramientas especializadas para la solución de problemas de ciberseguridad y seguridad informática en sistemas y redes. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | CF004 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Ingeniería social y detección de intrusos en *hacking* ético |
| BREVE DESCRIPCIÓN | La seguridad informática se ha convertido hoy en día en una preocupación para empresas y organizaciones en medio del mundo digital, es por ello que es importante conocer y aplicar diferentes herramientas digitales para ciberseguridad y conocer las vulnerabilidades y ataques a los cuales están expuestos los sistemas y redes y así protegerlos de cibercriminales. |
| PALABRAS CLAVE | ataque, *bootnets*, ingeniería, *pentesting*, redes, vulnerabilidad, virus |

| ÁREA OCUPACIONAL | 2 - Ciencias naturales, aplicadas y relacionadas |
| --- | --- |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

1. **Ingeniería social**
   1. Conceptos y generalidades
   2. Tipos y fases de la ingeniería social
   3. Riesgos de suplantación (redes sociales)
   4. Ataques y riesgos (vulnerabilidades)
   5. *Pentesting*
2. **Denegación de servicios**
   1. Conceptos y generalidades
   2. Herramientas y técnicas de ataque
   3. *Botnets*
   4. Contramedidas
3. **Detección y evasión de intrusos**
   1. Conceptos y generalidades
   2. Tipos de IDS
   3. *Firewall* y *Honeypot*
   4. Evasión de IDS y *firewalls*

**Síntesis**

1. **Desarrollo de contenidos**

**Introducción**

En el mundo digital de hoy, usted encuentra gran cantidad de información al alcance de su mano, la cual se ha convertido en uno de los activos más importantes para una persona u organización. Con el uso de las tecnologías de la información y la comunicación y su avance vertiginoso, aparecen agentes tanto internos como externos que pueden poner en riesgo los sistemas de información y los datos que se almacenan, al igual que la infraestructura tecnológica donde se encuentran. Es por ello que el *hacking* ético se ha convertido en una herramienta de gestión para poder salvaguardar los datos. Revise el siguiente recurso para contextualizar.



Para la elaboración de este componente, se abordaron varios autores conocidos en **ingeniería social y detección de intrusos en *hacking* ético**, de quienes se han citado y referenciado conceptos y ejemplos para los fines educativos de esta materia, en el entendido de que el conocimiento es social y, por lo tanto, es para ser usado por quienes necesitan adquirirlo. Se espera que este documento sea útil para todos aquellos, aprendices y lectores en general, que estén interesados en acercarse a asuntos básicos de ***hacking* ético en sistemas y redes**.

1. **Ingeniería social**

El activo más importante de una organización hoy en día es la información que esta maneja. Aunque usted se enfrente a un mundo digital y globalizado, las máquinas siguen siendo manipuladas y controladas por el ser humano; es por ese motivo que, dentro de la ingeniería social, se puede decir que el eslabón más débil de toda esta cadena informática es el usuario, y es así como los ciberdelincuentes aprovechan habilidades sociales para vulnerar sistemas e infraestructura. Es importante reconocer que muchas personas poseen este tipo de entrenamiento para atacar y es perentorio conocer su actuar para estar protegido frente a estas técnicas persuasivas que utilizan.

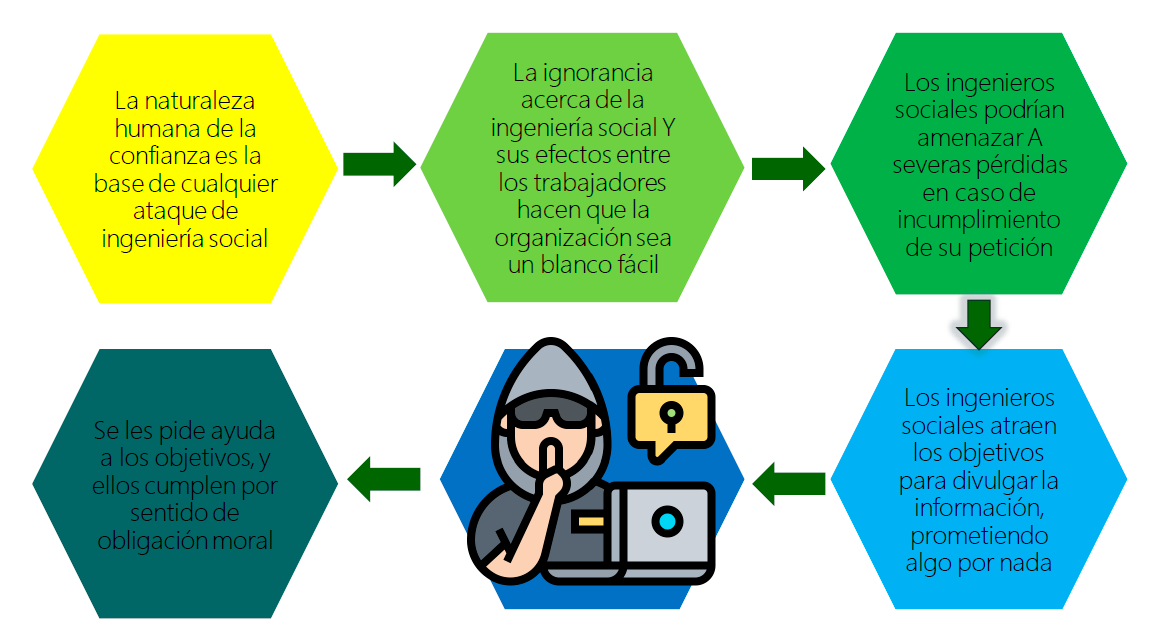
* 1. **Conceptos y generalidades**

La ingeniería social es el arte de manipular a la gente para que entregue información confidencial. Los tipos de información que estos criminales buscan pueden variar, pero cuando los individuos son el objetivo, los criminales normalmente intentan engañar para obtener las contraseñas o la información bancaria, o para que usted acceda a su ordenador para instalar secretamente *software* malicioso, lo que les dará acceso a sus contraseñas e información bancaria, además de darles control sobre su ordenador.

Los delincuentes utilizan tácticas de ingeniería social porque normalmente es más fácil explotar su inclinación natural a la confianza que descubrir formas de piratear su *software*. Por ejemplo, es mucho más fácil engañar a alguien para que le dé su contraseña que intentar piratear su contraseña (a menos que la contraseña sea realmente débil).

**Figura 1**

*Ingeniería social*



La seguridad consiste en saber en quién y en qué confiar. Es importante saber cuándo y cuándo no tomarle la palabra a una persona y cuándo la persona con la que se está comunicando es quien dice ser; lo mismo ocurre con las interacciones en línea y el uso de los sitios web:





**Figura 2**

*Riesgos*



En la infografía, se muestra cómo las empresas actualmente se ven enfrentadas a riesgos referentes a su información.

Sin embargo, los propios líderes empresariales a menudo no toman medidas sencillas para protegerse a sí mismos y a sus empresas contra los ataques de ingeniería social:

* Sólo el 51% de los líderes empresariales ajustan su configuración en sitios como Facebook para restringir quién puede ver su perfil.
* Sólo el 36% actúa cuando se cambian las configuraciones de privacidad en los sitios de medios sociales.
* Sólo el 24% comprueba regularmente la información disponible sobre ellos mismos en línea o comprueba las políticas de intercambio de datos al suscribirse a nuevos servicios en línea.





Si su empresa y su equipo son vulnerables a un intento de ingeniería social, le falta una pieza crítica de su estrategia de seguridad de datos.

La ingeniería social es el equivalente a señalar una mancha imaginaria en la camisa de alguien, solo para mover la nariz cuando mira hacia abajo - al hacerse pasar por alguien de confianza, un ciberdelincuente tiene la oportunidad de hacer lo que quiera con los datos de un negocio, estos ataques tienen dos factores a su favor, como se muestra a continuación.



La inteligencia de código abierto puede provenir de una amplia gama de fuentes de datos, que solo ayudan a un aspirante a ingeniero social; a través de algunas excavaciones en Internet, un ingeniero social puede encontrar mucha información que ayuda a su ataque.

**Figura 2**

*Ingeniero social*



Los ingenieros sociales manipulan los sentimientos humanos, como la curiosidad o el miedo, para llevar a cabo esquemas y atraer a las víctimas a sus trampas, por lo tanto, tenga cuidado cuando se sienta alarmado por un correo electrónico, atraído por una oferta mostrada en un sitio web, o cuando se encuentre con medios digitales extraviados mintiendo. Estar alerta puede ayudarle a protegerse contra la mayoría de los ataques de ingeniería social que tienen lugar en el ámbito digital.

**Impactos de la ingeniería social**

A diferencia de un virus, que depende de técnicas de *hacking* o código malicioso para entregar su carga, la ingeniería social depende de la psicología humana; bien utilizada, puede ser aprovechada para acceder a datos, sistemas e incluso edificios. Por ejemplo, en lugar de pasar meses trabajando en una nueva cepa de *malware*, los criminales centran su atención en engañar a los empleados para que divulguen su contraseña por teléfono, haciéndose pasar por un técnico de soporte informático; si hablan con la persona correcta y dicen las cosas correctas, podrían estar en la red en momentos.



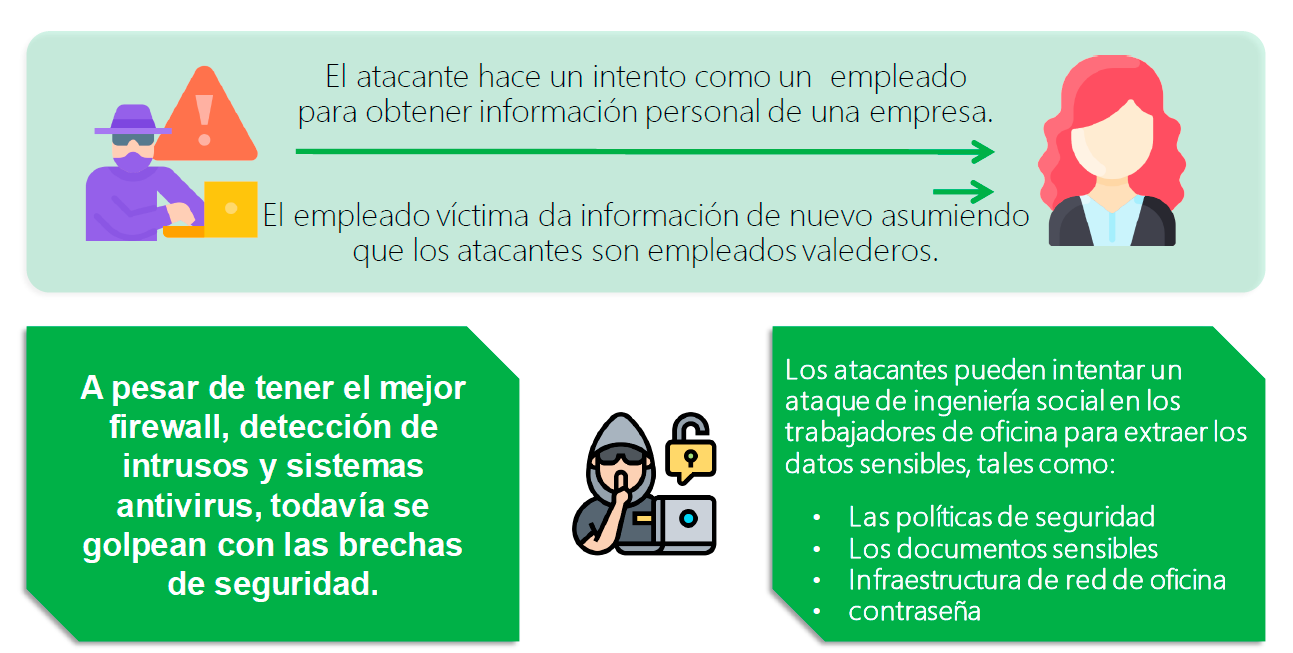
Con la investigación adecuada, un ingeniero social puede compilar un perfil inquietantemente exhaustivo de una empresa, sus empleados, sus operaciones y más. Algunos ejemplos muy breves e incompletos son los siguientes:

* **Tecnología:** La información sobre el tipo de tecnología que un negocio aprovecha es sorprendentemente común en línea; en los anuncios de empleo, por ejemplo, se suele identificar el *hardware* y el sistema operativo que utiliza una empresa para asegurarse de que el solicitante esté familiarizado con los sistemas con los que trabajaría, el problema es que esto también ayuda a un delincuente a identificar qué explotamientos serán efectivos contra una empresa; además, si una empresa no tiene cuidado, sus imágenes de medios sociales podrían proporcionar a un ciberdelincuente información sobre su *hardware* de redes.
* **Información de los empleados:** También es común que la gente comparta demasiado en los medios sociales, lo que puede llevar fácilmente a que también se comparta la información de la empresa, esto incluye, además del acceso a la información que muchos permiten que esté disponible públicamente a través de los medios sociales, imágenes del lugar de trabajo, esas imágenes suelen revelar el tipo de computadora utilizada por los empleados, así como el contenido de sus pantallas y toda la información que aparece en ellas. Además, muchas personas comentarán su horario de trabajo en los medios sociales, así como proporcionarán un relato detallado de su experiencia profesional, lo que dará a un ingeniero social más datos con los que trabajar.
* **Vendedores y otras empresas:** Los servicios externos que se prestan a una empresa pueden ayudar a un ingeniero social a acceder a esa empresa, especialmente si el proveedor de servicios los utiliza como prueba de valor en su sitio web. Los servicios de limpieza y los servicios de recogida de basura son especialmente valiosos, ya que los datos podrían ser robados después de salir del local de una empresa.

En resumen, si bien es crucial proteger sus datos con cortafuegos, requisitos de autenticación y otras medidas digitales, es igualmente crucial asegurarse de que sus empleados sean conscientes de los peligros que puede entrañar la ingeniería social. Establecer procesos que ayuden a frustrar los intentos de ingeniería social es algo que toda empresa debería hacer, ya que ayudará a protegerlos de estos ataques.

**Figura 3**

*Intentos de ingeniería social*



**A continuación, encuentra relacionadas algunas formas de protegerse:**

* Borre cualquier solicitud de información financiera o contraseñas. Si le piden que responda a un mensaje con información personal, es una estafa.
* Rechace las solicitudes de ayuda o las ofertas de ayuda. Las empresas y organizaciones legítimas no se ponen en contacto con usted para ofrecerle ayuda si no solicitó específicamente la ayuda del remitente. Considere cualquier oferta de "ayuda", para restaurar los puntajes de crédito, refinanciar una casa, responder a su pregunta, etc., como una estafa; del mismo modo, si recibe una solicitud de ayuda de una organización benéfica u organización con la que no tiene relación, elimínela. Para dar, busque por su cuenta organizaciones caritativas de buena reputación para evitar caer en una estafa.
* Ponga sus filtros de *spam* en alto. Todos los programas de correo electrónico tienen filtros de *spam*, para encontrar el suyo, mire las opciones de configuración y póngalas en alto. Recuerde revisar su carpeta de *spam* periódicamente para ver si el correo electrónico legítimo ha quedado atrapado allí accidentalmente; también puede buscar una guía paso a paso para configurar sus filtros de *spam*, buscando el nombre de su proveedor de correo electrónico más la frase 'filtros de *spam'*.
* Asegure sus dispositivos informáticos, instale *software* antivirus, cortafuegos y filtros de correo electrónico, y manténgalos actualizados. Configure su sistema operativo para que se actualice automáticamente, y si su *smartphone* no se actualiza automáticamente, actualícelo manualmente cada vez que reciba un aviso para hacerlo. Utilice una herramienta *antiphishing* ofrecida por su navegador web o por un tercero para alertarle de los riesgos.
  1. **Tipos y fases de la ingeniería social**

La ciberdelincuencia no solo opera bajo códigos y herramientas sofisticadas, también hace uso de habilidades sociales del comportamiento humano para su actuar. En este módulo, se presentan diferentes fases que un ingeniero social usa para poder acceder a toda la información sensible que le puede servir para poder identificar vulnerabilidades dentro del *hacking* ético:

* Fase 1: Recopilación de información

La probabilidad de éxito de la mayoría de los ataques depende de esta fase, por lo que es natural invertir la mayor parte del tiempo y la atención en ella. Las técnicas de recopilación de información se elaboran en el Marco. Parte de la información reunida se utiliza para determinar el vector de ataque, las posibles contraseñas, identificar las posibles respuestas de diversas personas, afinar los objetivos, familiarizarse y sentirse cómodo con el objetivo, y formular uno o varios pretextos sólidos.

* Fase 2: Establecer la relación y la compenetración

Esta fase establece una relación de trabajo con el objetivo, este es un punto crítico ya que la calidad de la relación construida por el atacante determina el nivel de cooperación y la medida en que el objetivo irá a ayudar al atacante a lograr el objetivo; puede ser tan breve como apurarse hacia la puerta con una gran sonrisa y contacto visual para que el objetivo mantenga la puerta abierta para que el atacante la atraviese; puede ser conectarse a nivel personal por teléfono o tan personal como mostrar fotos de la familia y compartir historias con la recepcionista en el vestíbulo; también puede ser tan extenso como construir una relación *online* con el objetivo, a través de un perfil falso en un sitio de citas o de redes sociales. La creación de una relación se trata más a fondo en el Marco.

* Fase 3: Explotación

Esto es cuando el atacante utiliza tanto la información como las relaciones para infiltrarse activamente en el objetivo. En esta fase, el atacante se centra en mantener el impulso de cumplimiento que se construyó en la fase 2, sin levantar sospechas; la explotación puede tener lugar mediante la divulgación de información aparentemente sin importancia o el acceso concedido/transferido al atacante.

Entre los ejemplos de explotación exitosa se incluyen:

* El acto de mantener la puerta abierta o permitir de cualquier otra forma que el atacante entre en las instalaciones.

* Revelar la contraseña y el nombre de usuario por teléfono.
* Ofrecer pruebas sociales presentando la SE a otros empleados de la compañía.
* Insertar una unidad flash USB con una carga útil maliciosa en un ordenador de la empresa.
* Abrir un archivo adjunto de un correo electrónico infectado.
* Exponer secretos comerciales en una discusión con un supuesto “par”.
* Fase 4: Ejecución

Esta fase es cuando se logra el objetivo final del ataque o, por diversas razones, se pone fin al mismo, de tal manera que no se levanten sospechas sobre lo que ha ocurrido. Por lo general, no es una buena práctica terminar un ataque con el objetivo cuestionando lo que acaba de ocurrir, en cambio, es mejor dejar que el objetivo sienta que ha hecho algo bueno por otra persona, lo que permite que continúen las posibles interacciones futuras. También se abordan aquí los cabos sueltos, como borrar las huellas digitales y asegurarse de que no quede ningún elemento o información para que el objetivo pueda determinar que se ha producido un ataque o la identidad del atacante. Una estrategia de salida bien planificada y sin problemas es el objetivo y el acto final del ataque.

**Tipos de ingeniería social**

Básicamente los tipos de ingeniería social que se abordarán en este módulo de aprendizaje son 2, aquel basado en humanos y otro basado en computadores.

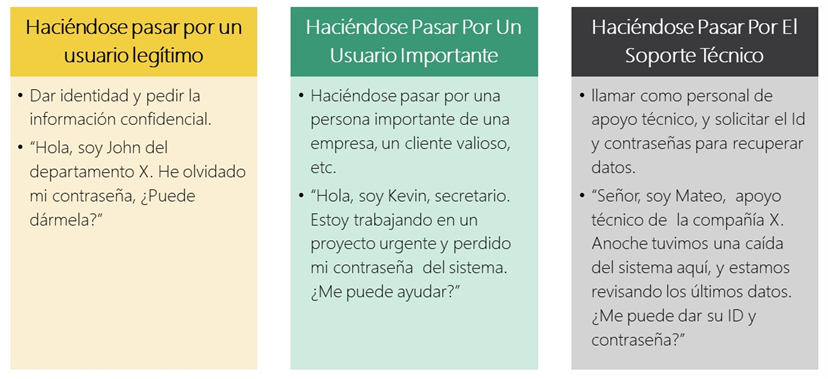
**Ataques basados en humanos:**

Suplantación de identidad: Actuar como otra persona para tener acceso a la información.

Pueden actuar como un usuario y una solicitud de información legítimos, o se hacen pasar por una autoridad superior y pueden solicitar información sensible, o se hacen pasar por una persona de apoyo técnico e intentan reunir detalles sensibles y confidenciales.

**Figura 4**

*Ataques basados en humanos*

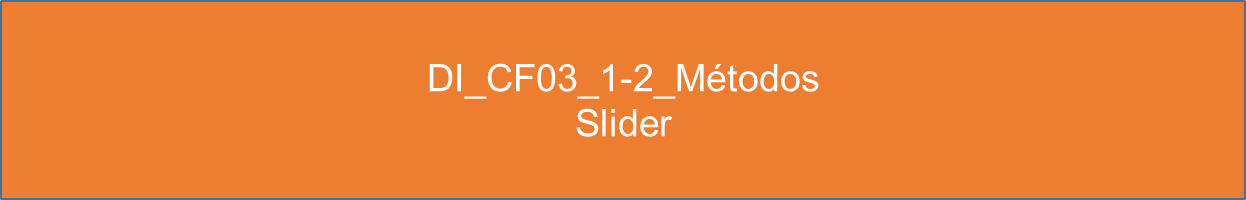




Otros tipos son los ataques basados en los seres humanos, revíselos a continuación:



Algunos de los métodos que los delincuentes usan para poder acceder a su información por medio de la ingeniería social son los siguientes:



Probablemente el ejemplo más famoso de buceo en contenedores fue realizado por Jerry Schneider en el sur de California. Mientras estaba en la escuela secundaria, en 1968, Jerry encontró documentación relativa al sistema automatizado de pedido y entrega de equipos de Pacific Telephone que se utilizaba para pedir equipos. Jerry acumuló cientos de miles de dólares en equipos telefónicos y estableció Creative Systems Enterprises para venderlos; parte de ellos se vendió a Pacific Telephone. Jerry fue arrestado en 1972 y fundó una empresa de seguridad en 1973 que dejó en 1977.

**Ataques basados en computadores:**

En los ataques más populares de ingeniería social por computadores, los ciberdelincuentes aprovechan mucho la red Internet para ejecutarlos y que las víctimas puedan caer en las trampas y engaños que estos ponen, ya que en el mundo digital de hoy es mucho más fácil acceder por estos medios. A continuación, se relacionan algunos de los ataques.

* Cartas engañosas: Estos son correos electrónicos falsos, que envían advertencias sobre *malware*, virus y gusanos, que causan daños a los ordenadores.
* Cartas en cadena: Pidiendo a la gente que reenvíe correos electrónicos o mensajes por dinero.
* Mensajes de spam: Son correos electrónicos no deseados e irrelevantes, que intentan reunir información sobre los usuarios.
* Mensajeros de chat instantáneo: Recopilar información personal de un solo usuario chateando con ellos.
* *Phishing*: Creación de un sitio web falso, clonado, que intenta reunir información sensible sobre los usuarios. Se puede hacer enviando un correo electrónico falso, como si viniera de un sitio web original, y luego tratando de recopilar información confidencial. El *phishing* también puede ejecutarse a través de aplicaciones móviles falsas. Revise el **Anexo\_ Phishing**, el cual profundiza sobre este aspecto.

Otros métodos utilizados son las ventanas emergentes o llamados comúnmente como *popups*; engañan a los usuarios para que hagan clic en un hipervínculo que los redirige a la página web de un atacante, pidiéndoles que den su información personal o que descarguen *software* que podría tener virus adjuntos en el *backend*; revíselos a continuación.

**Figura 5**

*Otros métodos*



* 1. **Riesgos de suplantación (redes sociales)**

No importa cuán seguro sea un sistema, siempre hay una forma de entrar; los piratas informáticos e ingenieros sociales malintencionados se dirigen a la parte más débil de la infraestructura, la gente, que suele ser la más fácil de manipular y engañar.

La suplantación de identidad es una de las diversas herramientas de ingeniería social que se utilizan para acceder a un sistema o red, con el fin de cometer fraude, espionaje industrial o robo de identidad. La suplantación de identidad se diferencia de otras formas de ingeniería social porque se produce en persona, en lugar de por teléfono o por correo electrónico.

**Figura 6**

*El ingeniero social*













La suplantación de identidad requiere mucha preparación, por lo que ocurre con menos frecuencia que otras formas de ingeniería social. Los ingenieros sociales prefieren el enfoque más anónimo del teléfono o el correo electrónico a aparecer en persona; sin embargo, si se hace bien, nadie sabe nunca que el imitador estuvo allí; para la gente con la que hablaban, eran solo otro individuo en un flujo continuo, aunque quizás un poco más agradable que el gruñón común y corriente.

**Los papeles del imitador**

Algunos de los papeles comunes que se pueden desempeñar en los ataques de suplantación de identidad son: 



Estos trucos funcionan porque todos interactúan regularmente con personas que no conocen. Es la naturaleza humana confiar en las credenciales - una placa o un uniforme - pero pueden ser falsificadas. Se confía en los uniformes, aunque se sabe que cualquiera puede usarlos y cuando se visita un sitio web, por ejemplo, se usa la apariencia profesional de la página para juzgar si es realmente legítima o no, sin importar que cualquiera pueda cortar y pegar gráficos de la misma manera. Tenemos la tendencia a confiar automáticamente en alguien con autoridad.

**Algunas funciones comunes de ingeniería social son:**

**Figura 7**

*Algunas funciones comunes de la ingeniería social*

**Los imitadores hacen sus deberes**: La suplantación funciona mejor cuando el ingeniero social da una actuación convincente, completa con la jerga técnica adecuada u otra información privilegiada. Los imitadores hacen sus deberes, vienen armados con:

* Un uniforme
* Una placa de identificación
* Una tarjeta de negocios falsa o falsificada
* Información privilegiada
* Nombres y detalles sobre los empleados

En el siguiente gráfico, podrá observar el riesgo de las redes sociales en las redes corporativas:

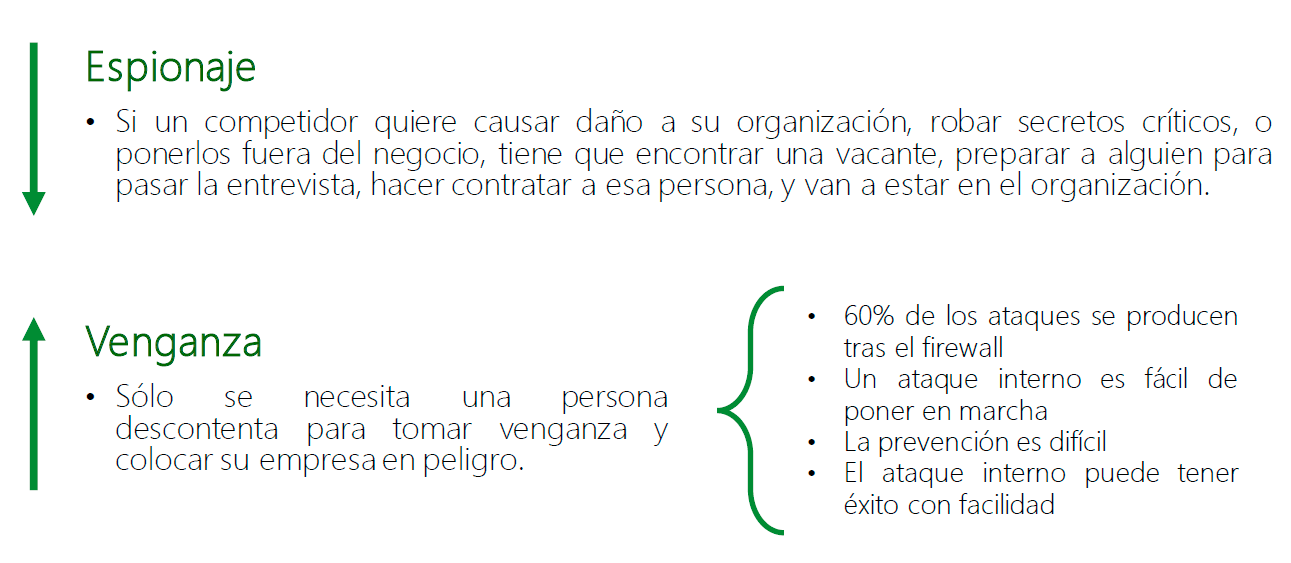
**Figura 8**

*Riesgo de las redes sociales en las redes corporativas*



* 1. **Ataques y riesgos (vulnerabilidades)**

Una amenaza interna es un riesgo para la seguridad que se origina dentro de la organización objetivo. Suele consistir en que un empleado o socio comercial actual o anterior tenga acceso a información confidencial o a cuentas privilegiadas dentro de la red de una organización, y que haga un uso indebido de ese acceso.



Las medidas de seguridad tradicionales tienden a centrarse en las amenazas externas y no siempre son capaces de identificar una amenaza que emana del interior de la organización.

Los tipos de amenazas internas incluyen:

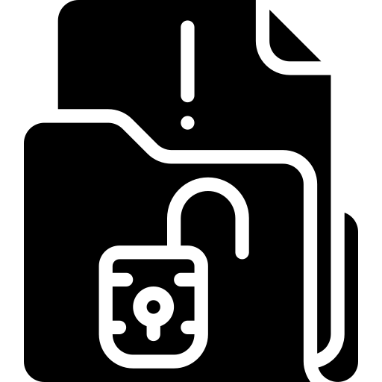
* Información privilegiada maliciosa: también conocida como *Turncloak*, alguien que maliciosa e intencionalmente abusa de las credenciales legítimas, típicamente para robar información para obtener incentivos financieros o personales. Por ejemplo, un individuo que guarda rencor a un antiguo empleador, o un empleado oportunista que vende información secreta a un competidor. Los *turncloaks* tienen una ventaja sobre otros atacantes, porque están familiarizados con las políticas y procedimientos de seguridad de una organización, así como con sus vulnerabilidades.
* Descuidado desde dentro: un peón inocente que, sin saberlo, expone el sistema a amenazas externas. Este es el tipo más común de amenaza interna, resultante de errores, como dejar un dispositivo expuesto o ser víctima de una estafa. Por ejemplo, un empleado que no tiene intención de hacer daño puede hacer clic en un enlace inseguro, infectando el sistema con *malware*.
* Un topo: un impostor, que es técnicamente un extraño, pero que ha logrado obtener acceso interno a una red privilegiada. Se trata de alguien de fuera de la organización que se hace pasar por empleado o socio.

**Prevención de amenazas internas**

Puede tomar las siguientes medidas para ayudar a reducir el riesgo de amenazas internas:



































Las amenazas internas pueden ser más difíciles de identificar o prevenir que los ataques externos, y son invisibles para las soluciones de seguridad tradicionales, como los cortafuegos y los sistemas de detección de intrusos, que se centran en las amenazas externas. Si un atacante explota un inicio de sesión autorizado, los mecanismos de seguridad establecidos pueden no identificar el comportamiento anormal, además, los iniciados maliciosos pueden evitar más fácilmente la detección si están familiarizados con las medidas de seguridad de una organización. Se recomienda realizar lo siguiente:



Existen herramientas como las aplicaciones de aprendizaje automático (ML) que ayudan a analizar el flujo de datos y a priorizar las alertas más relevantes. Se pueden utilizar herramientas digitales forenses y analíticas, como User and Event Behavior Analytics (UEBA), para detectar, analizar y alertar al equipo de seguridad sobre cualquier posible amenaza interna; el análisis del comportamiento de los usuarios puede establecer una línea de base para la actividad normal de acceso a los datos, mientras que la supervisión de la actividad de la base de datos puede ayudar a identificar las violaciones de las políticas. A continuación, se pueden revisar en la tabla las tácticas y estrategias según el área de riesgo.

**Tabla 1**

*Áreas de riesgo, tácticas y estrategias*

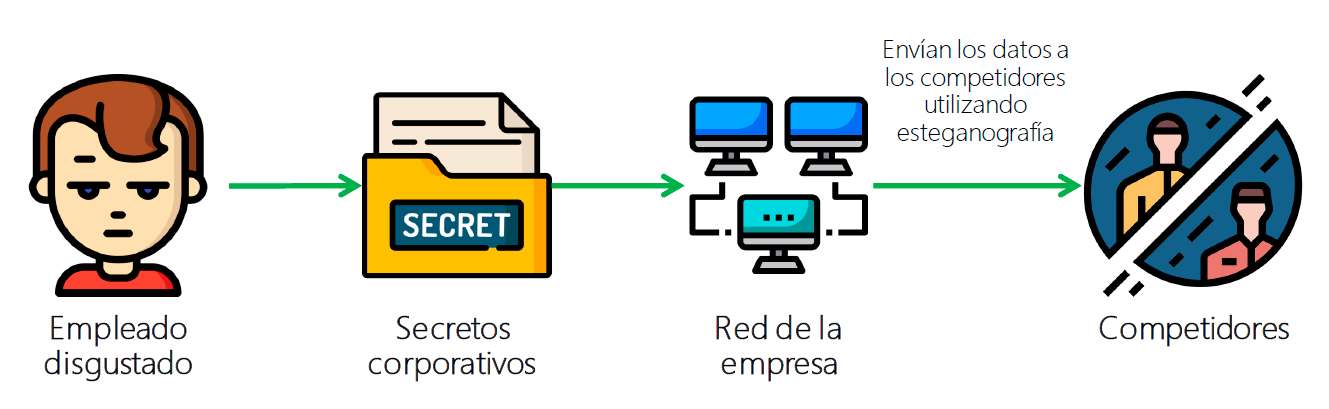
| ÁREA DE RIESGO | TÁCTICA DE ATAQUE | ESTRATEGIA DE COMBATE |
| --- | --- | --- |
| Teléfono (punto de ayuda) | Suplantación y persuasión. | Capacitar a los empleados los ayuda a no revelar contraseñas u otra información por teléfono. |
| Entrada del edificio | Acceso físico no autorizado. | Implementar fuertes medidas de seguridad y formación de los empleados y funcionarios de seguridad. |
| Oficina | *Shoulder surfing.* | No escribir las contraseñas con nadie más presente (o si tiene que hacerlo, hágalo rápidamente). |
| Teléfono (punto de ayuda) | La suplantación de llamadas al servicio técnico. | Asignar un PIN a todos los empleados de servicios de asistencia. |
| Oficina | Paseando por los pasillos en busca de la oficina abierta. | Escoltar a todos los visitantes. |
| Sala de correo | Inserción de notas falsificadas. | Bloquear y supervisar la sala de correo. |
| Sala de máquinas/ Armario telefónico | Intentar acceder, retirar los equipos y o adjuntar un analizador de protocolos para tomar los datos confidenciales. | Mantener closets telefónicos, salas de servidores, etc., bloqueados en todo momento y mantener el inventario actualizado de equipos. |
| Teléfono y PBX | Robar punto de acceso telefónico. | Controlar las llamadas internacionales y de larga distancia, llamadas de seguimiento, o denegar transferencias. |

La mayoría de casos de abuso de información privilegiada se pueden atribuir a los individuos que son

introvertidos, incapaces de lidiar con el estrés o conflicto y frustrados con su trabajo, las políticas de la oficina y la falta de respeto entre otros; los empleados disgustados pueden pasar secretos de la empresa y la propiedad intelectual a los competidores por beneficios propios.

**Figura 9**

*Secretos corporativos*



* 1. ***Pentesting***

Las pruebas de penetración de la ingeniería social se centran en las personas y los procesos y las vulnerabilidades asociadas a ellos, estas pruebas de penetración consisten típicamente en que un hacker ético lleva a cabo diferentes ataques de ingeniería social, como el *phishing*, las caídas de USB, o la suplantación de identidad que una persona podría enfrentar en el curso de su trabajo, el objetivo de esta prueba es identificar las debilidades de una persona, grupo de personas o proceso, e identificar las vulnerabilidades con un camino claro para remediarlas.

Hay cuatro pasos principales para realizar una prueba de penetración de ingeniería social que incluyen la planificación y el alcance de la prueba, la identificación del vector de ataque, los intentos de penetración y la presentación de informes.

* Paso 1: Planificación y alcance de la prueba

Este paso es el más importante durante la prueba de penetración. Durante este paso, identificará lo que está en el alcance y cómo se realizará la prueba; esto normalmente requiere una reunión entre la dirección y el personal que realiza la prueba. Una cosa que hay que tener en cuenta es que se quiere mantener el número de personas involucradas en esta reunión al mínimo, para evitar el número de personas que saben de la prueba.

* Paso 2: Identificación del vector de ataque

Después de que haya hecho la prueba del bolígrafo, debe tener un contrato claramente definido sobre qué y a quién se puede hacer la prueba; este paso de la prueba del bolígrafo implicará que el probador identifique todos los métodos que utilizará durante la prueba.

* Paso 3: Intentos de penetración

Durante este paso de la prueba del bolígrafo, el probador tomará todos los vectores de ataque listados en el paso anterior y ejecutará esas pruebas; la documentación es clave en este paso, ya que estas pruebas se convertirán más tarde en pruebas de apoyo para el informe.

El tipo de pruebas que debe recoger es:

* Llamadas telefónicas grabadas: Estas llamadas telefónicas son importantes, ya que no hay otro método para documentar que este ataque ocurrió, así como para mostrar su resultado.
* Correos electrónicos de los ataques de *phishing*: Estos correos electrónicos son importantes porque pueden mostrar hasta dónde un usuario permitió el ataque antes de atraparlo. En algunos casos, los usuarios no se dan cuenta hasta después de haber entregado información sensible.
* Documentación encontrada durante el *dumpster diving*. Este tipo de documentación debe incluir escaneos de los documentos encontrados e incluso imágenes del lugar donde se encontraron los documentos, si es apropiado. Junto con las pruebas, el examinador debe incluir la hora de inicio y final de cada prueba, el nombre de la persona que realiza la prueba y el nombre del empleado o empleados que están siendo examinados.

* Paso 4: Presentación de informes

El paso de informe de una prueba de bolígrafo es donde se juntan todos los resultados. Mientras escribe el informe, recuerde quién es su público, en la mayoría de los casos, la audiencia es la alta dirección y su informe debe hablar con ellos. Asegúrese de abordar todas las preocupaciones discutidas al inicio de la prueba, así como todas las vulnerabilidades que encontró durante la prueba, en el informe, no solo debe mencionar las vulnerabilidades encontradas, sino que también debe proporcionar recomendaciones sobre cómo mitigar las vulnerabilidades.

1. **Denegación de servicios**

Seguramente ha escuchado dentro del *hacking* ético que una de las formas más comunes de ataque es poder restringir servicios a una organización, saturarlos para que estos dejen de funcionar y se genere un colapso y volcamiento de información, ya que buscan primordialmente dejar inhabilitado al usuario para que pueda hacer uso y consumo de todos los servicios que se puedan proveer, estos por lo general son realizados por algoritmos cíclicos y repetitivos donde se hacen peticiones infinitas, desbordando la capacidad del sistema y generando bloqueos.

* 1. **Conceptos y generalidades**

En el siguiente gráfico, puede revisar el concepto de ataque de denegación de servicio.

**Figura 10**

*Ataque de denegación de servicio*















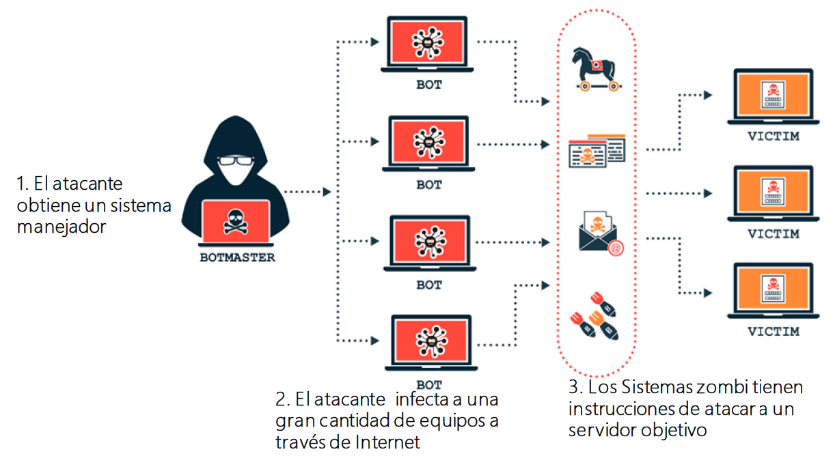








Un tipo adicional de ataque DoS es el **ataque de Negación de Servicio Distribuido (DDoS)**, este se produce cuando varios sistemas orquestan un ataque DoS sincronizado a un solo objetivo, la diferencia esencial es que, en lugar de ser atacado desde un lugar, el objetivo es atacado desde varios lugares a la vez. La distribución de *hosts* que define un DDoS proporciona al atacante múltiples ventajas:

* Puede aprovechar el mayor volumen de la máquina para ejecutar un ataque gravemente perturbador.
* La ubicación del ataque es difícil de detectar debido a la distribución aleatoria de los sistemas de ataque (a menudo en todo el mundo).
* Es más difícil apagar varias máquinas que una sola.
* El verdadero grupo atacante es muy difícil de identificar, ya que están disfrazados detrás de muchos sistemas (en su mayoría comprometidos).

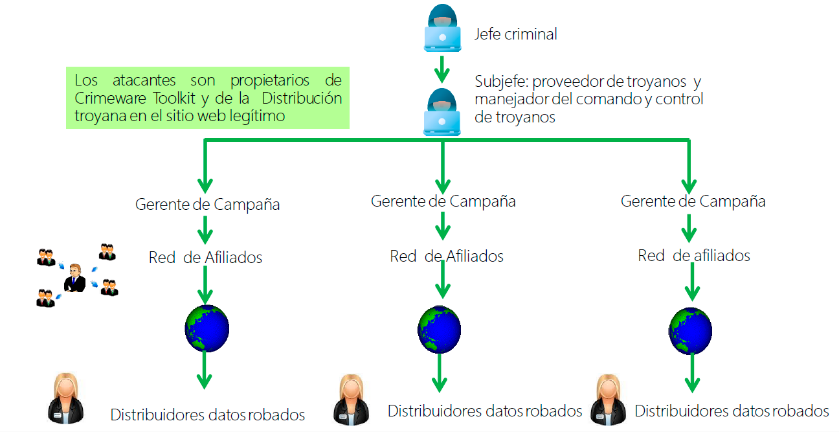
Hay dos métodos generales de ataques de DoS: servicios de inundación o servicios de choque.

Los ataques por inundación se producen cuando el sistema recibe demasiado tráfico para que el servidor almacene en el búfer, lo que hace que se ralentice y finalmente se detenga. Los ataques por inundación más comunes incluyen:

* Ataques de desbordamiento de búfer: El ataque DoS más común. El concepto es enviar más tráfico a una dirección de red de lo que los programadores han construido el sistema para manejar. Incluye los ataques que se enumeran a continuación, además de otros que están diseñados para explotar errores específicos de ciertas aplicaciones o redes
* Inundación de ICMP: Aprovecha los dispositivos de red mal configurados, enviando paquetes falsos que hacen *ping* a todos los ordenadores de la red objetivo, en lugar de solo a uno en concreto. La red se activa entonces para amplificar el tráfico. Este ataque también se conoce como el ataque pitufo o *ping* de la muerte.
* SYN flood: Envía una solicitud para conectarse a un servidor, pero nunca completa el apretón de manos. Continúa hasta que todos los puertos abiertos están saturados de solicitudes y ninguno está disponible para que los usuarios legítimos se conecten.

Otros ataques DoS simplemente explotan las vulnerabilidades que causan que el sistema o servicio objetivo se caiga; en estos ataques, se envían entradas que aprovechan los errores del objetivo, que posteriormente se bloquean o desestabilizan gravemente el sistema, de modo que no se puede acceder a él o utilizarlo.

**Denegación de servicio distribuido**

Un ataque de denegación de servicio distribuido (DDoS) se produce cuando varias máquinas operan juntas para atacar a un objetivo. Los atacantes DDoS a menudo aprovechan el uso de una red de robots, un grupo de dispositivos secuestrados conectados a Internet, para llevar a cabo ataques a gran escala. Los atacantes aprovechan las vulnerabilidades de seguridad o las debilidades de los dispositivos para controlar numerosos dispositivos mediante *software* de mando y control. Una vez que tiene el control, un atacante puede ordenar a su red de robots que realice DDoS en un objetivo. En este caso, los dispositivos infectados también son víctimas del ataque. Revise el siguiente recurso, donde se explica con mayor detalle.

Desafortunadamente, derribar a cualquiera de los miembros del equipo que se describen en el video no necesariamente compromete a toda la red criminal. Por un lado, los ciberdelincuentes a menudo prefieren dar y recibir compensación en forma de criptodivisas irrastreables, como *Bitcoin*. Esto elimina efectivamente los "rastros de papel" que han deshecho las organizaciones criminales en el pasado.

Además, los ciberdelincuentes se cuidan de compartir únicamente información incriminatoria en la Web profunda (un término que se refiere a todo el contenido en línea que no está indexado por los motores de búsqueda tradicionales), donde el anonimato es fácil de conseguir. Muchas redes de delincuentes cibernéticos "subcontratan" diversas funciones a personas anónimas que encuentran en estos rincones "ocultos" de la Internet, lo que reduce en gran medida la probabilidad de que una persona sepa lo suficiente como para perjudicar a otros miembros del equipo.

* 1. **Herramientas y técnicas de ataque**

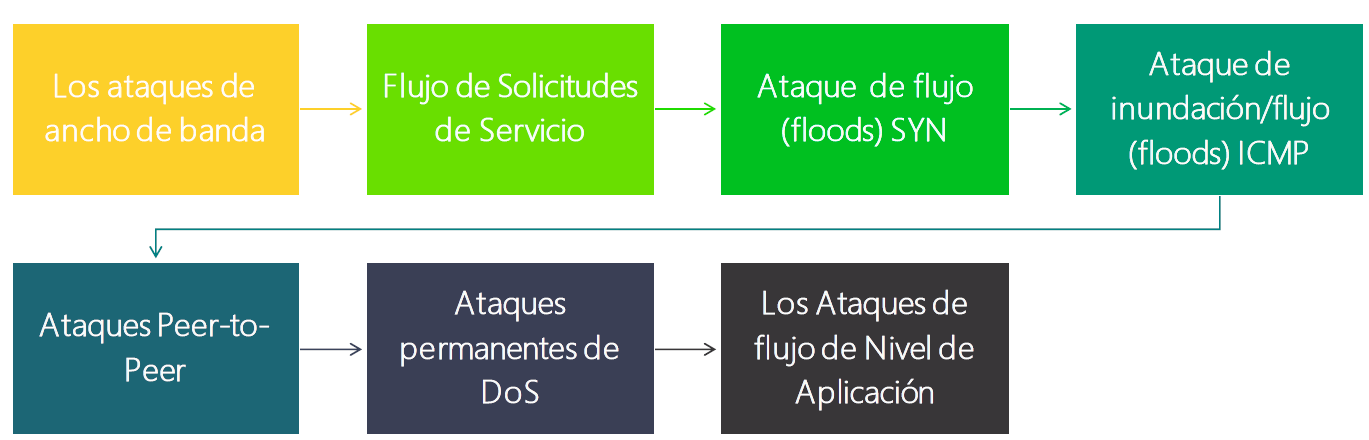
Aunque los DDoS ofrecen un modo de ataque menos complicado que otras formas de ciberataques, son cada vez más fuertes y sofisticados. Hay tres categorías básicas de ataque:

* Los ataques basados en el volumen, que utilizan un gran tráfico para inundar el ancho de banda de la red.
* Ataques de protocolo, que se centran en la explotación de los recursos del servidor.
* Ataques a aplicaciones, que se centran en las aplicaciones web y se consideran el tipo de ataque más sofisticado y grave.

Los diferentes tipos de ataques se clasifican en categorías basadas en la cantidad de tráfico y las vulnerabilidades a las que se dirigen, como se muestra en el siguiente gráfico.

**Figura 11**

*Tipos de ataques*

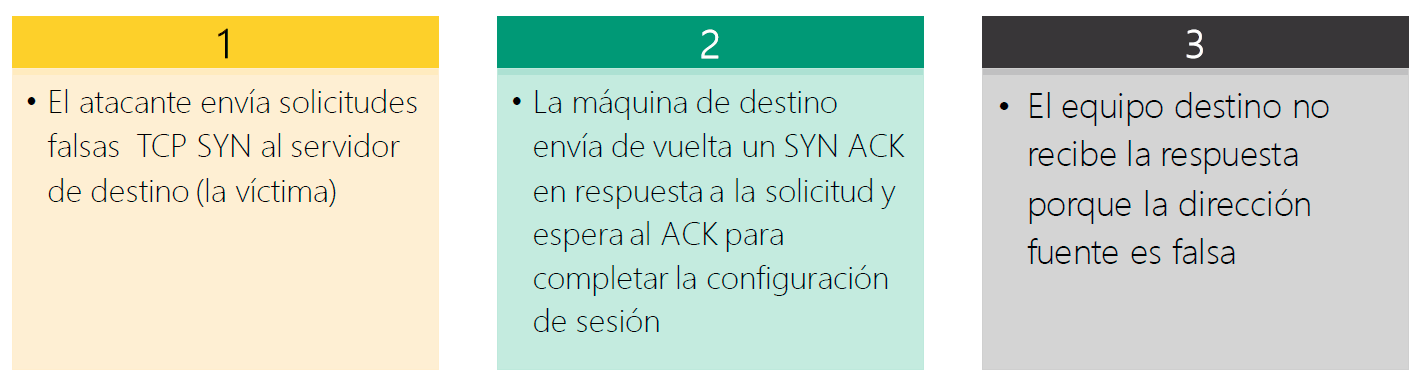


* **Inundación SYN**

SYN Flood explota las debilidades de la secuencia de conexión TCP, conocida como un apretón de manos de tres vías, la máquina anfitriona recibe un mensaje sincronizado (SYN) para iniciar el "*handshake*". El servidor reconoce el mensaje enviando un indicador de reconocimiento (ACK) al host inicial, que luego cierra la conexión; en una inundación SYN, sin embargo, se envían mensajes falsos y la conexión no se cierra, cerrando el servicio.

**Figura 12**

*Inundación SYN*



Los ataques de inundación SYN funcionan explotando el proceso de apretón de manos de una conexión TCP; en condiciones normales, la conexión TCP muestra tres procesos distintos para realizar una conexión.

* En primer lugar, el cliente envía un paquete SYN al servidor para iniciar la conexión.
* El servidor responde a ese paquete inicial con un paquete SYN/ACK, con el fin de reconocer la comunicación.
* Finalmente, el cliente devuelve un paquete ACK para acusar recibo del paquete del servidor.



* **SYN Flooding**

Un SYN Flood ocurre cuando la capa TCP está saturada, impidiendo que se complete el triple apretón de manos TCP entre el cliente y el servidor en cada puerto. Cada conexión que utiliza el protocolo TCP requiere el triple apretón de manos, que es un conjunto de mensajes intercambiados entre el cliente y el servidor, como se muestra a continuación.

**Figura 13**

*Protocolo TCP*



El propósito de este intercambio es validar la autenticidad de cada parte y establecer la clave de cifrado y las opciones que asegurarán las comunicaciones posteriores. Este proceso debe completarse antes de que un puerto de comunicaciones entre el cliente y el servidor pueda abrirse y estar disponible en su totalidad.

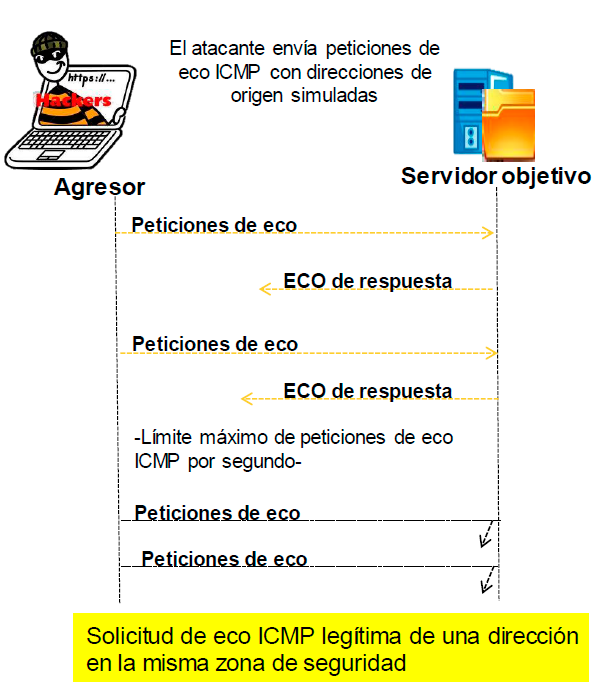


* **ICMP Flood Attack**

Un ataque por inundación con el Protocolo de Mensajes de Control de Internet (ICMP), también conocido como ataque por inundación Ping, es un ataque común de denegación de servicio (DoS) en el que un atacante intenta abrumar un dispositivo objetivo con peticiones de eco (pings) ICMP. Normalmente, los mensajes de solicitud de eco y respuesta de ICMP se utilizan para hacer ping a un dispositivo de red, con el fin de diagnosticar la salud y la conectividad del dispositivo y la conexión entre el remitente y el dispositivo. Al inundar el objetivo con paquetes de solicitud, la red se ve obligada a responder con un número igual de paquetes de respuesta. Esto hace que el objetivo se vuelva inaccesible para el tráfico normal.

**Figura 14**

*ICMP*



Otros tipos de ataques de petición ICMP pueden implicar herramientas o códigos personalizados, como *hping* y *scapy*. El tráfico de ataque que emana de múltiples dispositivos se considera un ataque de denegación de servicio distribuido (DDoS). En este tipo de ataque, tanto los canales de entrada como de salida de la red son abrumadores, consumen un ancho de banda considerable y dan lugar a una denegación de servicio.

* **Ataques de *peer to peer***

Los ataques entre pares explotan el tejido de la tecnología de pares para realizar los ataques. Estos ataques se distinguen de otros tipos de ataques por lo siguiente:

* El atacante no tiene que comunicarse con los clientes para la subversión y
* La naturaleza automatizada de la tecnología *peer-to-peer* puede permitir BOT como la amplificación de un ataque con el permiso de la víctima.

**Figura 15**

*Los ataques Phlashing*



















Contra estos ataques, existen herramientas de análisis, como **NetFlow Analyzer**, es una completa herramienta de análisis de tráfico, que aprovecha las tecnologías de flujo para proporcionar una visibilidad en tiempo real del rendimiento del ancho de banda de la red. A continuación, se presentan sus características.

**Figura 16**

*NetFlow Analyzer*





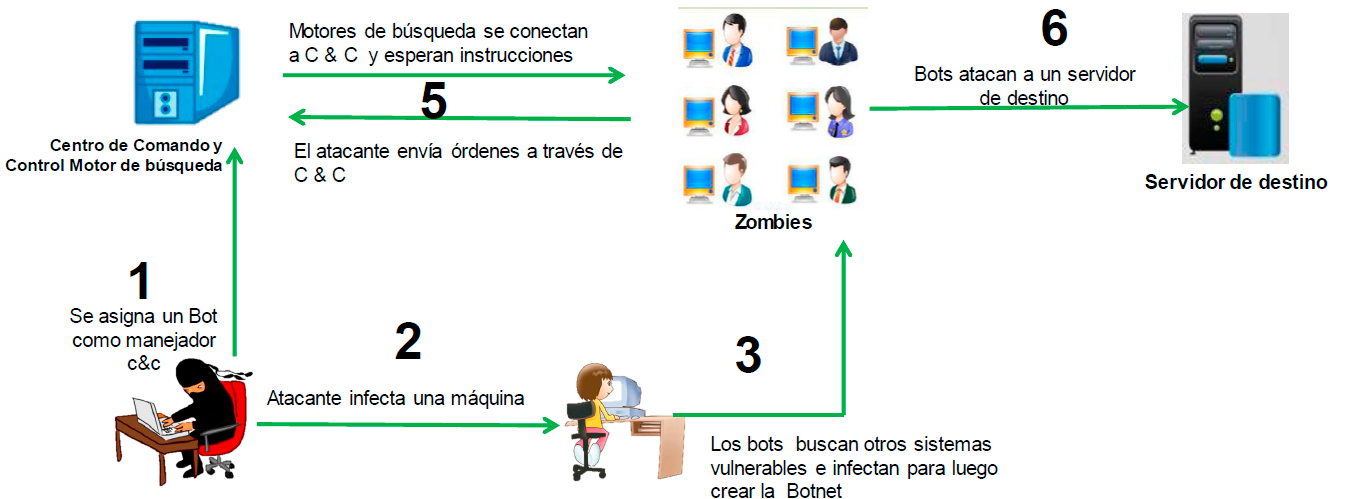


* 1. ***Botnets***

Los *botnets* se han convertido en una de las mayores amenazas para los sistemas de seguridad hoy en día. Su creciente popularidad entre los ciberdelincuentes se debe a su capacidad para infiltrarse en casi cualquier dispositivo conectado a Internet, desde reproductores de DVR hasta *mainframes* corporativos. Para mayor información, consulte el **Anexo\_ Bots**

**Figura 17**

*Botnets*



* 1. **Contramedidas**

La detección de DDoS es el proceso de distinguir los ataques de denegación de servicio distribuidos (DDoS) del tráfico normal de la red, a fin de realizar una mitigación efectiva de los ataques; el objetivo principal de un ataque DDoS es limitar el acceso a una aplicación o a un servicio de red, negando así a los usuarios legítimos el acceso a los servicios.

Hay muchos tipos de esquemas de ataque DDoS que se utilizan hoy en día y cada vez son más sofisticados, sin embargo, su objetivo común es sobrecargar los recursos de red específicos con tráfico o solicitudes de servicio de muchas fuentes diferentes, potencialmente cientos de miles o más; esto hace efectivamente imposible detener el ataque simplemente identificando y bloqueando una sola dirección IP, la mera distribución de las fuentes atacantes también hace muy difícil distinguir el tráfico legítimo de los usuarios del tráfico de ataque cuando se extiende por tantos puntos de origen.

**Figura 18**

*Detección de DDoS*







**Detección de DDoS**: Mejorar la precisión usando Big Data.

La primera generación de soluciones de detección de DDoS fuera de banda se basó en el diseño de software de un solo servidor, que en su mayoría se ejecutaba en dispositivos de servidor independientes montados en bastidor.

Aunque es mucho mejor que nada, los servidores individuales simplemente no tienen los recursos de computación, memoria y almacenamiento para rastrear grandes volúmenes de datos de tráfico en toda la red, esto es particularmente cierto cuando se intenta realizar una línea de base dinámica, lo que requiere escanear una cantidad masiva de datos de flujo para comprender lo que es normal, y luego mirar hacia atrás días o semanas para evaluar si las condiciones actuales constituyen una anomalía. Independientemente de que se despliegue en las instalaciones o en la nube, la detección de DDoS en un solo servidor es insuficiente para detectar con precisión los ataques actuales de una forma fiable y constante.

Al aprovechar las tecnologías de Big Data para almacenar los eventos de la red a medida que suceden y al acceder a este repositorio de datos en la nube, los clientes pueden evitar los dispositivos de detección de DDoS que no logran escalar a medida que sus redes *in situ* crecen y/o se vuelven a desplegar en la nube, o evitar los costosos proyectos internos que requieren inversiones continuas u obsoletas a medida que cambian los marcos de *software* abierto.

Las contramedidas para los ataques DoS y DDoS son:

* + Sistemas de Detección de Intrusos (IDS) y un Sistema de Protección de Intrusos (IPS).
  + Fuertes programas antivirus y anti-spyware en todos los sistemas con conectividad a Internet.
  + *Hashes* de archivos y carpetas en los archivos y carpetas del sistema, para identificar si han sido comprometidos.

1. **Detección y evasión de intrusos**

Es importante tener en cuenta que, dentro de un sistema en una organización, los sistemas y la información deben ser protegidos y reconocidos, para poder evitar que los piratas informáticos puedan ingresar archivos de *malware* y realizar daños en la estructura de datos, y así robar o secuestrar información. Estas técnicas de detección y evasión de intrusos hoy cuentan con herramientas para detectar intrusiones y aplicar los correctivos necesarios y salvaguardar la integridad de toda la información.

* 1. **Conceptos y generalidades**

Un sistema de detección de intrusos (IDS) es un dispositivo o aplicación de *software* que monitoriza una red en busca de actividades maliciosas o violaciones de la política. Por lo general, cualquier actividad maliciosa o violación se notifica o se recopila de forma centralizada, mediante un sistema de gestión de información y eventos de seguridad. Algunos IDS son capaces de responder a la intrusión detectada al ser descubierta; estos se clasifican como sistemas de prevención de intrusiones (IPS). Existen tres formas para detectar una intrusión.

**Figura 19**

*Formas de detectar una intrusión*















* 1. **Tipos de IDS**

Hay una amplia gama de IDS, que van desde *software* antivirus hasta sistemas de monitorización por niveles que siguen el tráfico de toda una red. Las clasificaciones más comunes son:

* Sistemas de detección de intrusos en la red (NIDS): Un sistema que analiza el tráfico entrante de la red; estos mecanismos consisten normalmente en una caja negra que se sitúa en la red en modo promiscuo, atento a los patrones indicativos de una intrusión
* Sistemas de detección de intrusos basados en host (HIDS): Un sistema que monitoriza los archivos importantes del sistema operativo, estos mecanismos suelen incluir la auditoría de eventos que ocurren en un host específico; estos no son tan comunes, debido a la sobrecarga en que incurren por tener que monitorear cada evento del sistema.
* Supervisión de archivos de inicio de sesión: Estos mecanismos suelen ser programas que analizan los archivos de registro después de un evento que ya ha ocurrido, como los intentos fallidos de conexión.
* Comprobación de integridad de archivos: Estos mecanismos de verificación son para los caballos de Troya, o archivos que de otra forma se han modificado, lo que indica que un intruso ya ha estado allí, por ejemplo, TRIPWIRE



La primera vez que se ejecuta Tripwire, almacena sumas de control, tamaños exactos y otros datos de todos los archivos seleccionados en una base de datos; las ejecuciones sucesivas comprueban si cada archivo sigue coincidiendo con la información de la base de datos e informan de todos los cambios. Tripwire fue lanzado inicialmente en 1992. Hoy en día, varios programas comparten este nombre, uno es GPL y dos son propietarios.

El enfoque general para la detección de intrusiones es:

* Observe sus sistemas, redes y actividades de usuario para cualquier cosa inusual.
* Investigue cualquier cosa que encuentre inusual.
* Si su investigación encuentra algo que no está explicado por las actividades autorizadas, inicie inmediatamente sus procedimientos de respuesta a la intrusión.

Aunque este proceso parece bastante simple, su implementación es una actividad que requiere recursos intensivos y un apoyo continuo y automatizado, así como un esfuerzo administrativo diario. Además, la escala de las prácticas de detección de intrusos puede necesitar cambiar, como amenazas, configuraciones del sistema o requisitos de seguridad.

En todos los casos, hay cinco áreas que deben ser abordadas:

**Figura 20**

*Áreas*





* 1. ***Firewall* y *Honeypot***

A continuación, se abordan estos dos términos importantes en la seguridad informática.

* **Firewall**

Un cortafuegos es un dispositivo de seguridad de red que monitoriza el tráfico de red entrante y saliente y decide si permite o bloquea un tráfico específico basándose en un conjunto definido de reglas de seguridad.

Los cortafuegos han sido la primera línea de defensa en la seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas aseguradas y controladas, que pueden ser confiables, y las redes externas no confiables, como la Internet.

Un cortafuegos puede ser de *hardware*, *software*, o ambos. Los tipos de cortafuegos pueden dividirse en varias categorías diferentes, según su estructura general y su método de funcionamiento. Aquí hay ocho tipos de cortafuegos:

**Figura 21**

*Tipos de cortafuegos*



















**Tipos de *firewall***

Una vez que los primeros administradores de sistemas de Internet comenzaron a entender que eran atacados con frecuencia, el cortafuegos en la red resultaba inevitable, estaba destinado a haber algún tipo de proceso que mirara el tráfico de la red en busca de señales claras de atacantes, exactamente cómo iba a funcionar esto no estaba tan claro.

Los dispositivos y servicios de cortafuegos pueden ofrecer protección más allá de la función estándar del cortafuegos, por ejemplo, proporcionando detección de intrusos, protección contra ataques de denegación de servicio y otros servicios de seguridad para proteger los servidores y otros dispositivos dentro de la red privada. Aunque algunos tipos de cortafuegos pueden funcionar como dispositivos de seguridad multifuncionales, no permita que tales ofertas distraigan de la cuestión clave: **¿Protege este cortafuegos la red privada de las amenazas externas mediante el examen de las unidades de datos del protocolo?**



Un cortafuegos de aplicación es un tipo de cortafuegos que gobierna el tráfico hacia, desde o por una aplicación o servicio. Los cortafuegos de aplicaciones, o cortafuegos de capa de aplicación, utilizan una serie de políticas configuradas para determinar si se deben bloquear o permitir las comunicaciones hacia o desde una aplicación.

Los cortafuegos tradicionales controlan el flujo de datos hacia y desde la CPU, examinando cada paquete a medida que pasa. Un cortafuegos de aplicación lo lleva más lejos, al controlar la ejecución de archivos o código por parte de aplicaciones específicas. De esta manera, incluso si un intruso entra en una red o un servidor, no puede ejecutar código malicioso.

Los cortafuegos de aplicaciones pueden ser activos o pasivos:

**Figura 22**

*Cortafuegos de aplicaciones*



Los cortafuegos de aplicaciones son generalmente actualizables de forma remota, lo que les permite prevenir vulnerabilidades recién descubiertas. Suelen estar más actualizados que el código específico centrado en la seguridad que se incluye en las aplicaciones, debido a los ciclos de desarrollo y prueba más largos que se requieren para incluir dicho código en las aplicaciones.

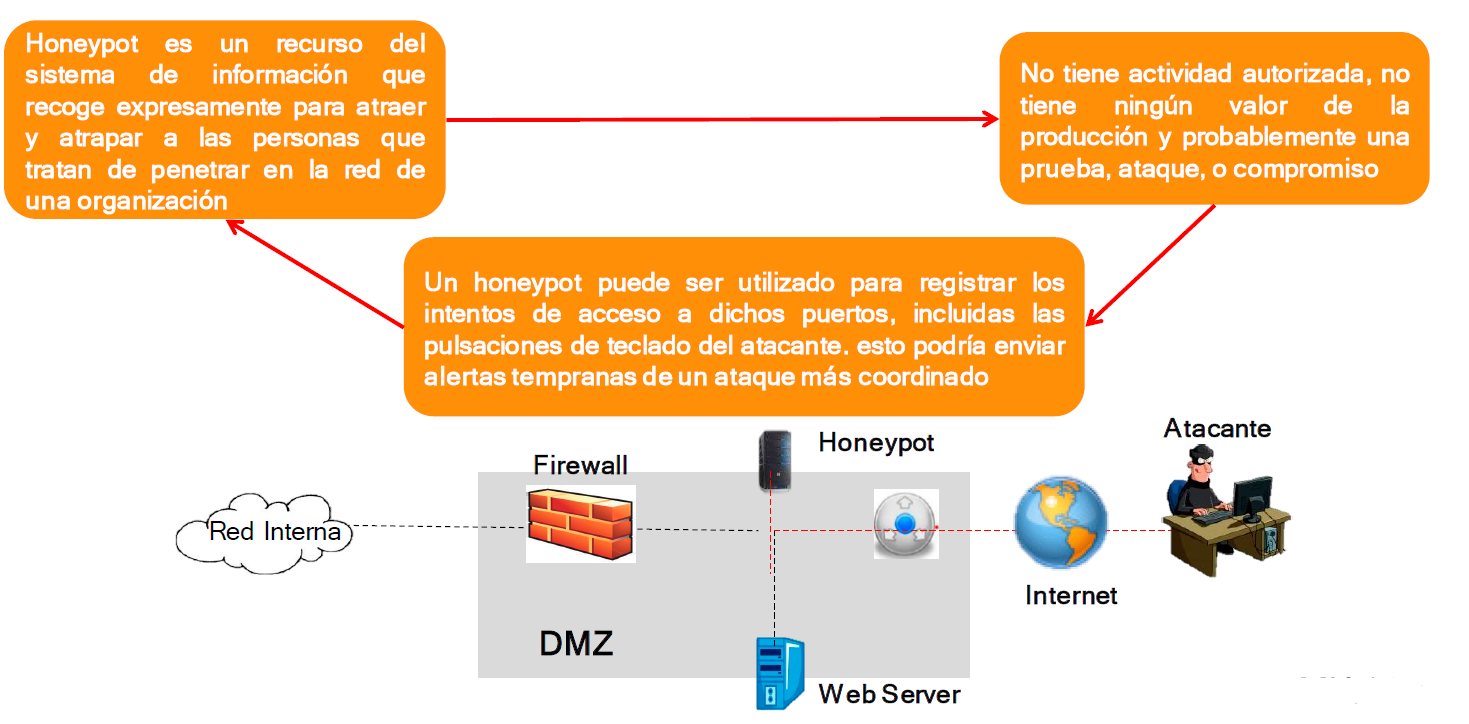
Hoy en día, lo más común es ver cortafuegos de aplicaciones web (WAF) para filtrar, monitorear y bloquear el tráfico HTTP/S hacia y desde una aplicación web, específicamente.

* ***Honeypots***

Una definición de *honeypot* viene del mundo del espionaje, donde los espías al estilo Mata Hari, que usan una relación romántica como una forma de robar secretos, son descritos como una "trampa de miel" o "honeypot". A menudo, un espía enemigo es comprometido por una trampa de miel y luego es chantajeado para entregar todo lo que sabe.

**Figura 23**

*Honeypot*



En términos de seguridad informática, un "honeypot" cibernético funciona de manera similar, poniendo un cebo para los hackers, es un sistema informático sacrificado, que pretende atraer los ciberataques, como un señuelo. Imita un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los ciberdelincuentes y la forma en que están operando o para distraerlos de otros objetivos.

**Tipos de *honeypot***

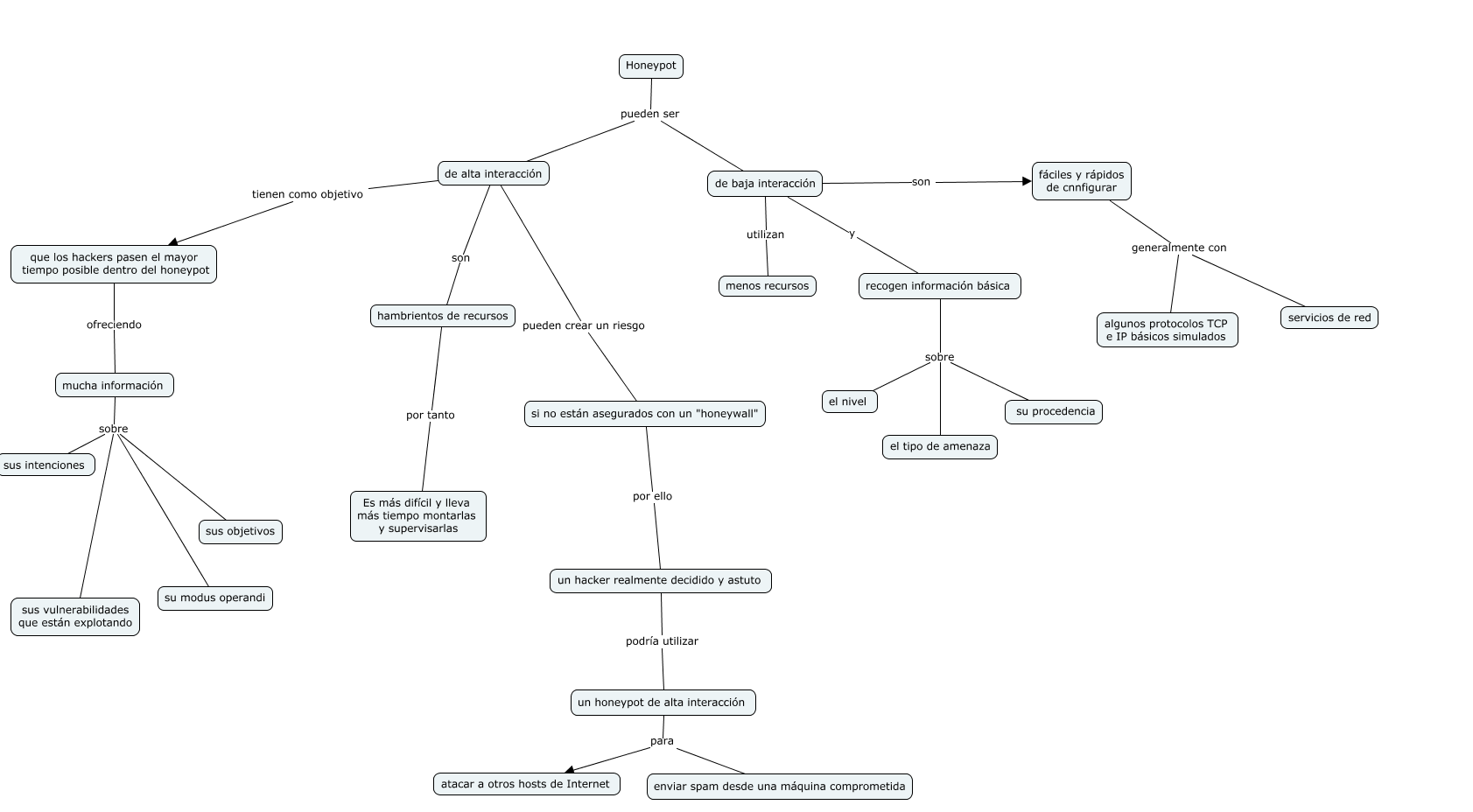
Se pueden utilizar diferentes tipos de *honeypot* para identificar diferentes tipos de amenazas, las distintas definiciones de *honeypot* se basan en el tipo de amenaza que se aborda, todas ellas tienen cabida en una estrategia de seguridad cibernética completa y eficaz.

* Las trampas de correo electrónico o de correo basura colocan una dirección de correo electrónico falsa en un lugar oculto, donde sólo un recolector de direcciones automatizado podrá encontrarla. Dado que la dirección no se utiliza para ningún otro propósito que no sea la trampa de spam, es 100% seguro que cualquier correo que llegue a ella es spam. Todos los mensajes con el mismo contenido que los enviados a la trampa de spam pueden ser bloqueados automáticamente, y la IP de origen de los remitentes puede ser añadida a una lista negra.
* Base de datos señuelo para monitorear las vulnerabilidades del *software* y detectar ataques que exploten la arquitectura insegura del sistema o que utilicen la inyección SQL, la explotación de servicios SQL o el abuso de privilegios.
* Un *honeypot* de *malware* imita las aplicaciones de *software* y las API, para invitar a los ataques de *malware*. A continuación, se pueden analizar las características del *malware* para desarrollar *software* antimalware o para cerrar las vulnerabilidades de la API.
* Un *honeypot* de araña tiene por objeto atrapar a las arañas web ("spiders"), creando páginas web y enlaces accesibles solo para las arañas. La detección de arañas puede ayudar a aprender a bloquear los *bots* maliciosos, así como las arañas de redes publicitarias.

Al monitorear el tráfico que entra al sistema de *honeypot*, se puede:

.

Revise, a continuación, otra definición de "*honeypot*":



Ambos tipos de *honeypot* tienen un lugar en la ciberseguridad de los *honeypot*. Utilizando una mezcla de ambos, se puede refinar la información básica sobre los tipos de amenazas que provienen de los *honeypots* de baja interacción, añadiendo información sobre las intenciones, comunicaciones y *exploits* del *honeypot* de alta interacción.

Al utilizar los *honeypots* cibernéticos para crear un marco de inteligencia de amenazas, una empresa puede asegurarse de que está dirigiendo su gasto en ciberseguridad a los lugares adecuados y puede ver dónde tiene puntos débiles de seguridad.

* 1. **Evasión de IDS y *firewalls***

Para luchar contra las intromisiones, hoy se dispone de diversos medios para detectarlos. Revise a continuación los posibles ataques.

* **Ataque por inserción**

Un IDS puede aceptar un paquete que un terminal rechace. Un IDS que hace esto comete el error de creer que el terminal ha aceptado y procesado el paquete, cuando en realidad no lo ha hecho. Un atacante puede explotar esta condición enviando paquetes a un terminal que este rechazará, pero que el IDS creerá que son válidos. Al hacer esto, el atacante está “insertando” datos en el IDS --- ningún otro sistema en la red se preocupa por los paquetes malos.

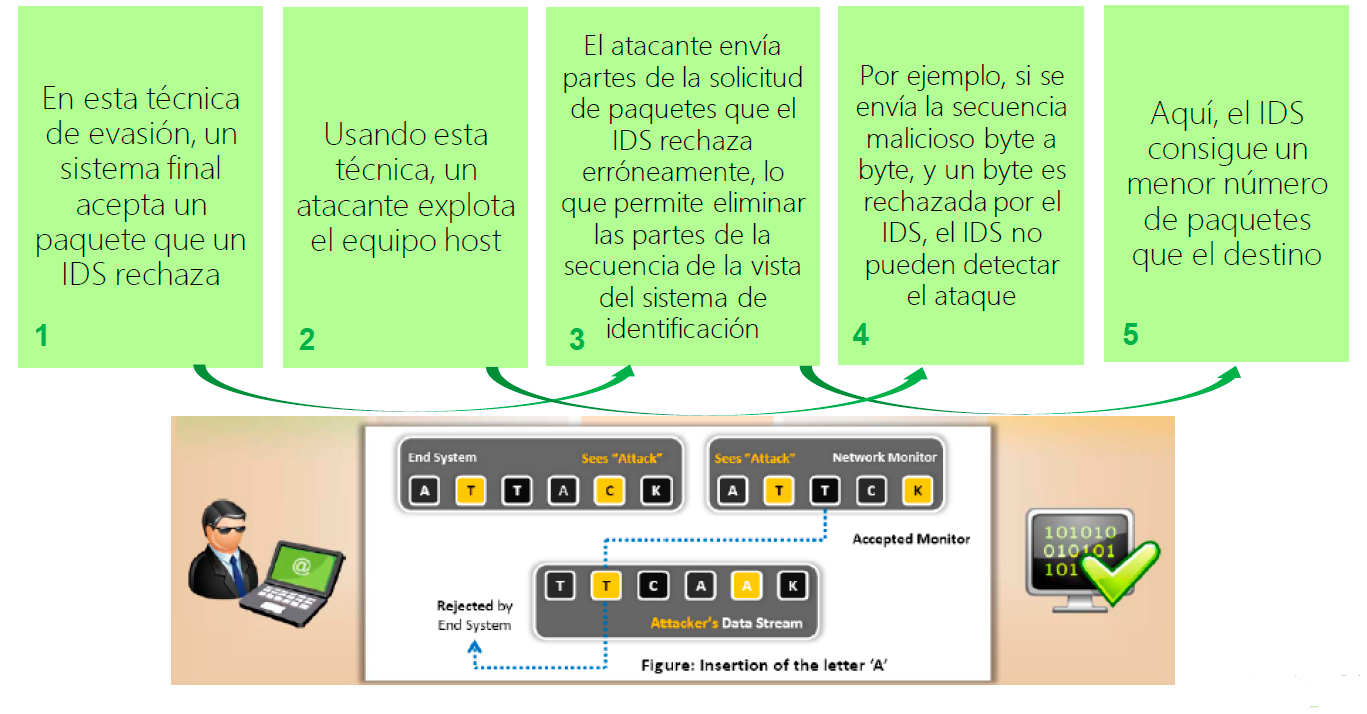
A esto se le llama un ataque de "inserción", y las condiciones que se prestan a los ataques de inserción son las vulnerabilidades más prevalentes en los sistemas de detección de intrusos que se han probado. Un atacante puede usar los ataques de inserción para derrotar el análisis de firmas, permitiéndole pasar los ataques a través de un IDS.

Para entender por qué los ataques de inserción frustran el análisis de firmas, es importante entender cómo se emplea la técnica en los sistemas de identificación reales. En su mayor parte, el "análisis de firmas" utiliza algoritmos de coincidencia de patrones para detectar una cierta cadena dentro de un flujo de datos. Por ejemplo, un IDS que trata de detectar un ataque PHF buscará la cadena “***phf”*** dentro de una petición **HTTP “GET”**, que es en sí misma una cadena más larga que podría parecerse a algo como **“GET /cgi-bin/phf?”**

El IDS puede detectar fácilmente la cadena "ff" en esa solicitud HTTP, usando una simple búsqueda de subcadena. Sin embargo, el problema se vuelve mucho más difícil de resolver cuando el atacante puede enviar la misma solicitud a un servidor web, pero obligar al IDS a ver una cadena diferente, como “GET /cgi-bin/pleasedontdetecttthisforme?”'. El atacante ha usado un ataque de inserción para añadir "Leasedontdetectt", "is" y "orme" al flujo original. El IDS ya no puede distinguir la cadena "ff" del flujo de datos que observa.

* **Ataque por evasión**

Un sistema final puede aceptar un paquete que un IDS rechaza. Un IDS que rechaza por error tal paquete pierde su contenido por completo. Esta condición también puede ser explotada, esta vez, deslizando información crucial a través del IDS en paquetes que el IDS es demasiado estricto en su procesamiento. Estos paquetes están "evadiendo" el escrutinio del IDS.



Se llama a estos ataques de "evasión", y son los más fáciles de explotar y los más devastadores para la precisión de un IDS. Sesiones enteras pueden ser llevadas a cabo en paquetes que evaden un IDS, y ataques descaradamente obvios, redactados en tales sesiones, ocurrirán justo bajo la nariz de incluso el más sofisticado motor de análisis.

Los ataques de evasión se ajustan al patrón de la lámina de aluminio de una manera muy similar a los ataques de inserción. De nuevo, el atacante hace que el IDS vea un flujo de datos diferente al del sistema final... esta vez, sin embargo, el sistema final ve más que el IDS, y la información que el IDS pierde es crítica para la detección de un ataque.

En el ataque de inserción que se menciona anteriormente, el atacante envía una petición HTTP, pero enturbia su contenido en el IDS con datos adicionales que hacen que la petición parezca inocua. En un ataque de evasión, el atacante envía porciones de la misma solicitud en paquetes que el IDS rechaza por error, permitiéndole eliminar partes del flujo de la vista del sistema de identificación. Por ejemplo, la petición original podría convertirse en “GET /gin/f”, lo que no tendría sentido para la mayoría de los sistemas de identificación.

* **Ataque por denegación de servicios**

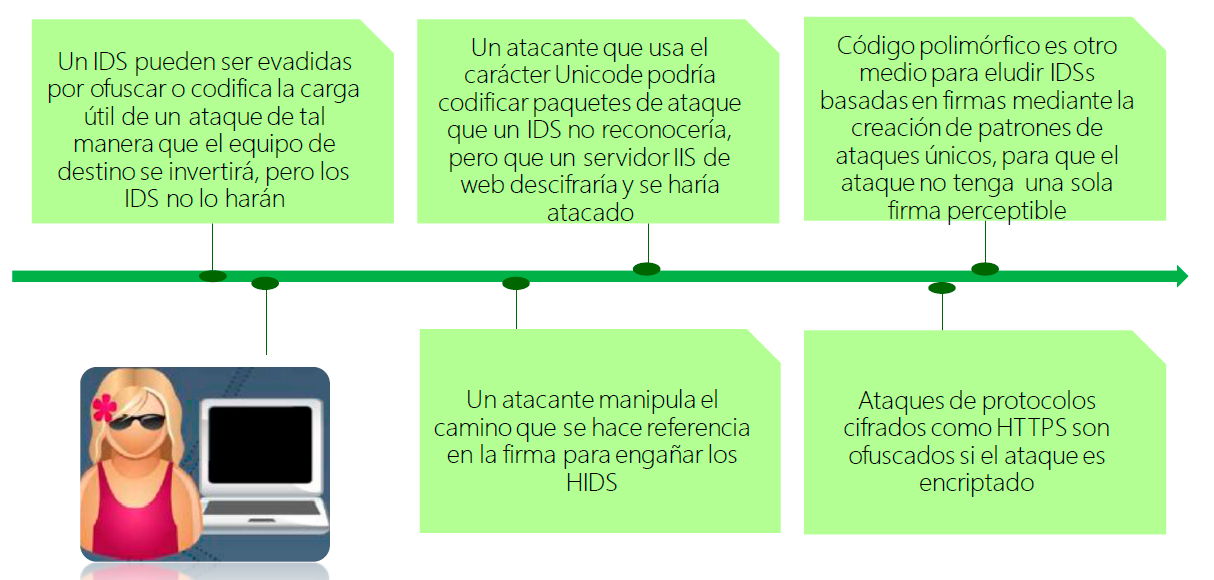
El ataque de denegación de servicio permite a los intrusos acceder a los servicios de la red, impidiendo así que los usuarios legítimos accedan a los servicios. Para superar los déficits del ataque DoS, es esencial diseñar un sistema de detección de intrusos.



El sistema de detección de intrusos (IDS) es un *software* que funciona **como un mecanismo de seguridad de la red para proteger el sistema de la red informática de los ataques**. Con el creciente número de datos que se transmiten gradualmente de una red a otra, el IDS identifica eficazmente las intrusiones en conjuntos de datos muy grandes. La minería de datos es una herramienta eficiente aplicada para perfilar el sistema de detección de intrusos y evitar que los datos de la red masiva sean accedidos por los intrusos. Los valores atípicos son patrones en los datos que no coinciden con una noción bien definida de comportamiento normal. La detección de valores atípicos tiene como objetivo encontrar patrones en los datos que no se ajustan al comportamiento esperado. Se utiliza ampliamente para desarrollar la detección de intrusos en la ciberseguridad. Este documento presenta el estudio de la técnica de detección de valores atípicos y cómo se utiliza para desarrollar el sistema de detección de intrusos para superar el ataque DoS.

* **Evasión por ofuscación**

La ofuscación, una técnica de evasión cada vez más popular, consiste en ocultar un ataque con personajes especiales. Puede utilizar caracteres de control, como el espacio, el tabulador, el retroceso y la supresión. Además, la técnica puede representar caracteres en formato hexadecimal para eludir el IDS.



El uso de la representación Unicode, en la que cada caracter tiene un valor único, independientemente de la plataforma, el programa o el idioma, también es una forma efectiva de evadir el IDS. Por ejemplo, un atacante podría evadir un IDS usando el caracter Unicode c1 para representar una barra inclinada para una solicitud de página web.

**Síntesis**



**C. Actividades didácticas**

| DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA | |
| --- | --- |
| Nombre de la Actividad | Quiz |
| Objetivo de la actividad | Apropiar conocimientos de la ingeniería social y detección y evasión de intrusos, para adquirir habilidades de *hacking* ético y evitar ataques de piratas informáticos, para salvaguardar la información. |
| Tipo de actividad sugerida | Opción múltiple |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Actividad\_didactica\_1 |

**D. Material complementario**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| Ingeniería social | LISA Institute. (2020). *Guía práctica contra la ingeniería social*. <https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social> | Artículo – Guía Práctica | <https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social> |
| Denegación de servicios | Wild IT Academy. (2020). *Ataques de Denegación de Servicio* [Video]. YouTube. <https://www.youtube.com/watch?v=c4JnYZYokJ8> | Clase Video | <https://www.youtube.com/watch?v=c4JnYZYokJ8> |
| Ataques de ingeniería social | Jimenez, J. (2021), *Tipos de ataques de ingeniería social y cómo evitarlos*. Redes Zone. <https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-ingenieria-social-consejos/> | Página Web | <https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-ingenieria-social-consejos/> |

**E. Glosario**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Activo | Componente o funcionalidad de un sistema, el cual puede ser atacado por parte de un ciberdelincuente, ya sea a nivel de *software* o de *hardware.* |
| Análisis de tráfico | Observación del comportamiento de los datos en una red por un canal de transmisión de información. |
| *Antispam* | Herramienta por la cual se infiere en las contramedidas en la contención de correos electrónicos. |
| Basura | Obtención de datos a partir de la basura de las personas o empresas, los cuales pueden brindar información relevante para un posible ataque. |
| Ciberespionaje | Actividad que tienen los hackers en el mundo digital para poder obtener información y datos sensibles, los cuales pueden obtenerse de manera pasiva o activa. |
| Falso positivo | Son *bugs* o errores que se producen cuando un sistema puede diagnosticar como actividad normal un ataque de un ciberdelincuente. |
| Ingeniería social | Técnica que se basa en engañar la conducta de una persona para que nos pueda brindar información relevante, con el fin de realizarle un ataque. |

**F. Referencias bibliográficas**

Borges, E. (2019a). *Servidor FTP*. Infranetworking. <https://blog.infranetworking.com/servidor-ftp/>.

Borges, S. (2019b). *Servidor web*. Infranetworking <https://blog.infranetworking.com/servidor-web/>.

Caballero, A. (2015). *Introducción a OSSTMM (Open Source Security Testing Methodology Manual)*. REYDES. <http://www.reydes.com/d/?q=Introduccion_a_OSSTMM_Open_Source_Security_Testing_Methodology_Manual>.

Castillo, J. (2018). *Active Directory qué es y para qué sirve*. Profesional Review. <https://www.profesionalreview.com/2018/12/15/active-directory/>.

Echeverry, J. (2009). *Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada*. Semantic Scholar.

<https://pdfs.semanticscholar.org/60c7/dbe2abab31a25422c92ead74085fd7093715.pdf>.

Gaviria, R. (2015). *Guía práctica para pruebas de pentest basada en la metodología OSSTMM V2.1 y la guía OWASP V3.0*. Universidad Libre Seccional Pereira. <https://hdl.handle.net/10901/17296>

Instituto Nacional de Ciberseguridad [INCIBE]. (2017). Amenaza vs vulnerabilidad, ¿sabes en qué se diferencian? <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>.

Jimenez, J. (2021), *Tipos de ataques de ingeniería social y cómo evitarlos*. Redes Zone. <https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-ingenieria-social-consejos/>

LISA Institute. (2020). *Guía práctica contra la ingeniería social*. <https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social>

Martinez, E. (2018). *Las diferentes amenazas de seguridad informática*. Las amenazas la informática. <https://sites.google.com/site/lasamenazaslainformatica/>.

Zuluaga, A. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia*. Universidad Nacional Abierta y a Distancia. <https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf>

**G. Control del documento**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor(es) | Pedro Javier Lozada Villota | Experto temático | Regional Cauca - Centro de Teleinformática y Producción Industrial | Noviembre de 2021 |
| Alix Cecilia Chinchilla Rueda | Diseñadora Instruccional | Regional Distrito Capital - Centro de Gestión Industrial | Noviembre de 2021 |
| Carolina Coca Salazar | Evaluador Instruccional | Regional Distrito Capital- Centro de Diseño y Metrología | Diciembre de 2021 |
| Rafael Neftalí Lizcano Reyes | Asesor pedagógico | Regional Santander - Centro Industrial del Diseño y la Manufactura | Noviembre de 2021 |
| Darío González | Corrección de estilo | Regional Tolima – Centro Agropecuario La Granja | Diciembre 2021 |

**H. Control de cambios**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del cambio |
| --- | --- | --- | --- | --- | --- |
| Autor(es) |  |  |  |  |  |