# Explicar las terminologías esenciales relacionadas con los ataques a la seguridad de la red

# Activo

Un activo puede ser cualquier cosa de interés para un atacante

Puede ser un recurso tangible o intangible de una organización con un valor monetario, que un atacante tiene como objetivo, para obtener el control de la misma, comprometer su seguridad, etc.

Ejemplos de Activos

# La amenaza

La amenaza es un evento potencialmente negativo que puede causar daños a un activo

Ejemplos de amenazas:

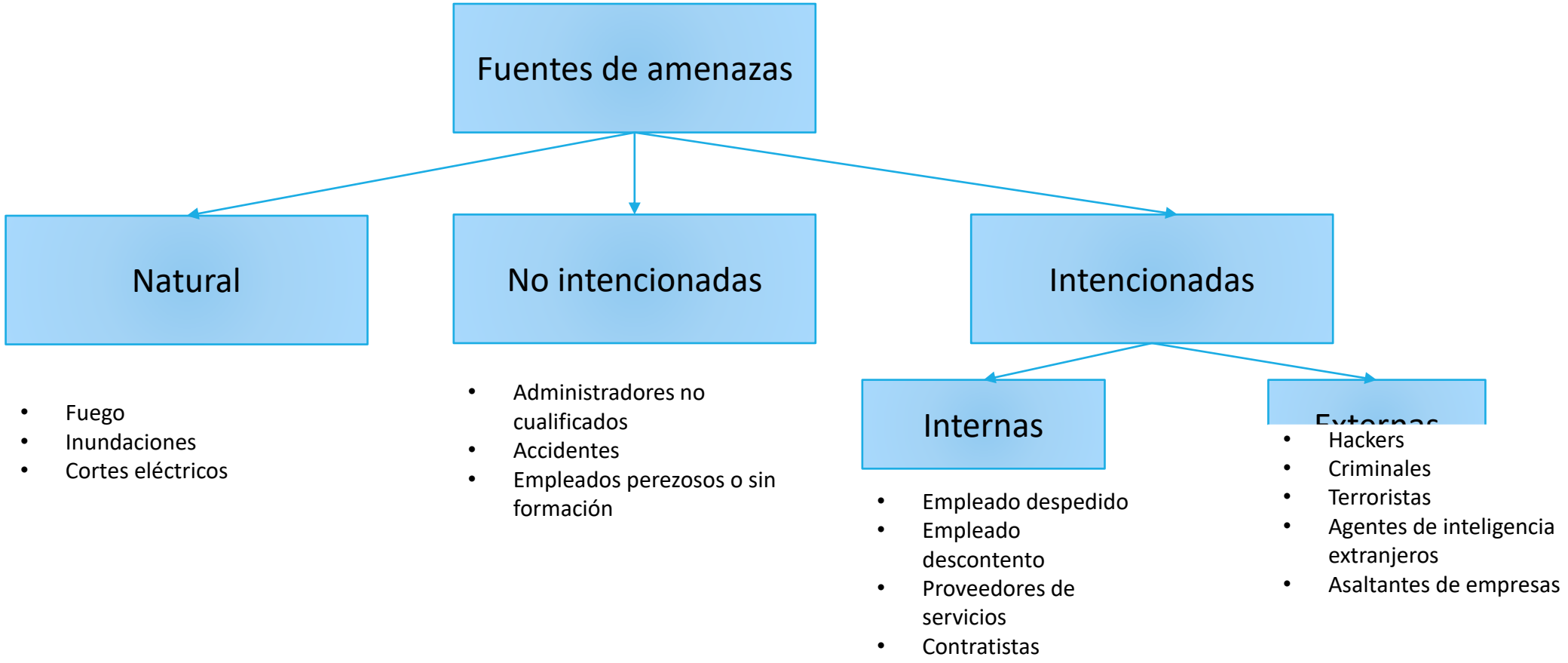
Un atacante puede robar datos sensibles de la organización

Un atacante puede hacer que el servidor se apague

Un atacante puede engañar a un empleado para que revele información sensible

Un atacante puede infectar el sistema con malware

# Fuentes de amenaza



# Actores/agentes de amenazas

Un actor de amenazas es un individuo o grupo que irrumpe en el sistema para lograr un objetivo específico

Tipos de actores de amenazas:

**Hacktivistas**

- Individuos que promueven una agenda política mediante la piratería informática, especialmente desfigurando o inutilizando sitios web

**Ciberterroristas**

- Individuos con una amplia gama de habilidades, motivados por creencias religiosas o políticas, para crear amenazas de interrupción a gran escala de las redes informáticas

**Hackers Suicidas**

- Individuos que tienen como objetivo derribar la infraestructura crítica por una "causa" y no son disuadidos por las penas de cárcel u otros tipos de castigo

# Actores/agentes de amenazas

| | |
|---|---|
| **Hackers patrocinados por el Estado** | Individuos empleados por el gobierno para penetrar y recopilar información de alto secreto y para dañar los sistemas de información de otros gobiernos |
| **Hackers organizados** | Hackers profesionales que atacan un sistema con fines de lucro |
| **Script Kiddies** | Hacker no calificado que compromete los sistemas ejecutando scripts, herramientas y software desarrollados por hackers reales |
| **Espías industriales** | Individuos que intentan atacar a las empresas con fines comerciales |
| **Amenaza interna** | Amenaza que se origina en personas dentro de la organización como empleados descontentos, empleados despedidos y personal poco capacitadoCopyright |

# Vulnerabilidad

Se refiere a la existencia de una debilidad en un activo que puede ser explotada por agentes de amenaza

Causas comunes para la existencia de una vulnerabilidad:

Mala configuración del hardware o del software

Diseño inseguro o deficiente de la red y la aplicación

Debilidades tecnológicas inherentes

Enfoque descuidado de los usuarios finales

# Vulnerabilidad

Ejemplo de vulnerabilidades de seguridad en la red: Vulnerabilidades tecnológicas

| Vulnerabilidades | Descripción |
|---|---|
| Vulnerabilidades del protocolo TCP/IP | HTTP, FTP, ICMP, SNMP, SMTP son inherentemente inseguros |
| Vulnerabilidades del sistema operativo | Un sistema operativo puede ser vulnerable porque: Es intrínsecamente inseguro No está parcheado con las últimas actualizaciones |
| Vulnerabilidades de los dispositivos de red | Varios dispositivos de red como routers, firewalls y switches pueden ser vulnerables debido a:<br>• Falta de protección con contraseña<br>• Falta de autenticación<br>• Protocolos de enrutamiento inseguros<br>Vulnerabilidades del cortafuegos |

# Vulnerabilidad

Ejemplo de vulnerabilidades de seguridad en la red: Vulnerabilidades de configuración

| Vulnerabilidades | Descripción |
|---|---|
| Vulnerabilidades de la cuenta de usuario | Originado por la transmisión insegura de los detalles de las cuentas de los usuarios, como los nombres de usuario y las contraseñas, a través de la red |
| Vulnerabilidades de la cuenta del sistema | Originado por la configuración de contraseñas débiles para las cuentas del sistema |
| Desconfiguración del servicio de Internet | La desconfiguración de los servicios de Internet puede plantear graves riesgos de seguridad. Por ejemplo, la activación de JavaScript y la configuración incorrecta de los servicios IIS, Apache, FTP y Terminal pueden crear vulnerabilidades de seguridad en la red. |
| Contraseña y configuración por defecto | Dejar los dispositivos/productos de red con sus contraseñas y ajustes por defecto |
| Desconfiguración del dispositivo de red | Configurar mal el dispositivo de red |

# Vulnerabilidad

Ejemplo de vulnerabilidad de la seguridad de la red: Política de seguridad

| Vulnerabilidades | Descripción |
|---|---|
| Política no escrita | Las políticas de seguridad no escritas son difíciles de aplicar y hacer cumplir |
| Falta de continuidad | Falta de continuidad en la aplicación y el cumplimiento de la política de seguridad |
| Política | La política puede causar problemas para la aplicación de una política de seguridad coherente |
| Falta de concienciación | Falta de conocimiento de la política de seguridad |

# Riesgo

El riesgo se refiere a la pérdida o daño potencial que puede ocurrir cuando existe una amenaza para un activo en presencia de una vulnerabilidad que puede ser explotada

**Ejemplo de riesgos**

Interrupción o cierre total de la empresa

Pérdida de privacidad Responsabilidad legal

Pérdida de productividad Pérdida/robo de datos

Daño a la reputación y pérdida de confianza del consumidor

**Representación del riesgo**

Riesgo = Activo + Amenaza + Vulnerabilidad

# Ataque

Un ataque es una acción iniciada para explotar una o más vulnerabilidades con el fin de actualizar una amenaza

**Ataque = Motivo (Objetivo) + Método (TTPs) + Vulnerabilidad**

Motivo (Objetivo)

Un motivo se origina en la noción de que el sistema objetivo almacena o procesa algo valioso, y esto lleva a una amenaza de ataque al sistema

Ejemplos de motivos detrás de los ciberataques:

| | | |
|---|---|---|
| Interrupción de la continuidad del negocio | Crear miedo y caos interrumpiendo infraestructuras críticas | Conseguir objetivos militares del Estado |
| Robo de información | Pérdidas financieras para el objetivo | Venganza |
| Manipulación de datos | Propagar creencias religiosas o políticas | Exigir un rescate |
| Dañar la reputación del objetivo | | |

# Ataque

**Métodos (TTPs)**

Los atacantes intentan varias técnicas de ataque para explotar las vulnerabilidades de un sistema informático o la política y los controles de seguridad para lograr sus motivos

Los términos Tácticas, Técnicas y Procedimientos (TTPs) se refieren a los patrones de actividades y métodos asociados con actores o grupos de actores de amenazas específicos

**Tácticas**

"Táctica" se define como la estrategia adoptada por un atacante para realizar el ataque desde el principio hasta el final

**Técnicas**

"Técnicas" se define como los métodos técnicos utilizados por un atacante para lograr resultados intermedios durante el ataque

**Procedimientos**

"Procedimiento" se define como un enfoque sistemático adoptado por los actores de la amenaza para lanzar un ataque

# Describir varios ejemplos de técnicas de ataque a nivel de red

# Ataques de reconocimiento

La explotación de la red objetivo comienza con el reconocimiento

En los ataques de reconocimiento, los atacantes intentan descubrir información sobre la red objetivo

Los atacantes pueden utilizar las siguientes técnicas para recopilar información de red sobre el objetivo:

- Ingeniería social
- Escaneo de puertos
- Huella DNS
- Barrido de ping

Información de la red obtenida mediante ataques de reconocimiento

- Nombres de dominio
- Nombres de dominio internos
- Bloqueos de red
- Direcciones IP de los sistemas alcanzables
- Sitios web fraudulentos/Sitios web privados
- Puertos abiertos
- Versiones de sistemas operativos en ejecución
- Servicios TCP y UDP
- Mecanismos de control de acceso y ACLs
- Protocolos de red
- Puntos VPN
- Cortafuegos en ejecución
- Números de teléfono analógicos/digitales
- Mecanismos de autenticación Sistema

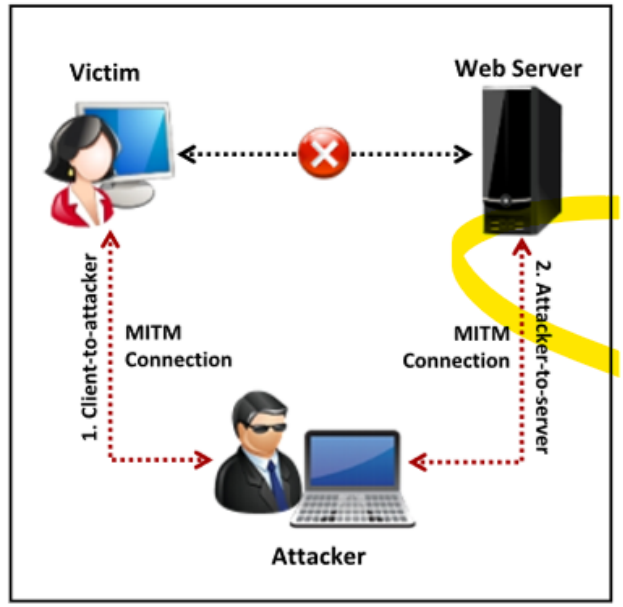
# Ataque de rastreo de red (Network Sniffing Attack)

El sniffing es un proceso de monitorización y captura de todos los paquetes de datos que pasan a través de una red determinada utilizando herramientas de sniffing

Los atacantes utilizan varias utilidades de sniffing para olfatear el tráfico de la red y recopilar información sensible

# Ataque de hombre en el medio (Man-in-the-Middle Attack)

1. En este ataque, el intruso despliega una estación entre el sistema de comunicación del cliente y el servidor para interceptar los mensajes que se intercambian
2. Los atacantes utilizan diferentes técnicas para dividir la conexión TCP en dos conexiones
    1. Conexión cliente-atacante
    2. Conexión atacante-servidor
3. La interceptación de la conexión TCP permite al atacante leer, modificar e insertar datos fraudulentos en la comunicación interceptada
4. En el caso de una transacción HTTP, el objetivo es la conexión TCP entre el cliente y el servidor



# Ataque a la contraseña

Un atacante intenta aprovechar los puntos débiles para descifrar contraseñas

El uso de contraseñas comunes hace que un sistema o aplicación sea vulnerable a los ataques de descifrado de contraseñas. Las contraseñas más utilizadas son: password, pa$$w0rd, root, administrator, admin, Test, guest, qwerty, o información personal como el nombre, el cumpleaños y los nombres de los hijos.

Los atacantes utilizan varias técnicas como la fuerza bruta, la ingeniería social, el spoofing, el phishing, el malware, el sniffing y el keylogging para adquirir las contraseñas

Los atacantes comienzan por descifrar las contraseñas para engañar a los dispositivos de red y hacerles creer que son usuarios válidos

# Ataque de escalada de privilegios

Un atacante puede obtener acceso a una red utilizando una cuenta de usuario que no sea de administrador y, posteriormente, obtener privilegios administrativos

El atacante realiza un ataque de escalada de privilegios, que aprovecha los defectos de diseño, los errores de programación, los fallos y los descuidos de configuración en el sistema operativo y la aplicación de software para obtener acceso administrativo a la red y a sus aplicaciones asociadas

La escalada de privilegios permite al atacante ver información privada, eliminar archivos o instalar programas maliciosos como virus, troyanos, gusanos, etc.

# Ataque de escalada de privilegios

Tipos de escalada de privilegios

Escalada vertical de privilegios

- Involucra el cambio de una cuenta de usuario a una cuenta con mayores privilegios

Escalada horizontal de privilegios

- Involucra el cambio de una cuenta de usuario a otra cuenta de usuario con los mismos privilegios

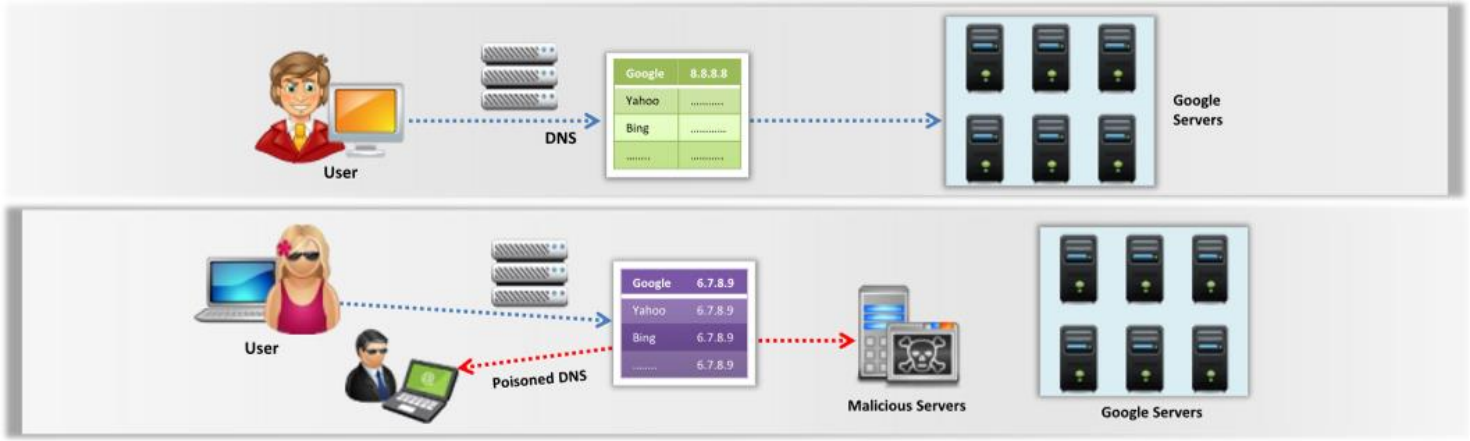
# Ataque de envenenamiento de DNS (DNS Poisoning Attack)

El envenenamiento del servidor de nombres de dominio (DNS) es la manipulación no autorizada de las direcciones IP en la caché del DNS

El DNS almacena las traducciones de los nombres de dominio de las direcciones IP para los dispositivos de red

Un DNS corrupto redirige la solicitud de un usuario a un sitio web malicioso para realizar actividades ilegales

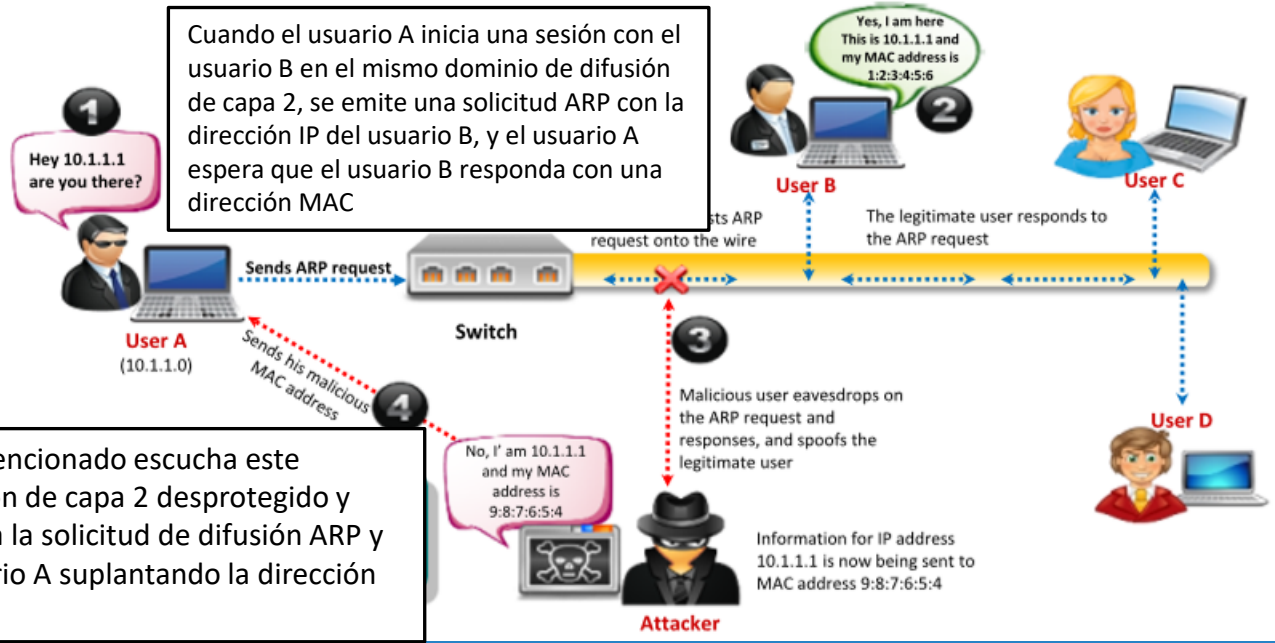
Si una víctima escribe ww.google.com, la solicitud se redirige al sitio web falso www.goggle.com



# Ataque de envenenamiento de ARP (ARP Poisoning Attack)

El Protocolo de Resolución de Direcciones (ARP) es un protocolo utilizado para asignar una dirección IP a una dirección de máquina física que se reconoce en la red local

La suplantación/envenenamiento de ARP implica el envío de un gran número de entradas falsas a la caché ARP de la máquina objetivo



# Ataque de inanición de DHCP (DHCP Starvation Attack)

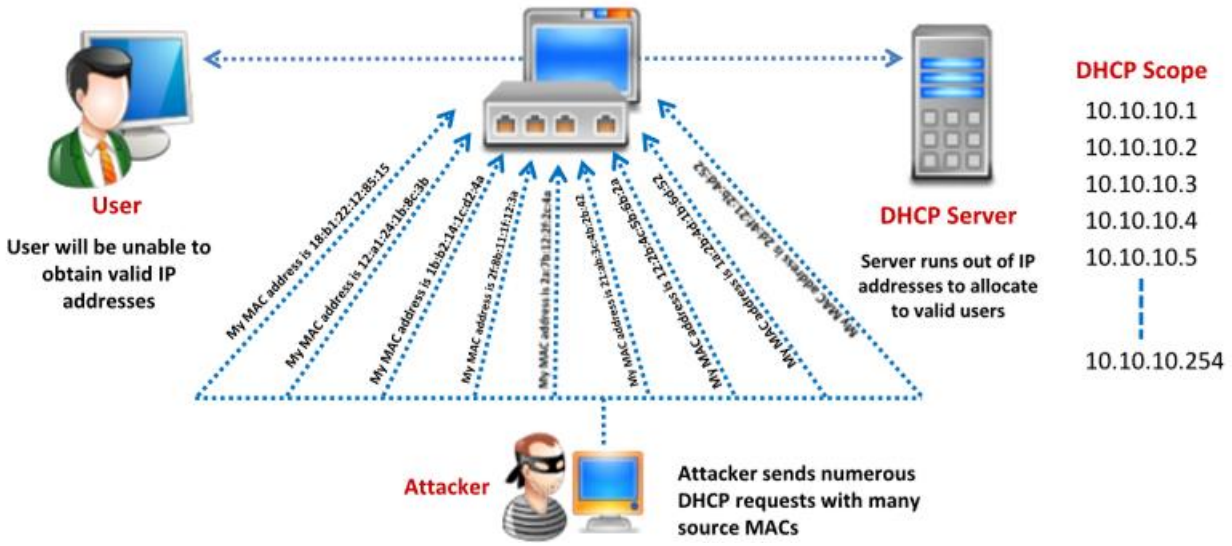
El protocolo de configuración dinámica de host (DHCP) es un protocolo de configuración que asigna direcciones IP válidas a los sistemas de host a partir de un conjunto preasignado de DHCP

El ataque de inanición de DHCP es un proceso que consiste en inundar los servidores DHCP con solicitudes falsas de DHCP y utilizar todas las direcciones IP disponibles

Esto da lugar a un ataque de denegación de servicio, en el que el servidor DHCP no puede emitir nuevas direcciones IP a las solicitudes de host genuinas

Los nuevos clientes no pueden obtener acceso a la red, lo que da lugar a un ataque de inanición de DHCP

# Ataque de inanición de DHCP (DHCP Starvation Attack)



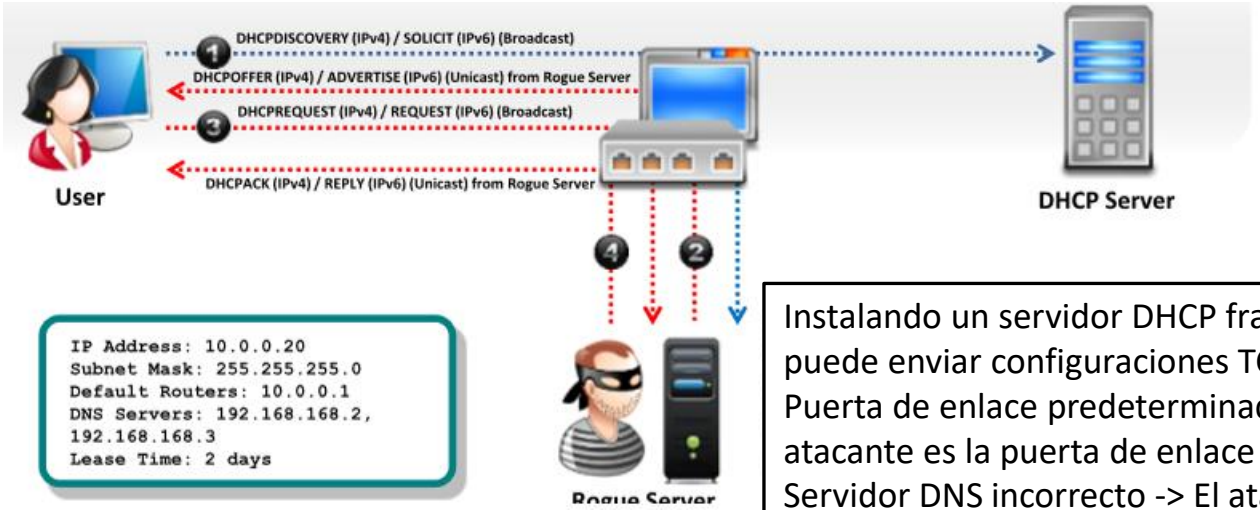
# Ataque de falsificación de DHCP (DHCP Spoofing Attack)

Los servidores DHCP asignan direcciones IP a los clientes de forma dinámica

Un atacante coloca un servidor DHCP falso entre el cliente y el servidor DHCP real

Cuando un cliente envía una solicitud, el servidor falso del atacante intercepta la comunicación y actúa como servidor DHCP respondiendo con direcciones IP falsas

# Ataque de falsificación de DHCP (DHCP Spoofing Attack)




Instalando un servidor DHCP fraudulento, el atacante puede enviar configuraciones TCP/IP incorrectas como:
Puerta de enlace predeterminada incorrecta -> El atacante es la puerta de enlace
Servidor DNS incorrecto -> El atacante es el servidor DNS
Dirección IP incorrecta -> DoS con página IP falsa

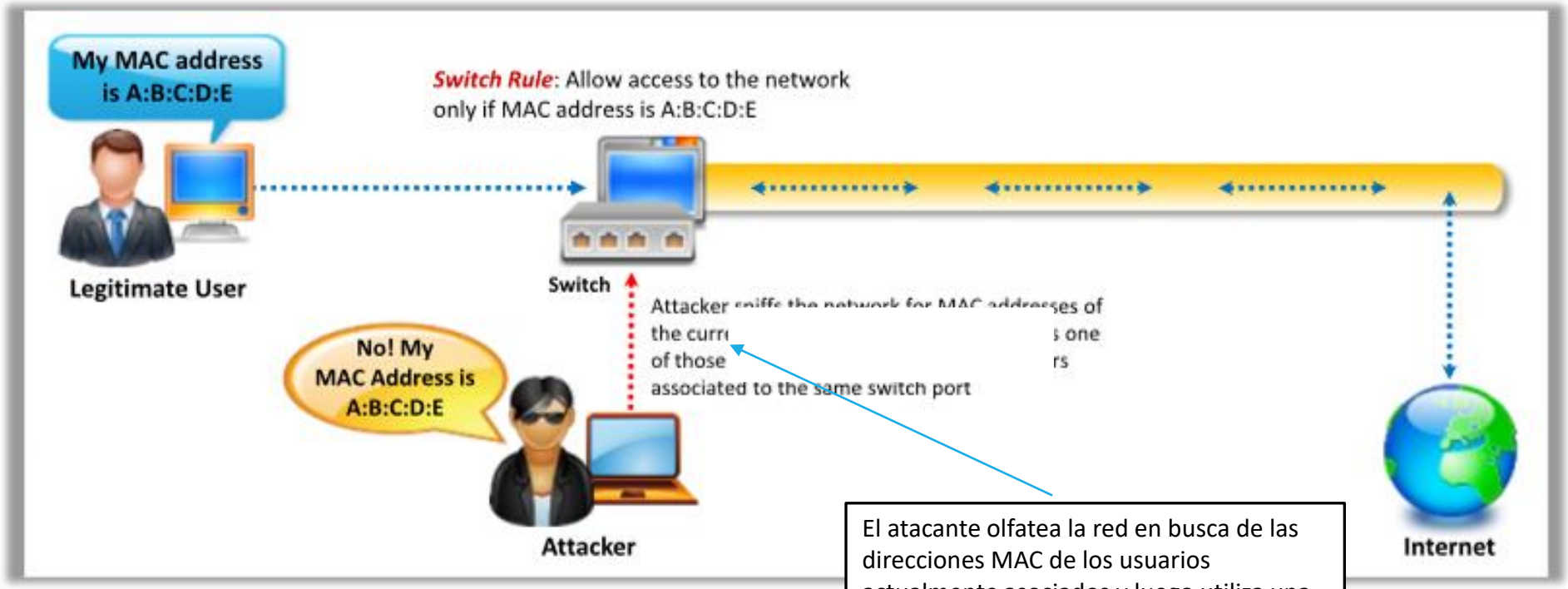
# Ataque de suplantación de MAC (MAC Spoofing Attack)

Un ataque de suplantación de MAC se lanza olfateando una red en busca de direcciones MAC de clientes que estén activamente asociados a un puerto de conmutación, y reutilizando una de esas direcciones

Al interceptar el tráfico de la red, el atacante replica la dirección MAC de un usuario legítimo para recibir todo el tráfico destinado al usuario específico

Este ataque permite a un atacante obtener acceso a la red fingiendo la identidad de otra persona que ya está en la red

# Ataque de suplantación de MAC (MAC Spoofing Attack)




El atacante olfatea la red en busca de las direcciones MAC de los usuarios actualmente asociados y luego utiliza una de esas direcciones MAC para atacar a otros usuarios asociados al mismo puerto del switchNota

# Ataque de denegación de servicio basado en la red (DoS)

En el ataque DoS basado en la red, el atacante envía una gran cantidad de tráfico a la red objetivo, agotando así los recursos de conexión de la víctima

El atacante lo hace explotando la implementación existente de los protocolos de red

Ejemplos de ataques DoS específicos del sistema operativo incluyen:

| | |
|---|---|
| Inundación TCP SYN (TCP SYN Flooding) | Inundación UDP (UDP Flooding) |
| Inundación de pitufos ICMP (ICMP Smurf Flooding) | Inundación intermitente (Intermittent Flooding) |

# Ataque distribuido de denegación de servicio (DDoS)

Los ataques DDoS implican una multitud de sistemas comprometidos que atacan un único objetivo, causando así una denegación de servicio para los usuarios legítimos

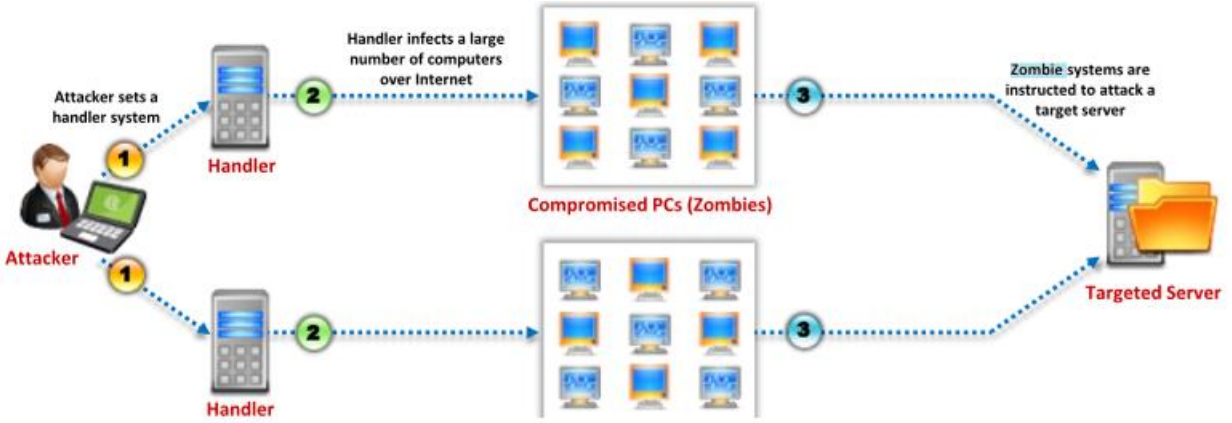
Los ataques DDoS deshabilitan toda la red y dificultan las operaciones comerciales causando pérdidas financieras y una mala reputación

Un atacante utiliza las redes de bots para explotar las vulnerabilidades que existen en el sistema objetivo y convertirlo en un bot master. Esto se utiliza para infectar el objetivo con malware, u obtener el control de otros sistemas en la red

**Dos tipos de DDoS**

Ataque centrado en la red: Sobrecarga un servicio consumiendo ancho de banda

Ataque centrado en la aplicación: Sobrecarga un servicio inundándolo de paquetes Zombie



# Ataque de malware

Los malware son programas de software o códigos maliciosos que se instalan en un sistema sin que el usuario lo sepa.

Un ataque de malware interrumpe los servicios, daña los sistemas, recopila información sensible, etc.

Ejemplos de malware son los virus, troyanos, adware, spyware, rootkits y backdoors

| | |
|---|---|
| **Virus**<br>Programa autorreplicable que se adhiere a otro programa, al sector de arranque del ordenador o a un documento | **Spyware**<br>Código de software que extrae información del usuario y la envía a los atacantes |
| **Trojan**<br>Programa que parece ser un software legítimo o útil pero que contiene código oculto y dañino | **Rootkit**<br>Programa de software malicioso que oculta ciertas actividades para que no sean detectadas por los sistemas operativos |
| **Adware**<br>Programa de software que rastrea los patrones de navegación del usuario con fines de marketing y para mostrar publicidad | **Backdoor**<br>Programa que permite a los atacantes eludir los controles de autenticación, por ejemplo, obteniendo privilegios administrativos sin contraseñas |

# Amenazas Persistentes Avanzadas (APTs)

Una Amenaza Persistente Avanzada (APT) se define como un tipo de ataque a la red, en el que un atacante obtiene acceso no autorizado a una red objetivo y permanece en ella sin ser detectado durante un largo período de tiempo

El objetivo principal de estos ataques es obtener información sensible en lugar de sabotear la organización y la red de la organización

# Amenazas Persistentes Avanzadas (APTs)

Información obtenida durante los ataques APT

Documentos clasificados

Credenciales de usuario

Información personal de empleados o clientes

Información de redInformación sobre transacciones

Información sobre tarjetas de crédito

Información sobre la estrategia empresarial de la organización

Información sobre el acceso al sistema de control

# Describir varios ejemplos de técnicas de ataque a nivel de aplicación

# Ataque de inyección SQL

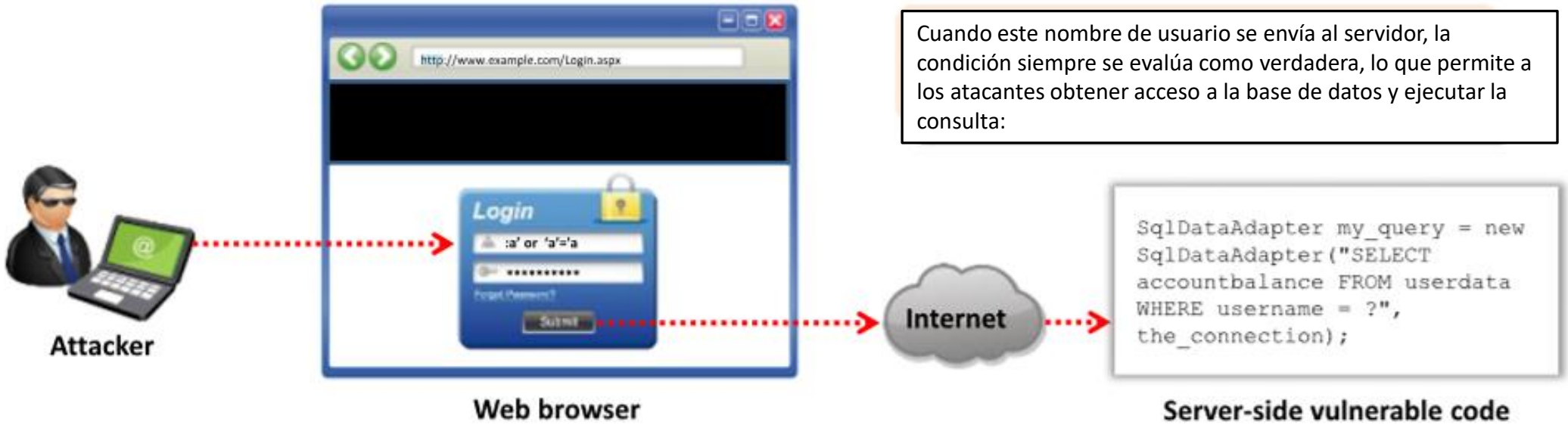
Los ataques de inyección SQL utilizan una serie de consultas SQL maliciosas para manipular directamente una base de datos

Un atacante puede utilizar una aplicación web vulnerable para saltarse las medidas de seguridad normales y obtener acceso directo a datos valiosos

Los ataques de inyección SQL pueden ejecutarse a menudo desde la barra de direcciones, desde los campos de la aplicación y a través de consultas y búsquedas

Este ataque sólo es posible cuando la aplicación ejecuta sentencias SQL dinámicas y almacena procedimientos con argumentos basados en la entrada del usuario

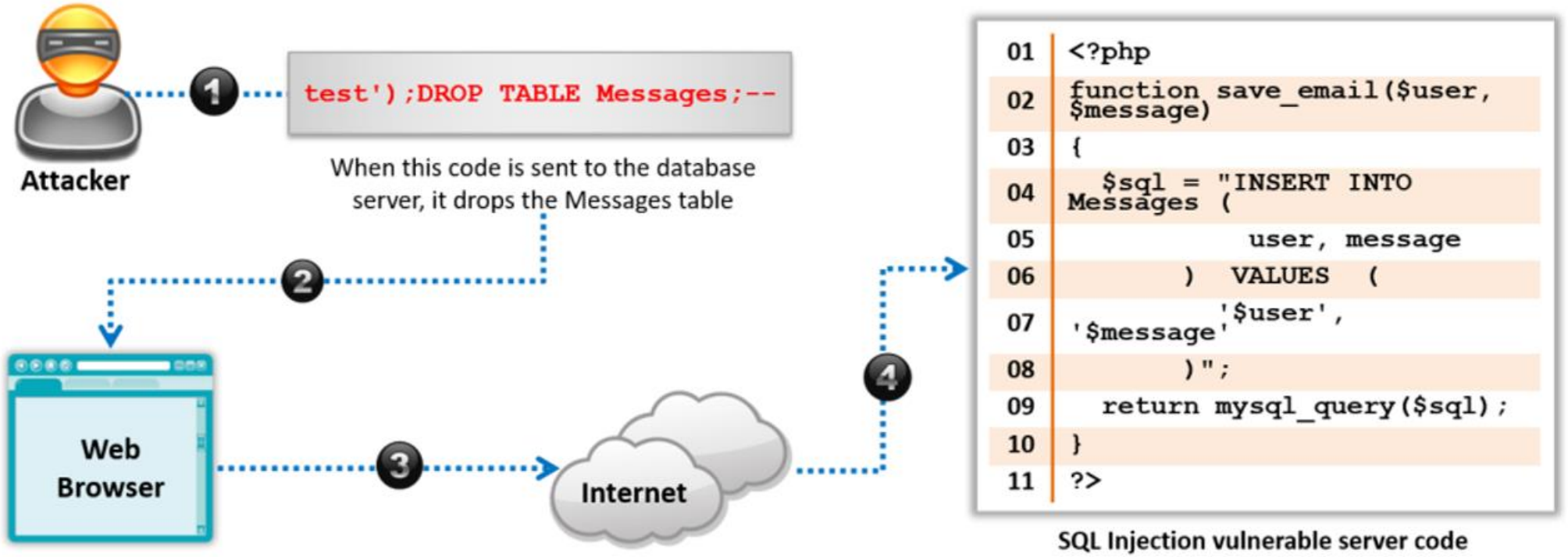
# Ataque de inyección SQL




Cuando este nombre de usuario se envía al servidor, la condición siempre se evalúa como verdadera, lo que permite a los atacantes obtener acceso a la base de datos y ejecutar la consulta:

SELECT * FROM tablename WHERE UserID= 2302
Se cambia por
SELECT * FROM tablename WHERE UserID= 2302 OR 1=1

# Ataque de inyección SQL

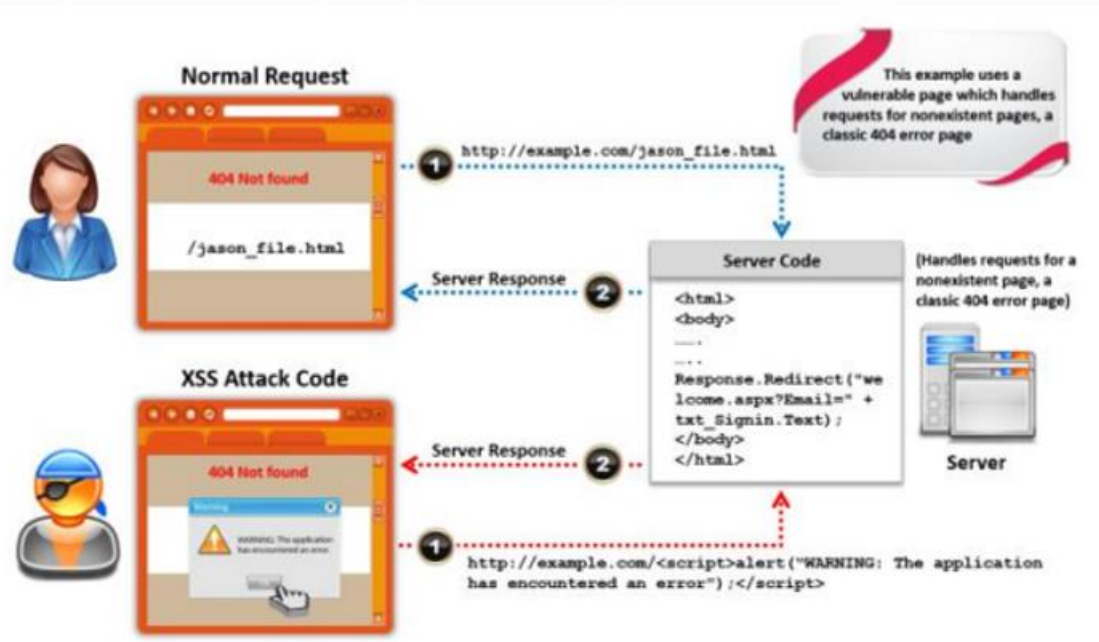


# Ataque de secuencias de comandos en sitios cruzados (XSS)
# (Cross-site Scripting (XSS) Attack)

Los ataques de secuencias de comandos en sitios cruzados ("XSS") aprovechan las vulnerabilidades de las páginas web generadas dinámicamente, lo que permite a los atacantes malintencionados inyectar secuencias de comandos del lado del cliente en las páginas web visualizadas por otros usuarios

Se produce cuando se incluyen datos de entrada invalidados en el contenido dinámico que se envía al navegador web de un usuario para su representación

Los atacantes inyectan JavaScript, VBScript, ActiveX, HTML o Flash malintencionados para su ejecución en un sistema víctima ocultándolos dentro de solicitudes legítimas

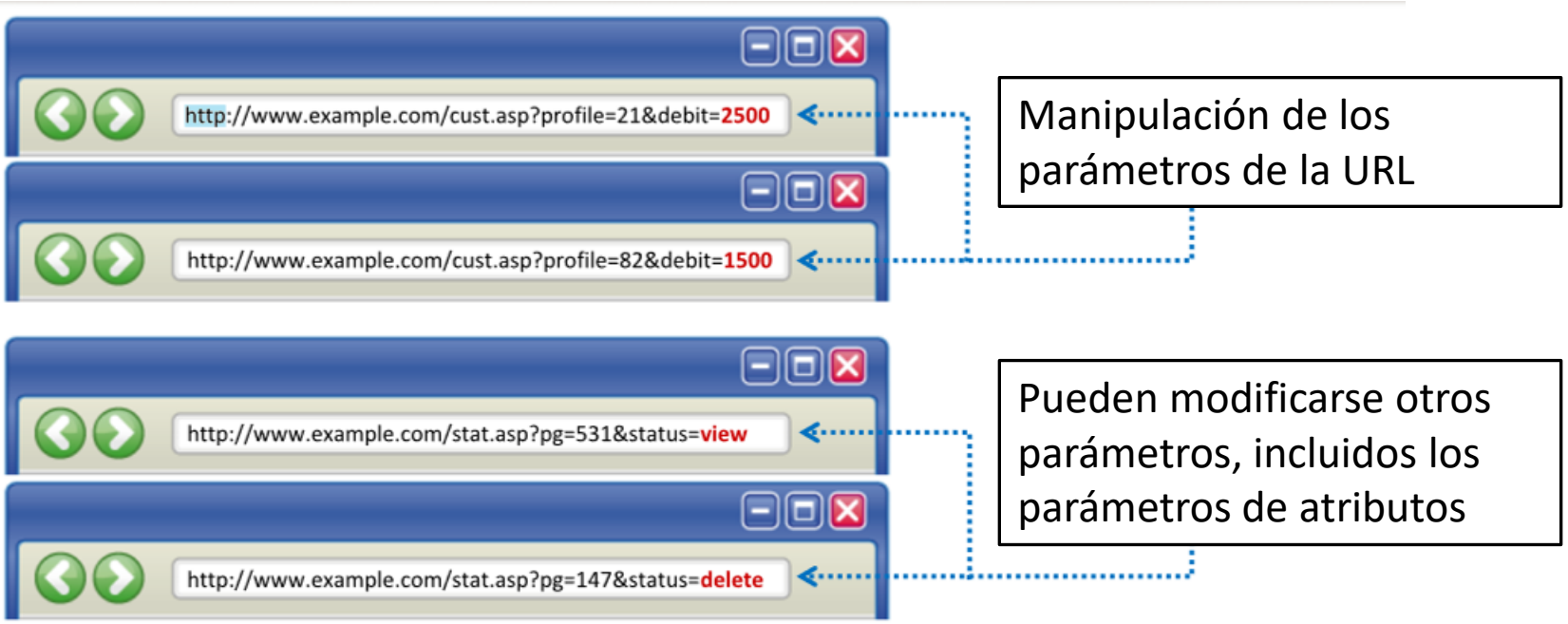


# Ataque de manipulación de parámetros

Un ataque de manipulación de parámetros web implica la manipulación de los parámetros intercambiados entre el cliente y el servidor con el fin de modificar los datos de la aplicación, como las credenciales y los permisos del usuario, el precio y la cantidad de productos

Un ataque de manipulación de parámetros explota las vulnerabilidades de los mecanismos de validación de la integridad y la lógica que pueden dar lugar a XSS, inyección SQL, etc.http

# Ataque de manipulación de parámetros



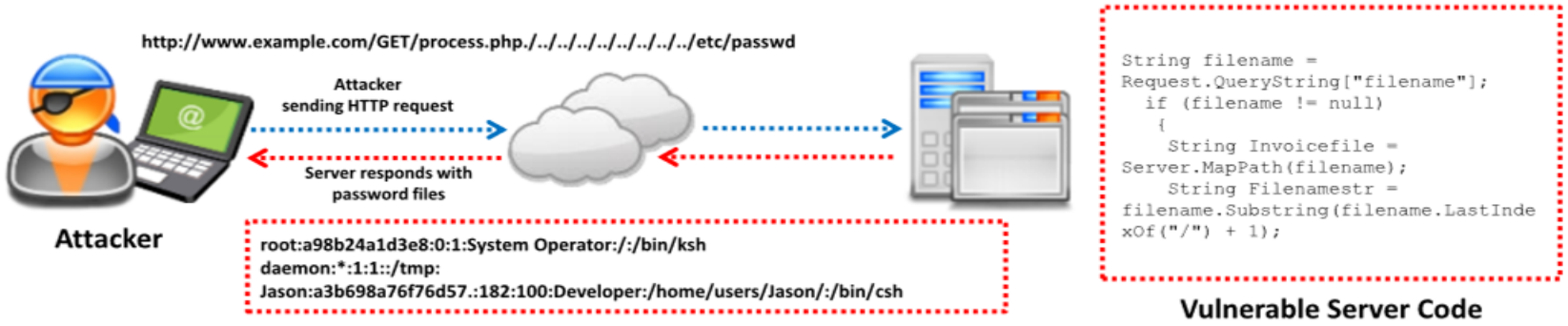
# Ataque de cruce de directorios

El cruce de directorios permite a los atacantes acceder a directorios restringidos, incluyendo el código fuente de la aplicación, la configuración y los archivos críticos del sistema, y ejecutar comandos fuera del directorio raíz del servidor web

Acceso a archivos ubicados fuera del directorio de publicación web mediante el cruce de directorios

Los atacantes pueden manipular variables que hacen referencia a archivos con secuencias de "barra de puntos (../)" y sus variaciones

- http://www.example.com/process.aspx=../../../../algo dir/algo_fichero
- http://w



# Ataque de falsificación de solicitud en sitios cruzados (CSRF)

Los ataques de falsificación de petición en sitios cruzados (CSRF) aprovechan las vulnerabilidades de las páginas web que permiten a un atacante forzar el navegador de un usuario desprevenido a enviar peticiones maliciosas

El usuario víctima mantiene una sesión activa con un sitio de confianza y simultáneamente visita un sitio malicioso, que inyecta una petición HTTP para el sitio de confianza en la sesión de la víctima, comprometiendo su integridad

# Ataque DoS a nivel de aplicación

Los atacantes agotan los recursos disponibles del servidor enviando cientos de solicitudes que consumen muchos recursos, como la recuperación de grandes archivos de imágenes o la solicitud de páginas dinámicas que requieren costosas operaciones de búsqueda en el backend de los servidores de bases de datos

Los ataques DoS a nivel de aplicación emulan la misma sintaxis de solicitud y las mismas características de tráfico a nivel de red que las de los clientes legítimos, lo que los hace indetectables para las medidas de protección DoS existentes

# Ataque DoS a nivel de aplicación

**Objetivos**

- PU, memoria y zócalos
- Ancho de banda del disco
- Ancho de banda de la base de datos
- Procesos de trabajo

**¿Por qué las aplicaciones son vulnerables al DoS?**

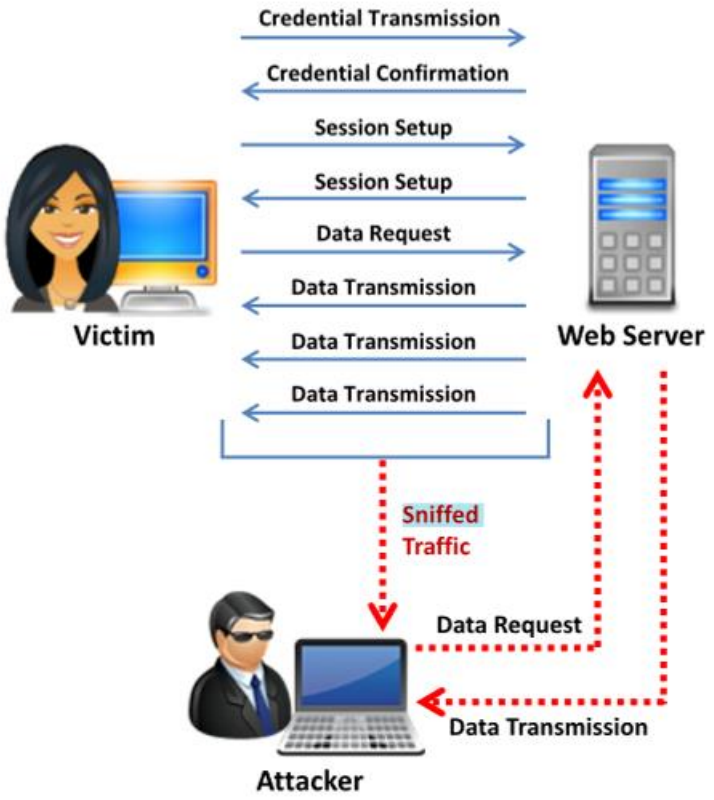
- Uso razonable de las expectativas
- Entorno de la aplicación
- Cuellos de botella
- Fallos de implementación
- Mala validación de los datos

# Ataque de secuestro de sesión

El secuestro de sesión se refiere a un ataque en el que un atacante se apodera de una sesión de comunicación TCP válida entre dos ordenadores

Los atacantes pueden olfatear todo el tráfico de las sesiones TCP establecidas y realizar robos de identidad, de información, fraudes, etc.

El atacante roba un ID de sesión válido y lo utiliza para autenticarse con el servidor



# Describir varios ejemplos de técnicas de ataque de ingeniería social

# Ataques de ingeniería social

La ingeniería social es el arte de convencer a las personas para que revelen información confidencial

Suplantación de identidad

En este ataque de ingeniería social, el atacante se hace pasar por alguien legítimo o por una persona autorizada

Los atacantes pueden hacerse pasar por una persona legítima o autorizada, ya sea en persona o utilizando un medio de comunicación como el teléfono, el correo electrónico, etc.

La suplantación permite a los atacantes engañar a un objetivo para que revele información sensible.

# Ataques de ingeniería social

Hacerse pasar por un usuario final legítimo

- Proporcionar la identidad y pedir la información sensible
  - "¡Hola! Soy Juan, del departamento de finanzas. He olvidado mi contraseña. ¿Puedo obtenerla?".

Hacerse pasar por un usuario importante

- Se hace pasar por un VIP de una empresa objetivo, un cliente valioso, etc.
  - "¡Hola! Soy Pepe, secretario del director financiero. Estoy trabajando en un proyecto urgente y he perdido la contraseña de mi sistema. ¿Puedes ayudarme?“

Hacerse pasar por soporte técnico

- Llamar como personal de soporte técnico y solicitar identificaciones y contraseñas
  - "Señor, soy Luis, de soporte técnico, de la empresa X. Anoche tuvimos una caída del sistema aquí, y estamos comprobando los datos perdidos. ¿Puede darme su ID y contraseña para poder comprobarlo?"

# Ataques de ingeniería social

**Espionaje**

- El espionaje se refiere a la escucha no autorizada de conversaciones o a la lectura de mensajes
- Intercepción de comunicaciones de audio, vídeo o escritas
- Puede llevarse a cabo utilizando canales de comunicación como las líneas telefónicas, el correo electrónico y la mensajería instantánea.

**Shoulder Surfing**

- El Shoulder Surfing utiliza técnicas de observación directa como mirar por encima del hombro de alguien para obtener información como contraseñas, PINs y números de cuenta.
- El Shoulder Surfing también se puede llevar a cabo desde una distancia más larga con la ayuda de dispositivos de mejora de la visión como prismáticos que están equipados con la capacidad de obtener información a larga distancia

# Ataques de ingeniería social

**Dumpster Diving**

- Buscar información sensible, como facturas de teléfono, información de contacto, información financiera e información relacionada con operaciones, en la basura de alguien

**Piggybacking**

- Una persona autorizada permite (intencionadamente o no) que una persona no autorizada pase por una puerta segura

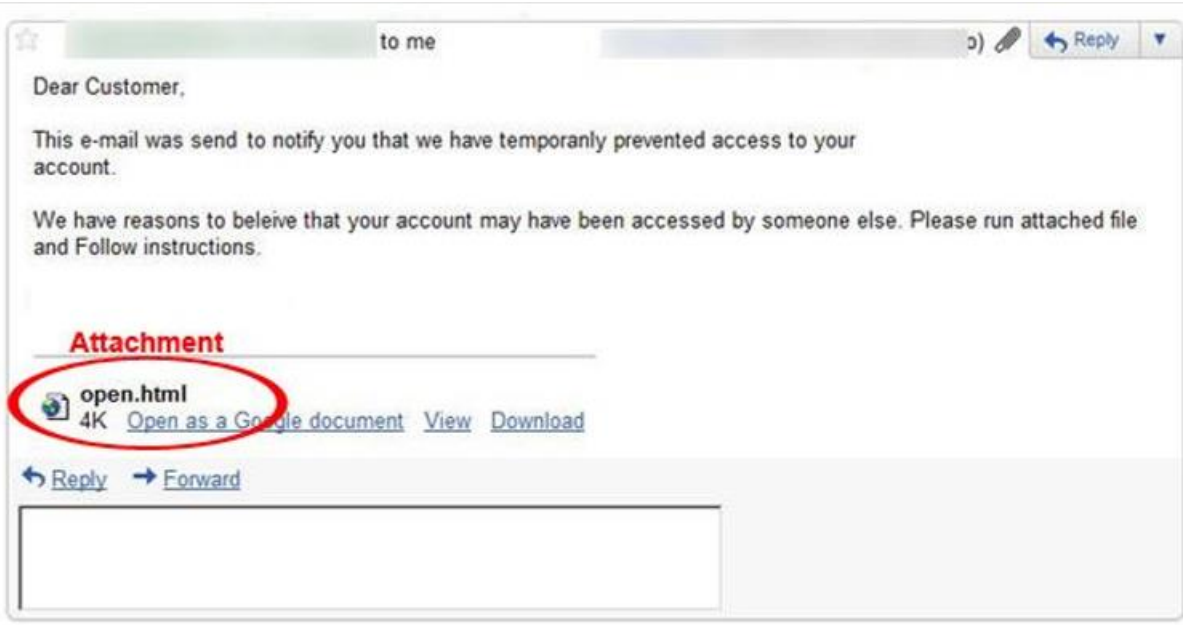
**Tailgating**

- Una persona no autorizada, que lleva una tarjeta de identificación falsa, entra en una zona segura siguiendo de cerca a una persona autorizada a través de una puerta que requiere acceso con llave

# Describir varios ejemplos de técnicas de ataque al correo electrónico

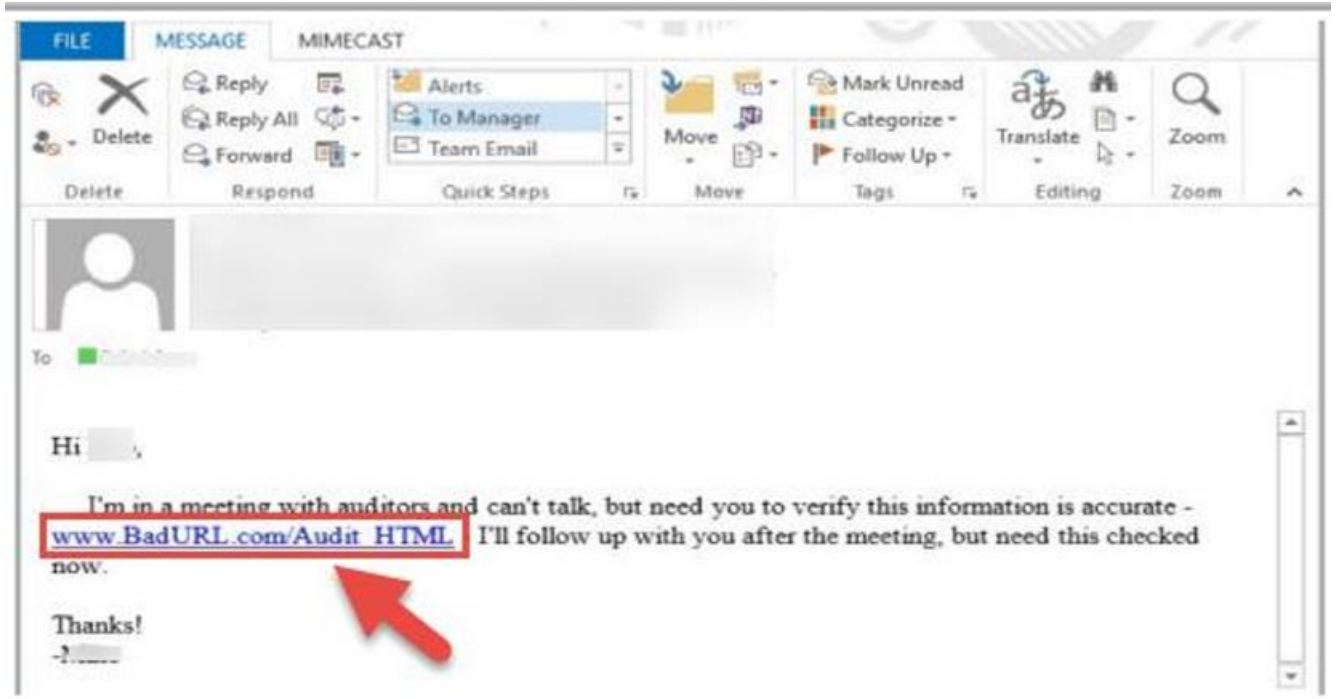
# Ataques por correo electrónico: Archivos adjuntos maliciosos en el correo electrónico

Los archivos adjuntos al correo electrónico son una importante amenaza para la seguridad, ya que pueden transmitir programas maliciosos (como virus, gusanos, troyanos, rootkits y programas espía) al ordenador de la víctima cuando ésta los abre



# Ataques de correo electrónico: Redireccionamiento malicioso de usuarios

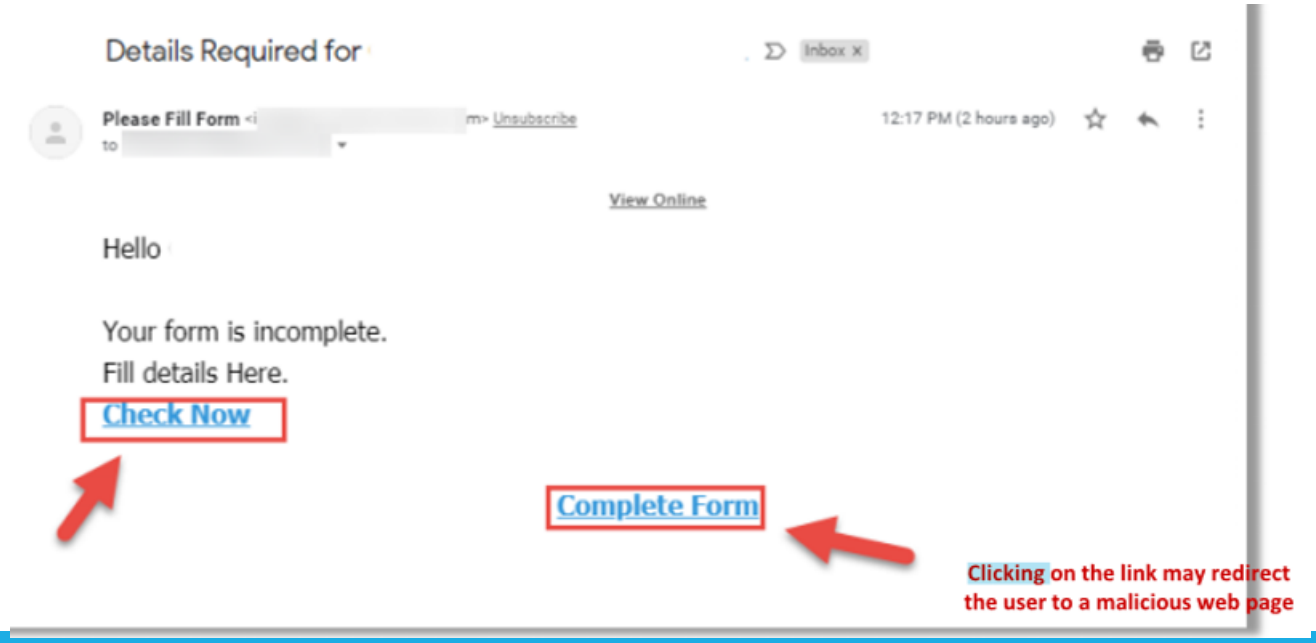
Los emails pueden contener enlaces, y al pulsarlos pueden redirigir a la victima a sitios web con malware.



# Ataques por correo electrónico: Phishing

El atacante envía un correo electrónico solicitando a la víctima información personal/financiera junto con un enlace similar a un sitio web genuino

Si la víctima hace clic en el enlace, introduce los detalles y luego hace clic en "Enviar", la información se envía al atacante



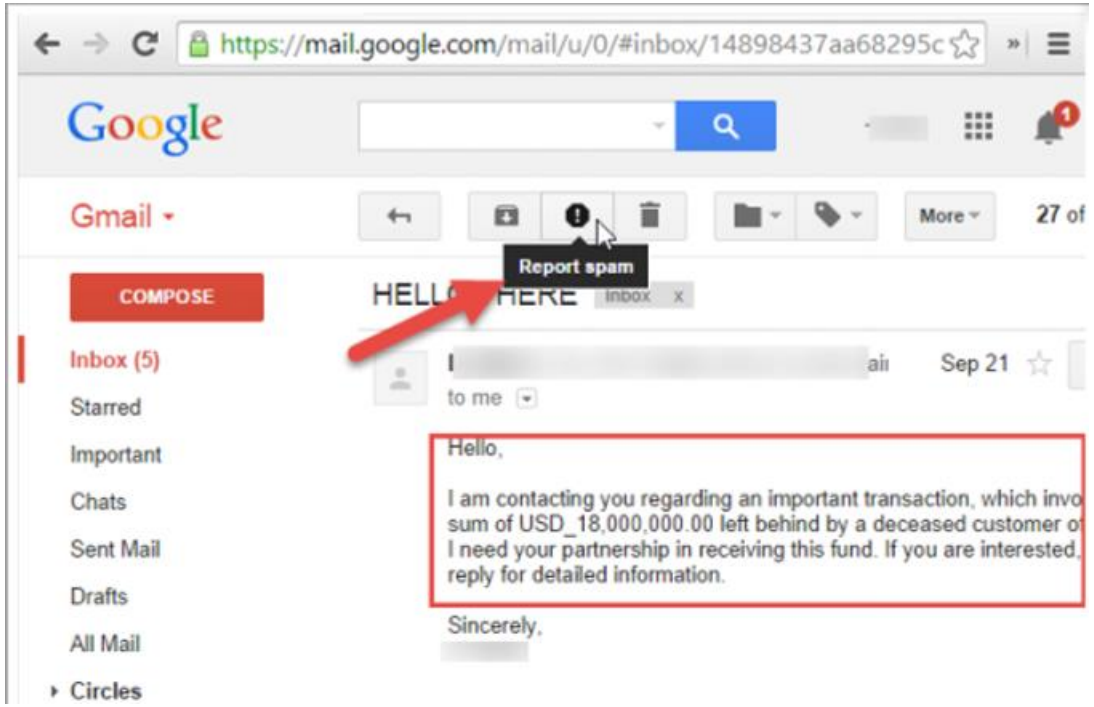
# Ataques por correo electrónico: Spamming

El spam se refiere a los anuncios comerciales no solicitados que se distribuyen en línea.

El spam suele contener contenidos falsos, poco fiables y sin valor

Aunque el correo electrónico sigue siendo la forma más común de enviar spam, también puede encontrarse en los tablones de anuncios y las salas de chat en línea

El spam sigue existiendo debido a las personas que responden a ellos



# Describir varios ejemplos de técnicas de ataque específicas para dispositivos móviles

# Rooting y Jailbreaking

## Rooting en teléfonos Android

- El rooting permite a los usuarios de Android obtener un control privilegiado (conocido como "acceso root") dentro del subsistema de Android
- El rooting implica explotar las vulnerabilidades de seguridad en el firmware del dispositivo, y copiar el binario su a una ubicación en el PATH del proceso actual (por ejemplo /system/xbin/su) y concederle permisos de ejecución con el comando chmod

## Jail breaking en teléfonos iOS

- Jailbreaking se define como el proceso de instalación de un conjunto modificado de parches del kernel que permite a los usuarios ejecutar aplicaciones de terceros no firmadas por el proveedor del sistema operativo
- Jailbreaking proporciona acceso root al sistema operativo y permite la descarga de aplicaciones, temas y extensiones de terceros en dispositivos iOS

# Carga de aplicaciones maliciosas en la App Store

Las tiendas de aplicaciones son objetivos comunes para que los atacantes distribuyan malware y aplicaciones maliciosas

Los atacantes también pueden hacer ingeniería social para que los usuarios descarguen y ejecuten aplicaciones fuera de las tiendas de aplicaciones oficiales

Las aplicaciones maliciosas pueden dañar otras aplicaciones y datos, y enviar datos confidenciales a los atacantes

# Spamming en el móvil

Mensajes de texto/correo electrónico no solicitados enviados a dispositivos móviles desde números de teléfono/identificadores de correo electrónico conocidos/desconocidos

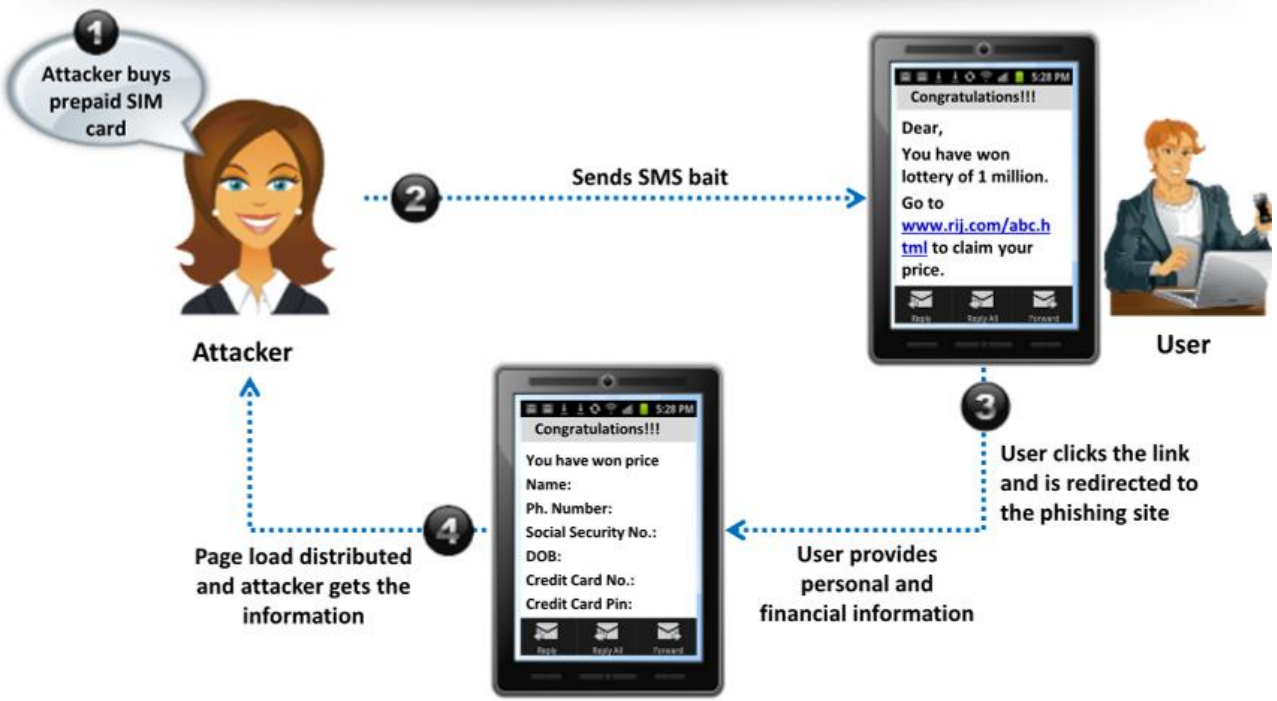
Los mensajes de spam contienen anuncios o enlaces maliciosos que pueden engañar a los usuarios para que revelen información confidencial

Los mensajes de spam desperdician una gran cantidad de ancho de banda

Los ataques de spam se realizan con fines económicos

# Ataque de phishing por SMS (SMiShing)

El phishing por SMS es el acto de intentar obtener información personal y financiera mediante el envío de SMS (o IM) que contienen un enlace falso




**¿Por qué es eficaz el phishing por SMS?**

La mayoría de los usuarios acceden a Internet a través de un móvil

Fácil de montar una campaña de phishing por móvil

Difícil de detectar y detener antes de que causen daños

Los usuarios de móviles no están acostumbrados a recibir mensajes de texto de spam en su móvil

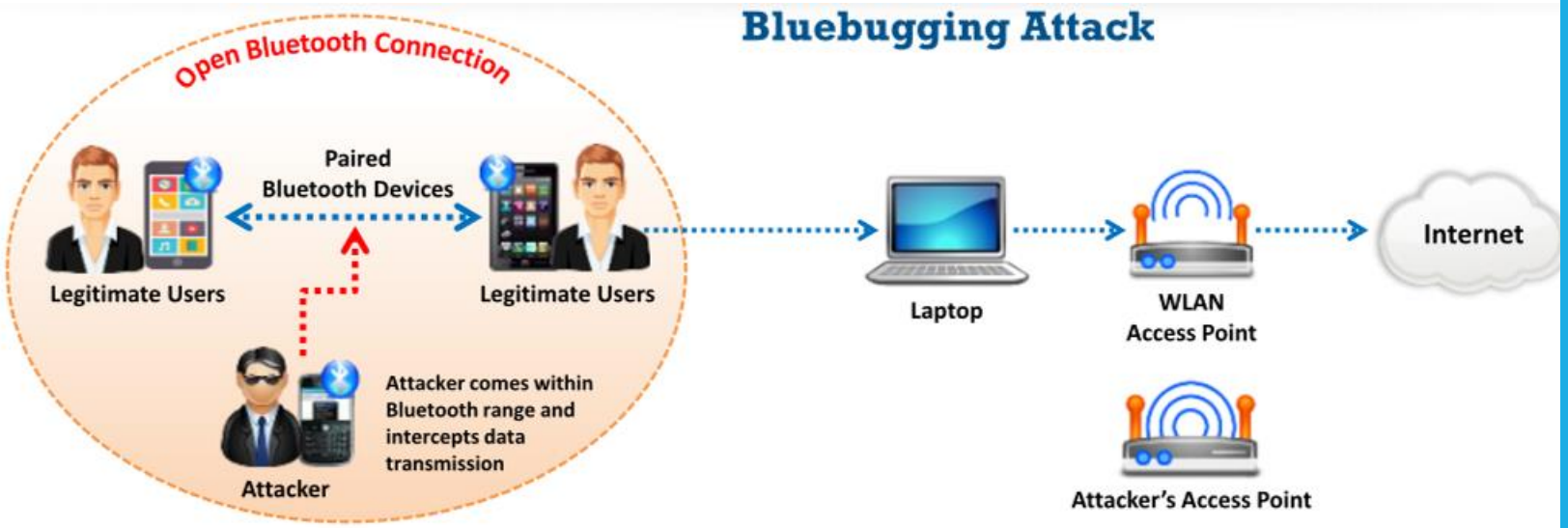
La mayoría de las aplicaciones antivirus para móviles no comprueban los SMS

# Ataque a la Bluebugging

El emparejamiento de dispositivos móviles en conexiones abiertas (Wi-Fi público/routers Wi-Fi sin cifrar) permite a los atacantes espiar e interceptar la transmisión de datos mediante técnicas como:

- Bluesnarfing (Robo de información a través de Bluetooth)
- Bluebugging (Obtención de control sobre el dispositivo a través de Bluetooth)

Compartir datos de dispositivos maliciosos puede infectar/acceder a los datos del dispositivo receptor



# Describir varios ejemplos de técnicas de ataque específicas de las redes inalámbricas

# Ataques a la red inalámbrica

**War Driving**
- Los atacantes conducen con portátiles con Wi-Fi para detectar redes inalámbricas abiertas

**Asociación errónea de clientes**
- Un atacante instala un punto de acceso fraudulento fuera del perímetro corporativo y engaña a los empleados para que se conecten a él

**Ataque de punto de acceso fraudulento**
- Los puntos de acceso inalámbrico fraudulentos colocados en una red 802. 11 pueden utilizarse para secuestrar las conexiones de los usuarios legítimos de la red

**Ataque de punto de acceso mal configurado**
- Los puntos de acceso mal configurados permiten a los intrusos robar el SSID que les da acceso a la red

**Ataque de punto de acceso "honeypot"**
- Un atacante atrae a las personas utilizando AP falsos

**Ataque de conexión ad hoc**
- Los clientes Wi- Fi se comunican directamente a través de un modo ad hoc que no requiere que un AP retransmita los paquetesAP

**MAC Spoofing**
- Un hacker falsifica la dirección MAC del equipo de un cliente WLAN para actuar como un cliente autorizado y se conecta al AP como el cliente y espía el tráfico

**Asociación no autorizada**
- Los atacantes infectan un equipo víctima y activan los AP para proporcionarles una conexión no autorizada a la red de la empresa

# Ataques a la red inalámbrica

### Ataque de denegación de servicio

- Los ataques DoS inalámbricos interrumpen las conexiones inalámbricas de la red mediante el envío de comandos de "desautentificación" de difusión

### Abuso de la clave WPA-PSK

- Los atacantes olfatean y capturan los paquetes de autenticación y ejecutan un ataque de fuerza bruta para descifrar la clave WPA-PSK

### Reproducción de RADIUS

- Los atacantes reproducen la respuesta válida del servidor RADIUS y se autentican con éxito en el cliente sin credenciales válidas

### Abuso de suplantación de MAC

- Un atacante falsifica la MAC de un cliente e intenta autenticarse en el AP, lo que lleva a la actualización de la información de la dirección MAC en los routers y switches de la red

### WEP Cracking

- Los atacantes olfatean y capturan paquetes y ejecutan un programa de cracking WEP para obtener la clave WEP

### Man-in-the-Middle Attack

- Los atacantes despliegan un AP falso, y falsifican la dirección MAC del cliente para situarse entre el punto de acceso real y el cliente y escuchar el tráfico

### Ataque de fragmentación

- Los atacantes obtienen 1.500 bytes de un algoritmo de generación pseudoaleatoria (PRGA) para generar paquetes WEP falsos que, a su vez, se utilizan para diversos ataques de inyección

### Ataque de señal de interferencia

- Un atacante vigila la zona desde un lugar cercano con un amplificador de alta ganancia, ahogando el punto de acceso legítimo

# Describir las metodologías y los marcos de hacking de los atacantes

# Metodología CEH-Hacking

Según la certificación CEH (Certified Ethical Hacker) de EC-Council, las operaciones de sombrero negro que tienen éxito suelen seguir cinco fases:

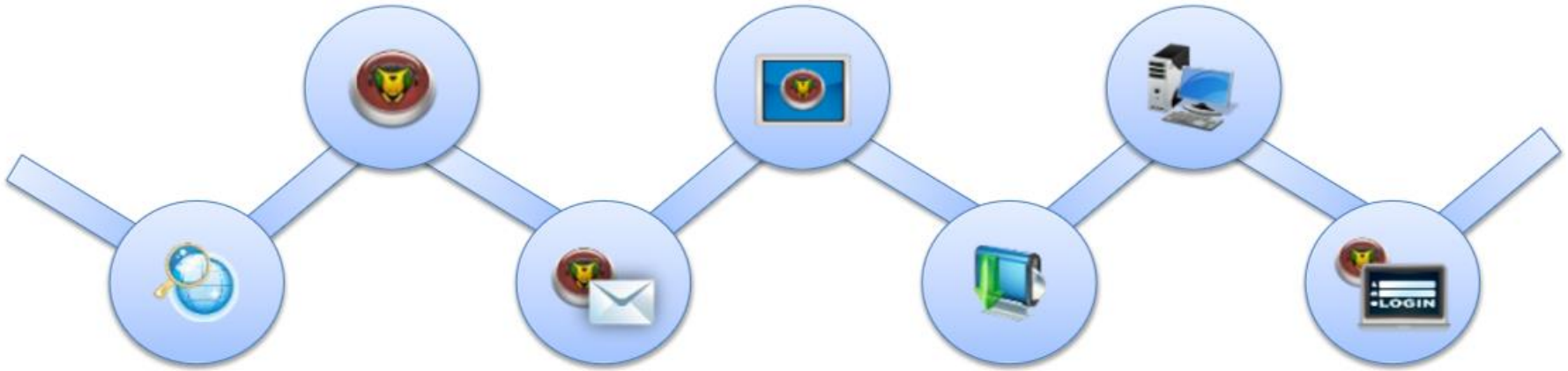
1. Reconocimiento
2. Escaneo
3. Obtención de acceso
4. Mantenimiento del acceso
5. Eliminación de pistas

# Metodología de la cadena de muerte cibernética de Lockheed Martin (Cyber Kill Chain Methodology)

Crear una carga útil maliciosa entregable utilizando un exploit y un backdoor
**Armatización**

Explotar una vulnerabilidad ejecutando código en el sistema víctima
**Explotación**

Crear un canal de mando y control para comunicar y pasar datos de ida y vuelta
**Comando y control**




**Reconocimiento**
Recopilar datos sobre el objetivo para buscar puntos débiles

**Entrega**
Enviar un paquete armado a la víctima mediante correo electrónico, USB, etc.

**Instalación**
Instalar un malware en el sistema de destino

**Acciones sobre los objetivos**
Realizar acciones para alcanzar los objetivos/metas previstos

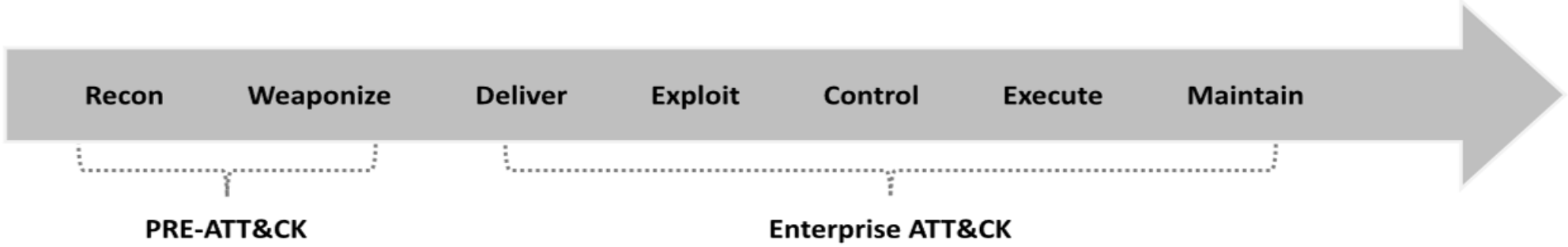
# Marco de ataque de MITRE

MITRE ATT&CK es una base de conocimiento globalmente accesible de las tácticas y técnicas de los adversarios basada en observaciones del mundo real

La base de conocimiento ATT&CK se utiliza como base para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, el gobierno y la comunidad de productos y servicios de ciberseguridad

Las 11 categorías de tácticas dentro de ATT&CK para la empresa se derivan de las últimas etapas (explotar, controlar, mantener y ejecutar) de las siete etapas de la Cyber Kill Chain

Esto proporciona un nivel más profundo de granularidad en la descripción de lo que puede ocurrir durante una intrusión



# Comprender el objetivo fundamental, las ventajas y los retos de la defensa de la red

# Objetivo de la defensa de la red

El objetivo final de la defensa de la red es proteger la información, los sistemas y la infraestructura de la red de una organización contra el acceso no autorizado, el uso indebido, la modificación, la denegación de servicio o cualquier degradación e interrupción

Las organizaciones se basan en los principios de garantía de la información (AI) para lograr una seguridad de defensa en profundidad

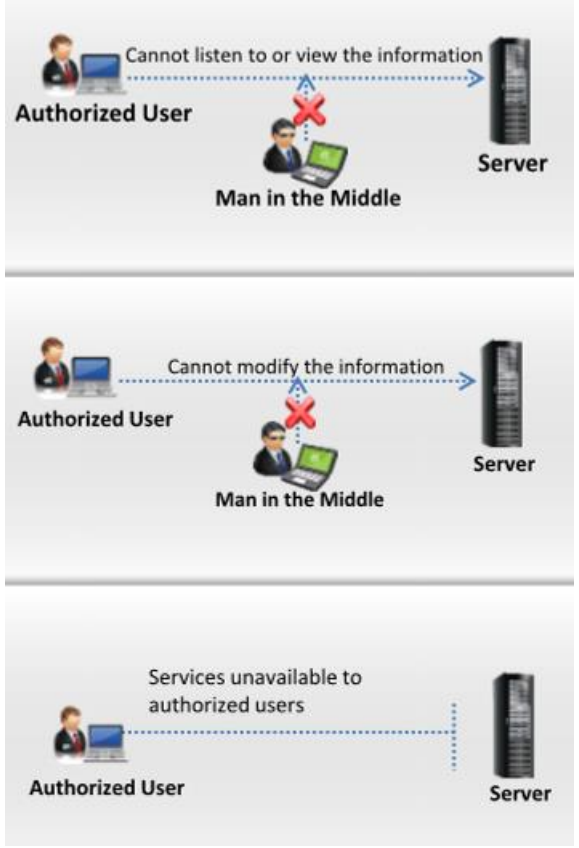
Los principios de garantía de la información (AI) actúan como facilitadores de las actividades de seguridad de una organización para proteger y defender la red de la organización de los ataques a la seguridad

# Principios de seguridad de la información (IA)

Confidencialidad: Garantiza que la información no se revele a partes no autorizadas

Integridad: Garantiza que la información no sea modificada o manipulada por partes no autorizadas

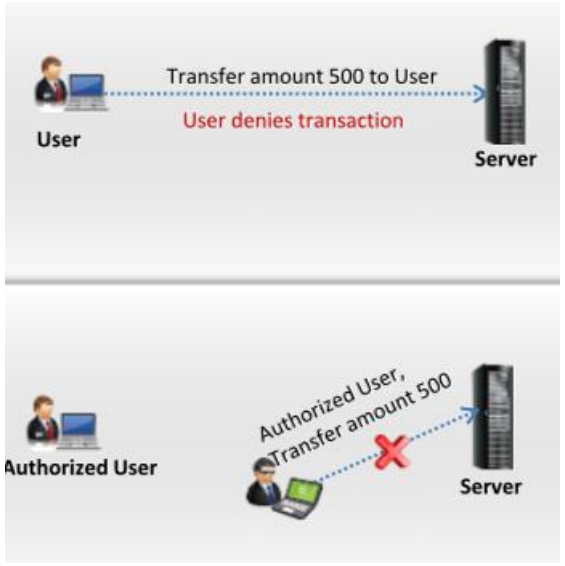
Disponibilidad: Garantiza que la información esté disponible para las partes autorizadas sin ninguna interrupción



# Principios de seguridad de la información (IA)

No repudio: Garantiza que una de las partes de una comunicación no pueda negar el envío del mensajes

Autenticación: Garantiza que la identidad de un individuo es verificada por el sistema o servicio



# Beneficios de la defensa de la red

Proteger los activos de información

Cumplir con las normativas gubernamentales y específicas del sector

Garantizar una comunicación segura con los clientes y proveedores

Reducir el riesgo de ser atacado

Obtener una ventaja competitiva frente a la competencia proporcionando servicios más segros

# Desafíos de la defensa de la red

| | |
|---|---|
| Entornos informáticos distribuidos: | Con el avance de la tecnología moderna y para cumplir con los requisitos de las empresas, las redes se están volviendo vastas y complejas, lo que puede dar lugar a graves vulnerabilidades de seguridad. Los atacantes explotan las vulnerabilidades de seguridad expuestas para comprometer la seguridad de la red |
| Amenazas emergentes: | Las amenazas potenciales a la red evolucionan cada día. Los ataques a la seguridad de la red son cada vez más sofisticados técnicamente y están mejor organizados |
| Falta de conocimientos sobre seguridad de la red: | Las organizaciones no consiguen defenderse de los crecientes ataques a la red debido a la falta de conocimientos sobre seguridad de la red. |

# Explicar la estrategia de seguridad continua/adaptativa

# Defensa de las redes informáticas

La defensa de la red informática implica la aplicación de un conjunto de reglas, configuraciones, procesos y medidas para proteger la integridad, la confidencialidad y la disponibilidad de los sistemas y recursos de información de la red

## Enfoques de seguridad de la red

**Enfoques preventivos**

- Consiste en métodos o técnicas que se utilizan para evitar amenazas o ataques a la red objetivo

**Enfoques reactivos**

- Consiste en métodos o técnicas que se utilizan para detectar ataques en la red objetivo

**Enfoques retrospectivos**

- Consiste en métodos o técnicas que examinan las causas de los ataques, y contienen, remedian, erradican y recuperan los daños causados por el ataque en la red objetivo

**Enfoques proactivos**

- Consiste en métodos o técnicas que se utilizan para tomar decisiones informadas sobre posibles ataques en el futuro a la red objetivo

# Estrategia de seguridad continua/adaptativa

Las organizaciones deben adoptar una estrategia de seguridad adaptativa, que implica la aplicación de los cuatro enfoques de seguridad de la red La estrategia de seguridad adaptativa consiste en cuatro actividades de seguridad correspondientes a cada enfoque de seguridad

**Proteger**

- Incluye un conjunto de contramedidas previas para eliminar todas las posibles vulnerabilidades de la red

**Detectar**

- Implica la monitorización continua de la red y la identificación de las anomalías y sus orígenes

**Responder**

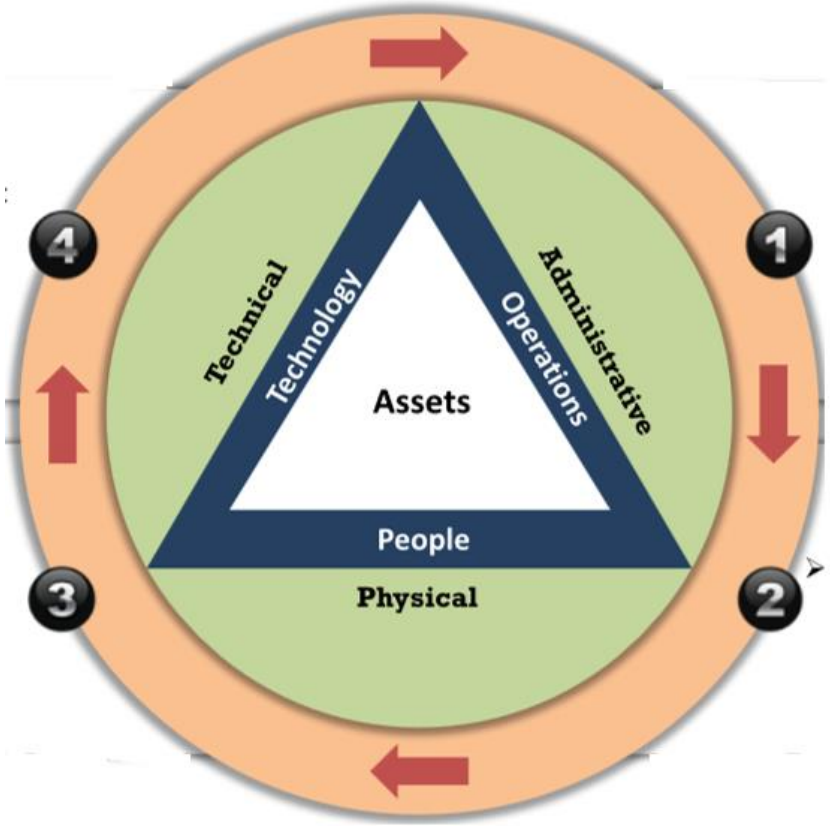
- Incluye un conjunto de acciones para contener, erradicar, mitigar y recuperarse del impacto de los ataques en la red

**Predecir**

- Incluye la identificación de los ataques más probables, los objetivos y los métodos antes de la materialización de un posible ataque

# Estrategia de seguridad continua/adaptativa

**Predecir**
- Evaluación de riesgos y vulnerabilidades
- Análisis de la superficie de ataque Inteligencia de amenazas




**Proteger**
- Estrategia de seguridad de defensa en profundidad
- Proteger los puntos finales
- Proteger la red
- Proteger los datos

**Responder**
- Respuesta a incidentes

**Detectar**
- Vigilancia continua de amenazas

# Seguridad administrativa de la red: Control de seguridad administrativa

La dirección implementa controles administrativos de acceso para garantizar la seguridad de la organización

Ejemplos de controles administrativos de seguridad

Cumplimiento del Marco normativo

Vigilancia y supervisión de los empleados

Sensibilización y formación en materia de seguridad

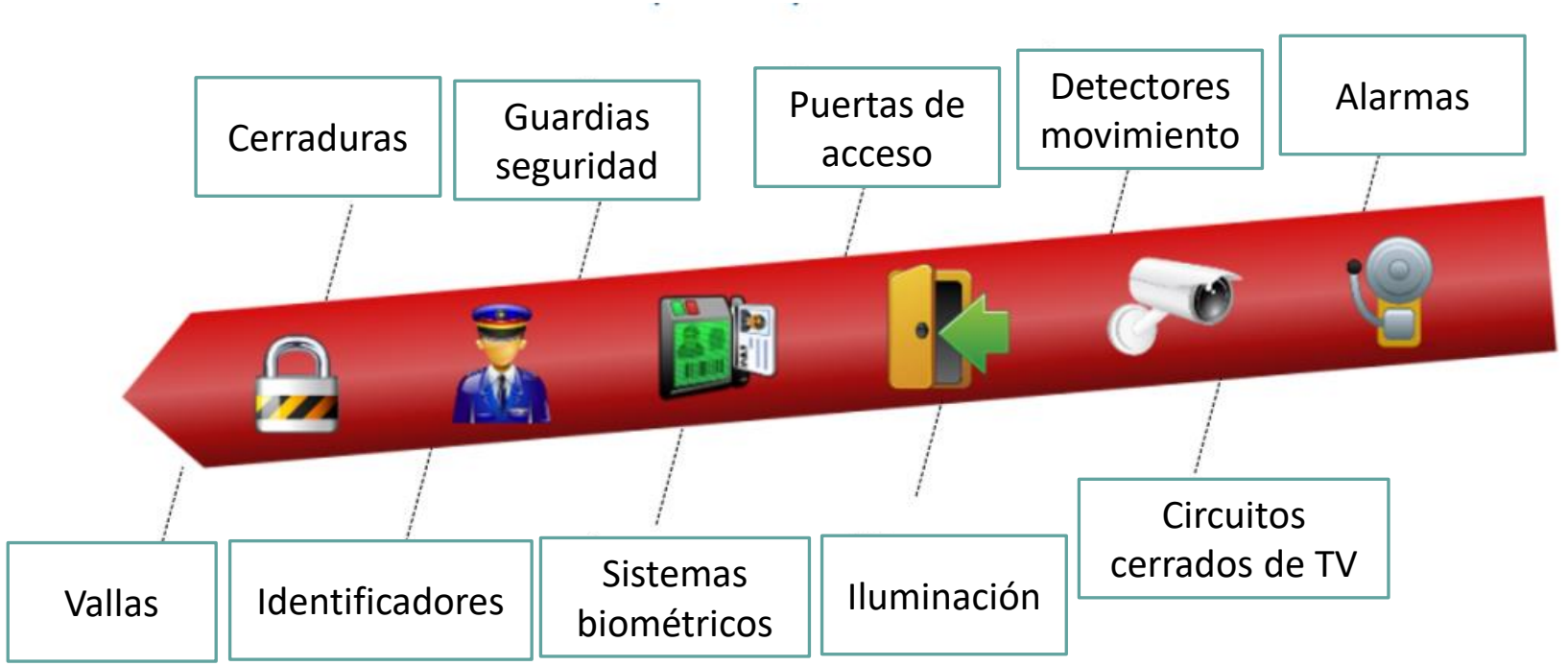
Política de seguridad

Clasificación de la información

# Seguridad física de la red: Controles de seguridad física

Se trata de un conjunto de medidas de seguridad adoptadas para evitar el acceso no autorizado a los dispositivos físicos

Ejemplos de controles de acceso físico



# Seguridad técnica de la red: Controles técnicos de seguridad

Se trata de un conjunto de medidas de seguridad adoptadas para proteger los datos y los sistemas del personal no autorizado

Ejemplos de controles técnicos de seguridad

# Tecnología, operaciones y personas

La selección adecuada de la tecnología, las operaciones bien definidas y el personal cualificado son necesarios para la aplicación eficaz de las estrategias de seguridad

**Tecnología**:

La selección de la tecnología adecuada es crucial, ya que una selección incorrecta de la tecnología puede proporcionar una falsa sensación de seguridad.

Ejemplo de cuestionario para facilitar la selección adecuada de la tecnología:

- ¿Qué cortafuegos, IDS, antivirus, etc., son necesarios para la red?
- ¿Qué tipo de algoritmo de cifrado debe utilizarse?
- ¿Es más adecuado para la red un mecanismo de acceso centralizado o distribuido?
- ¿Qué tipo de complejidad de las contraseñas debe adoptarse?
- ¿Deben colocarse los servidores críticos en un segmento separado?

# Tecnología, operaciones y personas

**Operaciones**:

Las implantaciones tecnológicas no son suficientes por sí mismas, sino que deben estar respaldadas por operaciones bien definidas

Ejemplos de operaciones:

- No basta con implantar la tecnología adecuada, sino que las tecnologías implantadas deben estar respaldadas por operaciones bien gestionadas
- Creación y aplicación de políticas de seguridad
- Creación y aplicación de procedimientos estándar de funcionamiento de la red
- Planificación de la continuidad de la actividad
- Gestión del control de la configuración
- Creación y aplicación de procesos de respuesta a incidentes
- Planificación de la recuperación de desastres
- Concienciación y formación en materia de seguridad Aplicación de la seguridad como cultura

# Tecnología, operaciones y personas

**Las personas**:

La tecnología adecuada y las operaciones bien definidas no pueden sustituir a las personas cualificadas, que son necesarias para implantar la tecnología y gestionar las operaciones bien definidas.

Equipo azul:

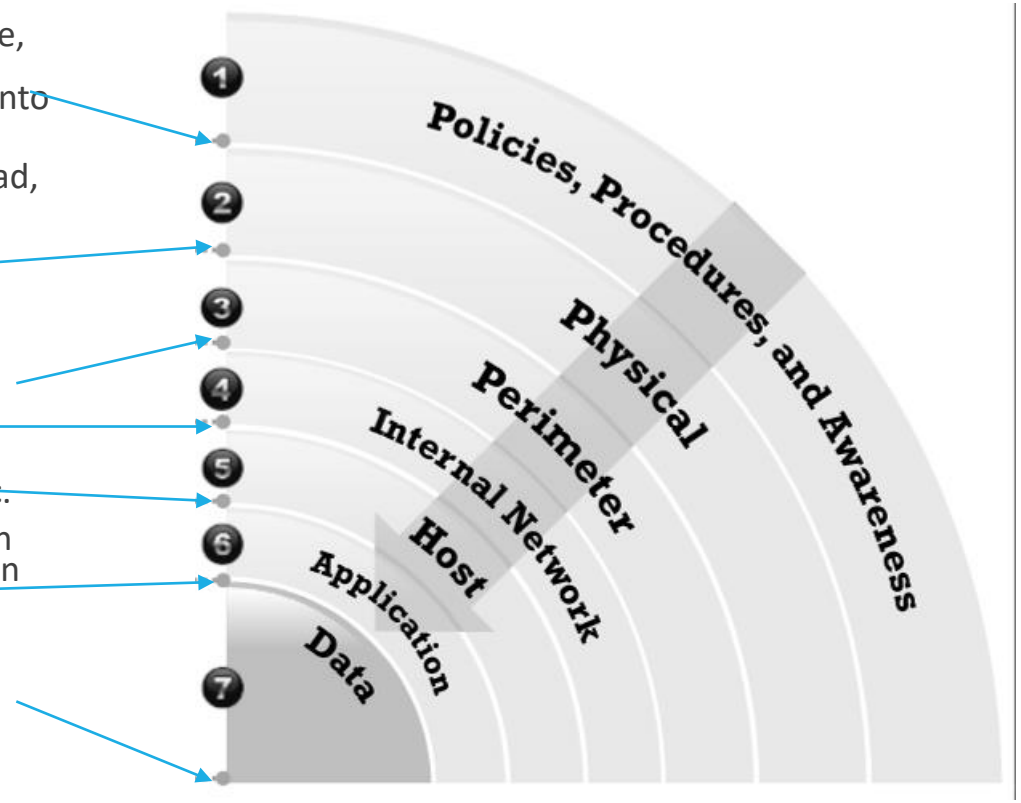
- Las personas que son responsables colectivamente de desarrollar una defensa eficaz de la red suelen formar parte del equipo azul
- El equipo azul se encarga de determinar la adecuación global de las medidas de seguridad. Examinan el estado actual de la seguridad y las deficiencias de seguridad existentes en la red, y proponen medidas de seguridad eficaces para defender la red de diversos tipos de ataques
- El equipo azul incluye a defensores de la red como el administrador de la red, el administrador/ingeniero de seguridad de la red, los analistas de seguridad, los técnicos de la red, los usuarios finales y las personas implicadas en las operaciones de seguridad de la red.

# Explicar la estrategia de seguridad de defensa en profundidad

# Estrategia de seguridad de defensa en profundidad: seguridad en varios niveles

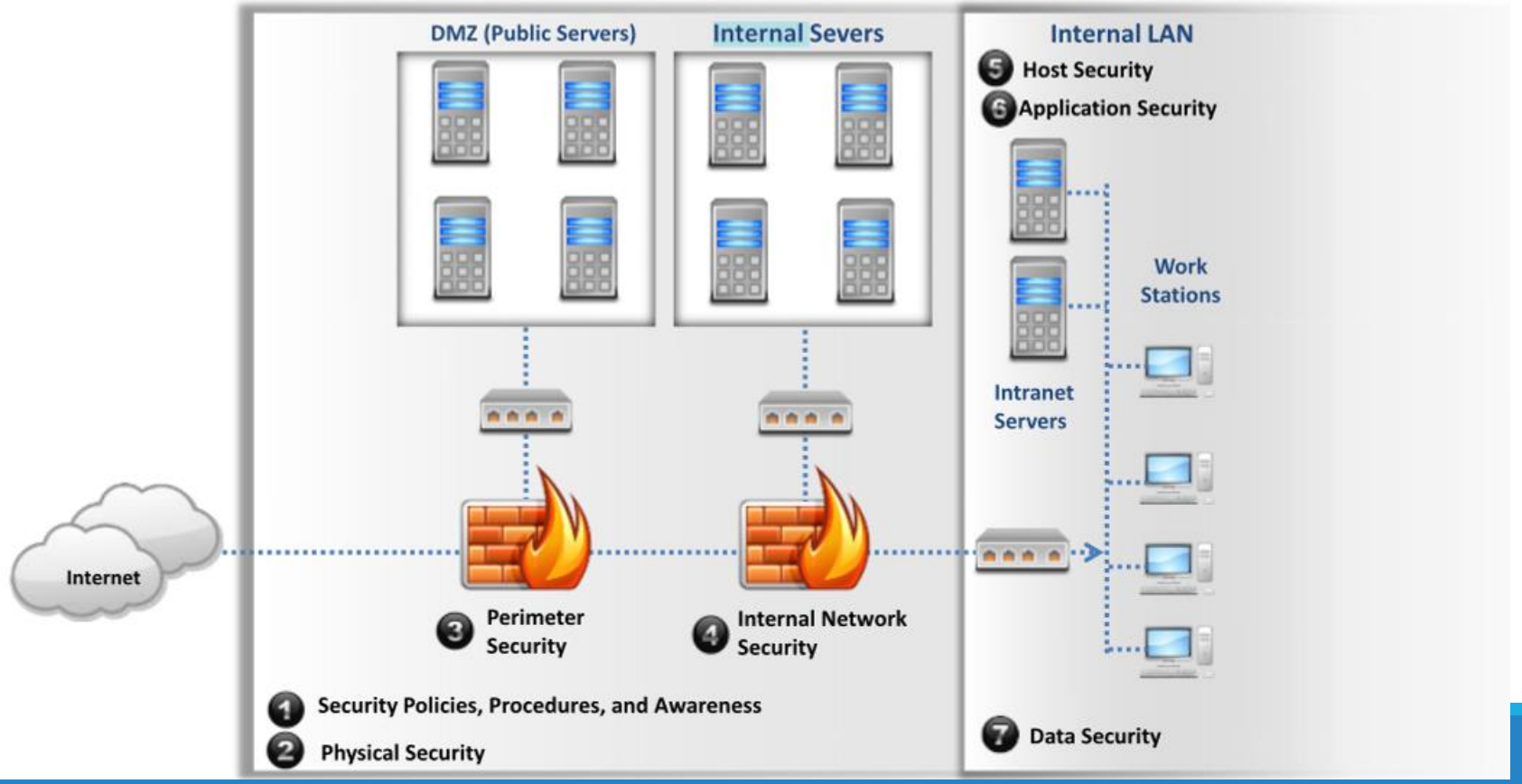
Los datos son de suma importancia y están en el centro de cualquier organización

- Políticas relacionadas con el acceso a Internet, uso aceptable, cuenta de usuario, cortafuegos, seguridad del correo electrónico, contraseñas, seguridad física, BYOD. Cumplimiento de normas como ISO/IEC 27001, PCI-DSS, HIPAA, etc.
- Cerraduras físicas, controles de acceso, personal de seguridad, sistemas contra incendios, suministro de energía, videovigilancia, iluminación, sistema de alarma, etc.
- Servidores, DNS, routers, cortafuegos, conmutadores.
- Routers, servidores, conmutadores, cortafuegos
- SO , antivirus, gestión de parches, gestión de contraseñas, registro, etc.
- Listas negras, listas blancas, gestión de parches, gestión de contraseñas, configuración de aplicaciones, cortafuegos, etc.
- Cifrado, hashing, controles de acceso a los datos, prevención de fugas de datos, copia de seguridad de datos, recuperación de datos, retención de datos, eliminación de datos, etc.Defensa



# Estrategia de seguridad de defensa en profundidad: seguridad en varios niveles

Las organizaciones deben adoptar una estrategia de seguridad de defensa en profundidad para proteger eficazmente sus sistemas y recursos de información.



# Resumen del módulo

Una amenaza es un acto en el que un adversario intenta obtener acceso no autorizado a la red de una organización explotando las vías de comunicación

La intención, la capacidad y la oportunidad siempre están detrás de la presencia de una amenaza.

Los atacantes siguen varias metodologías de ataque para la ejecución exitosa de un ataque

La defensa de la red informática incluye un conjunto de procesos y medidas de protección adoptadas para defender la red contra la denegación, degradación e interrupción del servicio o de la red

El equipo azul es responsable colectivamente de desarrollar una defensa eficaz de la red

Las organizaciones deben adoptar una mejora continua de la seguridad y estrategias de seguridad de defensa en profundidad para una protección eficaz de sus sistemas y recursos de información