

Estudio de tipos de ataques.

¿CÓMO ACTÚAN LOS PIRATAS INFORMÁTICOS?

**SERVIDORES WEB DE
ALTAS PRESTACIONES
2018-2019**



Realizado por:
Francisco José González García
Pablo Robles Molina

Índice

Introducción.....	3
1. Ataque DoS.....	4
2. Escaneo de puertos	9
3. ARP Spoofing.....	10
4. Ataque Man-In-The-Middle	11
5. Ataque Ingeniería Social	18
6. OS Finger Printing.....	21
7. Conocer los puertos expuestos.....	23
8. KeyLoggers	25
9. ICMP Tunneling.....	27
10. Ataque de secuencia TCP	28
11. CAM Table Overflow	30
12. Ataques a Aplicaciones Web	34
13. Virus y Worms	42
14. Malware, Adware y Spyware.....	42
15. Troyanos	45
Bibliografía	49

Introducción

En el mundo de la seguridad informática es imposible definir un listado de tipos de ataques de forma realista debido a su constante estado de cambio, pero mediante esta base de datos de amenazas, veremos algunos de los más conocidos o generalizados. Para poder mantener un cierto grado de seguridad, primero debemos conocer **cómo funcionan** dichas amenazas (en qué consisten y cómo pueden atacarnos).

La última década ha sido testigo del cambio de paradigma en el que los hackers buscan explotar vulnerabilidades dentro de las organizaciones e infraestructuras tanto nacionales como internacionales. Con el fin de contrarrestar esta tendencia, todos tenemos que cambiar nuestra perspectiva hacia la forma en que percibimos la seguridad, conocer ciertos ataques y cómo podemos aprender de los mismos para estar lo mejor preparados posibles.

A continuación se hablará de los ataques o amenazas más conocidas, sus variantes y qué medidas tomar para prevenirlos, combatirlos o mitigar su acción. También se hará especial hincapié en aquellos ataques que afectan de manera más directa a los servidores web.

1. Ataque DoS

En un ataque de denegación de servicio (DoS), un atacante intenta evitar la legitimidad de que los usuarios accedan a información o a servicios. El tipo más común y obvio de ataque DoS ocurre cuando un atacante "inunda" una red con información. Cuando escribimos una URL de una página web en nuestro navegador, estamos enviando una solicitud al servidor web del sitio para poder ver la página en concreto. El servidor solo puede procesar una cierta cantidad de solicitudes de una vez, por lo que si un atacante sobrecarga el servidor con solicitudes, no puede procesarse dicha solicitud. Esto es lo que se denomina "denegación de servicio" ya que no se puede acceder al sitio.

Síntomas de DoS

- Rendimiento de la red inusualmente lento (abrir archivos o acceder a sitios web)
- Indisponibilidad de un sitio web en particular
- Incapacidad para acceder a cualquier sitio web
- Aumento dramático en la cantidad de spam que recibimos

Tipos de ataques DoS:

- a. **ICMP Flood Attack:** Es una técnica DoS que pretende agotar el ancho de banda de la víctima. Consiste en enviar de forma continuada un número elevado de paquetes ICMP Echo request (ping) de tamaño considerable a la víctima, de forma que esta ha de responder con paquetes ICMP Echo reply (pong) lo que supone una sobrecarga tanto en la red como en el sistema de la víctima. Dependiendo de la relación entre capacidad de procesamiento de la víctima y el atacante, el grado de sobrecarga varía, es decir, si un atacante tiene una capacidad mucho mayor, la víctima no puede manejar el tráfico generado.
- b. **Tear Drop Attack:** Una serie de paquetes de datos se envían al ordenador de destino con superposición de valores de campo y cargas útiles de gran tamaño. Como resultado, el objetivo no puede volver a ensamblar estos paquetes y se fuerza a que se bloquee o incluso a reiniciar.
- c. **Smurf Attack:** El atacante envía una gran cantidad de solicitudes de eco ICMP a la dirección IP Broadcast. Estas solicitudes ICMP tienen una dirección de origen falsificada de la víctima. Por ello, si el dispositivo de enrutamiento entrega tráfico a esas direcciones de difusión, entrega la transmisión IP a todos los hosts, la mayoría de las direcciones IP envían un Mensaje de respuesta ECHO. Sin

embargo, en una red de difusión de acceso múltiple, cientos de ordenadores podrían responder a cada paquete cuando la red objetivo se vea abrumada por todos los mensajes enviados simultáneamente. La red no podrá funcionar con normalidad.

- d. **SYN Flood:** La inundación SYN envía una inundación de paquetes TCP / SYN, a menudo con un remitente falsificado en dirección. Cada uno de estos paquetes se maneja como una solicitud de conexión, causando al servidor una conexión semiabierta, mediante el envío de un paquete TCP / SYN-ACK , y esperando un paquete en respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente está falsificada, la respuesta nunca llega. Estos halfopen en conexiones, saturan la cantidad de conexiones disponibles que el servidor puede hacer, evitando que responda a solicitudes legítimas hasta después de que el ataque termine.
- e. **Land Attack:** El atacante envía un paquete TCP SYN falsificado en el que la dirección IP del objetivo se completa en los campos de origen y destino. Al recibir el paquete falsificado, el objetivo se confunde y se bloquea. Estos tipos de ataques son detectados por Anti-virus.
- f. **Jolt Dos Attack:** Un atacante fragmenta el paquete ICMP de tal manera que el objetivo no puede volver a armarlo, como consecuencia, el uso de la CPU aumenta y se crean cuellos de botella y estrechamientos.
- g. **Fraggle Dos Attack:** El atacante envía una gran cantidad de tráfico de solicitudes de eco UDP a una dirección IP de Difusión. Estos paquetes UDP tienen una dirección fuente falsificada de la víctima prevista. Por ello, si el dispositivo de enrutamiento entrega tráfico a esas direcciones, entrega la transmisión IP a todos los hosts, donde la mayoría de las direcciones IP envían un mensaje de respuesta ECHO. Sin embargo, en una red de difusión de acceso múltiple, cientos de ordenadores podrían responder a cada paquete cuando la red objetivo se vea abrumada por todos los mensajes enviados simultáneamente. La red no podrá funcionar con normalidad.

Ping Flood

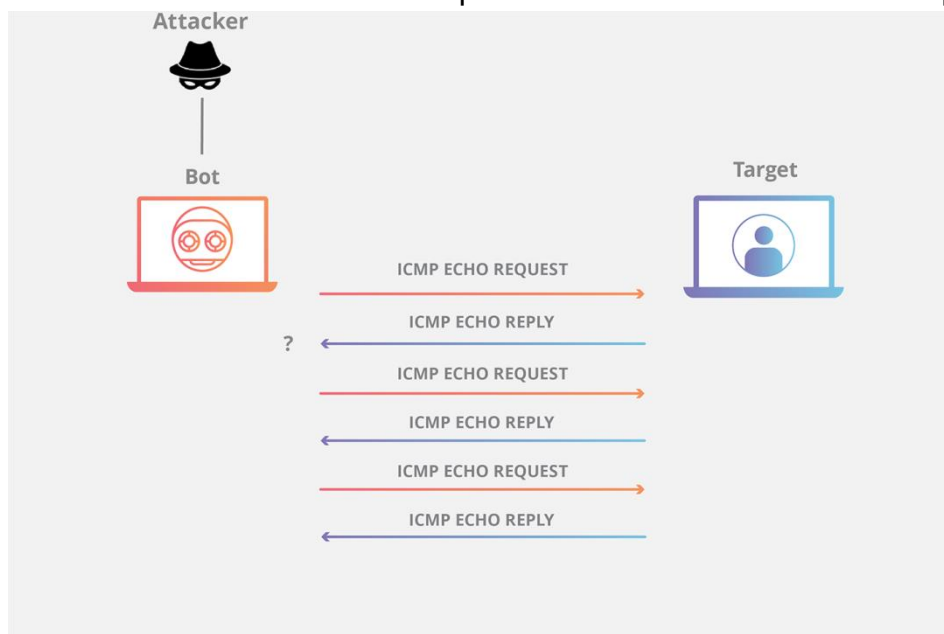
Una inundación de ping es un ataque de denegación de servicio en el que el atacante intenta abrumar un dispositivo de destino con paquetes de solicitud de eco ICMP, lo que hace que el objetivo sea inaccesible para el tráfico normal. Cuando el tráfico de ataques proviene de múltiples dispositivos, el ataque se convierte en un ataque de denegación de servicio o DDoS distribuido.

El Protocolo de mensajes de control de Internet (ICMP) , que se utiliza en un ataque de Ping Flood, es un protocolo de capa de Internet que los dispositivos de red usan para comunicarse. Las herramientas de diagnóstico de red traceroute y ping operan utilizando ICMP. Comúnmente, los mensajes de solicitud de eco ICMP y de respuesta de eco se utilizan para hacer ping a un dispositivo de red con el fin de saber su estado, la conectividad del dispositivo y la conexión entre remitente y el dispositivo.

Una solicitud ICMP requiere de recursos del servidor para procesar cada solicitud y enviar una respuesta. La solicitud también necesita ancho de banda tanto en el mensaje (solicitud de eco) como en la respuesta saliente (respuesta de eco). El ataque de Ping Flood pretende abrumar la capacidad del dispositivo objetivo para responder a la gran cantidad de solicitudes y sobrecargar la conexión de red con tráfico falso. Al tener muchos dispositivos en una red de bots que apunta a la misma propiedad de Internet o componente de infraestructura con solicitudes ICMP, el tráfico de ataques aumenta sustancialmente, lo que potencialmente provoca una interrupción de la actividad normal de la red.

La forma DDoS de una Inundación de Ping (ICMP) se puede dividir en 2 pasos repetidos:

1. El atacante envía muchos paquetes de solicitud de eco ICMP al servidor de destino utilizando múltiples dispositivos.
2. El servidor de destino envía un paquete de respuesta de eco ICMP a la dirección IP de cada dispositivo solicitante como respuesta.



El efecto dañino de un Ping Flood es directamente proporcional al número de solicitudes realizadas al servidor de destino. A diferencia de los ataques DDoS basados en la reflexión, como la amplificación NTP y la amplificación DNS, el tráfico de ataques Ping Flood es simétrico; La cantidad de ancho de banda que recibe el dispositivo de destino es simplemente la suma del tráfico total enviado desde cada bot.

¿Cómo mitigar un ataque de ping?

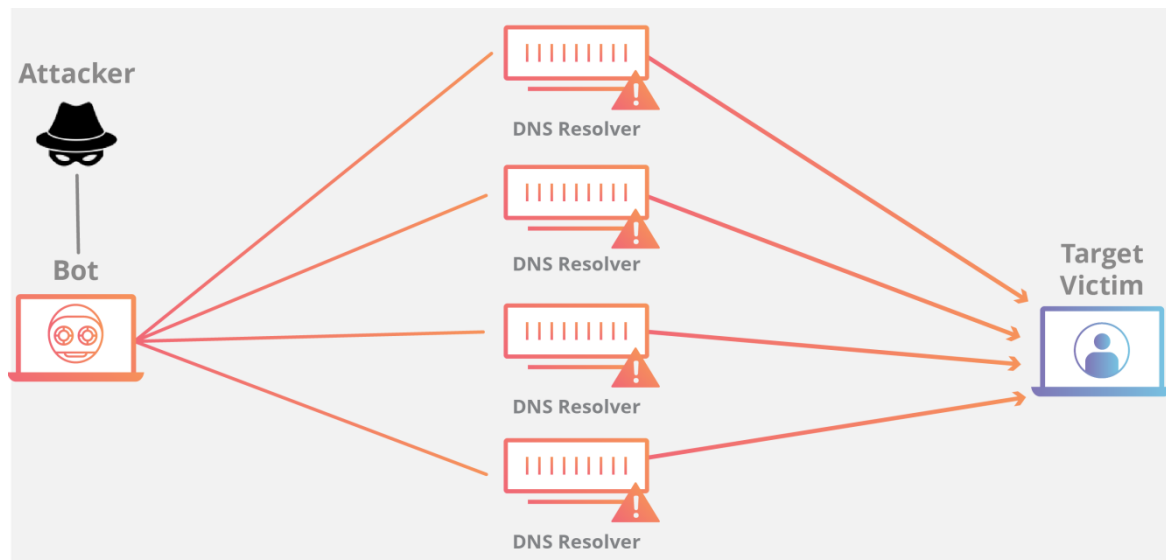
La desactivación de un ping flood se realiza más fácilmente al desactivar la funcionalidad ICMP del enrutador, el ordenador u otro dispositivo de destino. Un administrador de red puede acceder a la interfaz administrativa del dispositivo y deshabilitar su capacidad para enviar y recibir cualquier solicitud utilizando el ICMP, eliminando de manera efectiva tanto el procesamiento de la solicitud como la Respuesta de eco. La consecuencia de esto es que todas las actividades de la red que involucran ICMP están deshabilitadas, lo que hace que el dispositivo no responda a las solicitudes de ping, las solicitudes de traceroute y otras actividades de la red.

Ping de la muerte

El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. Hoy en día, el sistema operativo descarta dichos paquetes por sí mismo.

Distributed Denial of Service (DDoS)

Ataque distribuido de denegación de servicio (DDoS): un atacante puede usar un equipo para atacar a otro. Al aprovechar las vulnerabilidades o debilidades de seguridad, un atacante podría tomar el control del PC / Servidor. Él o ella podría obligar al PC a enviar grandes cantidades de datos a un sitio web o enviar correo no deseado a direcciones de correo electrónico particulares. El ataque se "distribuye" porque el atacante está utilizando varios PCs, incluida la suya, para lanzar el ataque de denegación de servicio. Actualmente dichos ataques son lanzados desde las Botnet.



Ejemplo de ataque con ampliación

¿Cómo prevenir ataques DDoS?

1. Aplicación de filtrado de enrutador
2. Bloquear direcciones IP sin usar
3. Permitir el acceso a la red solo al tráfico deseado
4. Deshabilitar servicios de red innecesarios
5. Actualización de antivirus regularmente
6. Tener una muy buena política de contraseñas
7. Limitar la cantidad de ancho de banda de la red
8. Uso de la red de filtrado de acceso

2. Escaneo de puertos

El escaneo de puertos se basa en la evaluación de vulnerabilidades que se logra con analizadores de red. Esto permite verificar la seguridad de un equipo en una red, a través del análisis de sus puertos, localizando los puertos abiertos, permitiendo la ejecución de una técnica adicional (normalmente un Xploit), con el fin de tomar control remoto del pc víctima.

¿Cómo funciona?

Los puertos TCP/IP que existen son 65.535, y cada uno de ellos cumple una función estándar a nivel internacional. Cuando se lleva a cabo un escaneo de vulnerabilidades, lo que se logra es identificar los puertos que se encuentran abiertos en un sistema. Esto se logra enviando solicitudes puerto por puerto, y analizando cada una de las respuestas.

En algunos casos es posible incluso determinar el tipo de sistema operativo que se utiliza en la máquina víctima, así como también las versiones de las versiones de las aplicaciones que se están utilizando para los puertos que se encuentren activos.

Tipos de Escaneo de Puertos

Existen dos métodos para el escaneo de puertos, uno que consiste en adquirir de manera activa la información, y otro de manera pasiva:

- **Adquisición Activa de Información:** En esta metodología, se envían grandes cantidades de paquetes de información, con encabezados que no satisfacen los estándares, con el fin de analizar la información de respuesta, y así lograr la identificación incluso, de las versiones de las aplicaciones utilizadas para el manejo de los puertos abiertos y activos.
- **Adquisición Pasiva de Información:** Es un método no agresivo que además de ser efectivo, logra evadir los IDS (Intruder Detection Systems) Sistemas de Detección de Intrusos por sus siglas en inglés. Funciona de manera similar al Activo, realizando análisis de los campos de los datagramas IP que van por la red, utilizando un rastreador de puertos. Dado que el análisis realizado de esta manera divide los valores de los campos del datagrama, convirtiéndolos en pequeños fragmentos, toma mucho más tiempo que la primera metodología, pero también, reduce incluso en algunos casos, totalmente las posibilidades de ser detectado mientras realiza el escaneo.

Aspectos Positivos del Escaneo de Puertos

Los administradores de red deben tener a mano un escáner de puertos, con el fin de mantener en evaluación constante la infraestructura que tiene a su cargo, y así poder dar pronta solución a las fallas detectadas a tiempo.

Un escaneo a profundidad puede terminar en un ataque Xploit, y un ataque de esta magnitud, puede terminar en un Defacement, una Inclusión Remota de Archivos, o la toma de control total de manera remota del servidor.

3. ARP Spoofing

El principio del ARP Spoofing es enviar mensajes ARP falsos (falsificados, o spoofed) a la Ethernet. Normalmente la finalidad es asociar la dirección MAC del atacante con la dirección IP de otro nodo (el nodo atacado), como por ejemplo la puerta de enlace predeterminada (gateway). Cualquier tráfico dirigido a la dirección IP de ese nodo, será erróneamente enviado al atacante, en lugar de a su destino real. El atacante, puede entonces elegir, entre reenviar el tráfico a la puerta de enlace predeterminada real (ataque pasivo o escucha), o modificar los datos antes de reenviarlos (ataque activo). El atacante puede incluso lanzar un ataque de tipo DoS (Denegación de Servicio) contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.

El ataque de ARP Spoofing puede ser ejecutado desde una máquina controlada (el atacante ha conseguido previamente hacerse con el control de la misma: intrusión), o bien la máquina del atacante está conectada directamente a la LAN Ethernet.

Tipos de ataques ARP Spoofing:

1. **Ataque de inundación MAC:** En un ataque típico de inundación MAC, un switch se inunda con paquetes, cada uno con diferentes direcciones MAC de origen. La intención es consumir la memoria limitada reservada en el switch para almacenar la tabla de traducción de puerto a físico de MAC.

El resultado de este ataque hace que el switch ingrese a un estado llamado modo de apertura fallida, en el cual todos los paquetes entrantes se emiten en todos los puertos (como con un concentrador), en lugar de simplemente hacia abajo del puerto correcto según la operación normal. Un usuario malintencionado podría utilizar un analizador de paquetes (como Wireshark) ejecutándose en modo promiscuo para capturar datos confidenciales de otros ordenadores

(como contraseñas no encriptadas, correo electrónico y conversaciones de mensajería instantánea), que no serían accesibles si el interruptor funcionara con normalidad.

2. **Envenenamiento de caché DNS:** Esta es una situación creada o no intencionalmente creada que proporciona datos a un servidor de nombres de almacenamiento en caché que no se originó en fuentes autorizadas del Sistema de nombres de dominio (DNS). Esto puede suceder a través del diseño incorrecto del software, la mala configuración de los servidores de nombres y los escenarios diseñados maliciosamente que explotan la arquitectura tradicionalmente abierta del sistema DNS. Una vez que un servidor DNS ha recibido datos no auténticos y los almacena en caché para aumentar el rendimiento en el futuro, se considera envenenado, proporcionando los datos no auténticos a los clientes del servidor.
3. **IP Spoofing:** La suplantación de IP se refiere a la creación de paquetes de Protocolo de Internet (IP) con un forjado de dirección IP de origen, llamada suplantación de identidad, con el propósito de ocultar la identidad del remitente o hacerse pasar por otro sistema informático.

4. Ataque Man-In-The-Middle

Como sugiere su nombre en inglés, en este método se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente: una página de banca online o una cuenta de correo electrónico. Estos ataques son realmente efectivos y, a su vez, muy difíciles de detectar por el usuario, quien no es consciente de los daños que puede llegar a sufrir.

El concepto de un ataque MiTM es muy sencillo. Además, no se limita únicamente al ámbito de la seguridad informática o el mundo online. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas. Por ejemplo, en el mundo offline, se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos. En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente; pasando totalmente desapercibido para poder alcanzar con éxito la meta.

En el ataque MiTM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario. Esto se puede realizar configurando el router malicioso para que parezca legítimo o atacando un error del mismo e interceptando la sesión del usuario. En el primero de los casos, el atacante

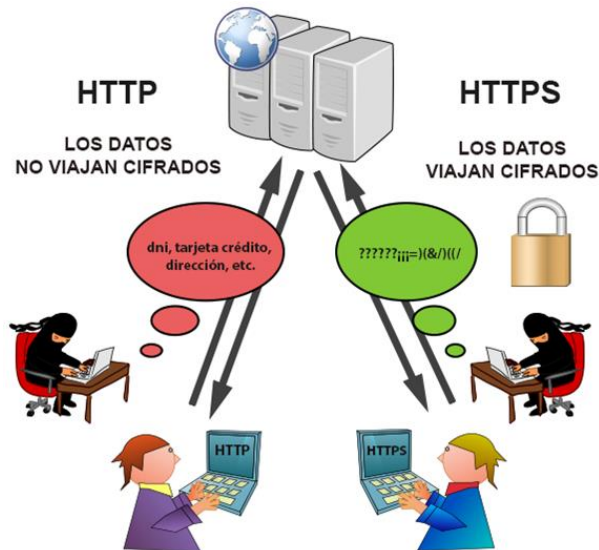
configura su ordenador u otro dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería). Después, el usuario se conecta al “router” y busca páginas de banca o compras online, capturando el criminal las credenciales de la víctima para usarlas posteriormente. En el segundo caso, un delincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router. Éste es el método más complejo de los dos, pero también el más efectivo; ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.

Una variante más reciente de este tipo de ataque es el ataque man-in-the-browser. En este contexto, el ciberdelincuente usa una serie de métodos para insertar un código malicioso en el equipo de la víctima, el cual funciona dentro del navegador. Este malware registra, silenciosamente, los datos enviados entre el navegador y las páginas. Estos ataques han ganado en popularidad porque permiten al delincuente atacar a un grupo mayor de víctimas sin la necesidad de estar cerca de éstas.

Problemas de http vs https

El Protocolo de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol o HTTP) es el protocolo de comunicación que permite las transferencias de información en la World Wide Web (internet). Sigue el esquema petición-respuesta y aporta una capa de abstracción entre equipos de una red que permite que cualquier dispositivo pueda comunicarse con cualquier otro sin importar que hardware o software esté corriendo o la configuración que tenga cada uno.

Centrándonos en el tema de la seguridad, este protocolo envía los paquetes en texto plano y sin cifrar lo que supone un grave problema de seguridad ya que cualquiera con unos conocimientos básicos podría interceptar estos paquetes y ver la totalidad de su contenido. Esto no supondría mucho problema si solo fueran páginas html las que sirviéramos en nuestro servidor, pero si en cambio en nuestro sitio manejamos datos sensibles como datos bancarios o de inicio de sesión sería una grave brecha de seguridad ya que como veremos posteriormente es muy fácil obtener estos datos si no están cifrados.



Para solucionar este problema se creó el Protocolo seguro de transferencia de hipertexto (en inglés: Hypertext Transfer Protocol Secure o HTTPS). Estrictamente hablando, HTTPS no es un protocolo separado, pero refiere el uso del HTTP ordinario sobre una Capa de Conexión Segura cifrada Secure Sockets Layer (SSL) o una conexión con Seguridad de la Capa de Transporte (TLS). Para preparar un servidor web que acepte conexiones HTTPS, el administrador debe crear un certificado de clave pública para el servidor web. Este certificado debe estar firmado por una autoridad de certificación para que el navegador web lo acepte.

Una vez configurado, los paquetes servidos por nuestro servidor pasarán a estar cifrados y será prácticamente imposible que nadie, aunque intercepte estos mensajes, pueda ver su contenido.

Interceptando datos de inicio de sesión

En este ejemplo usaremos la herramienta *wireshark* para interceptar la comunicación entre un cliente un sitio web de una librería que funciona con http sin cifrado de los paquetes y veremos como de simple es obtener los datos de inicio de sesión del cliente y apoderarnos de su cuenta en unos pocos pasos.



Figura 1: Página de login de la librería que vamos a atacar

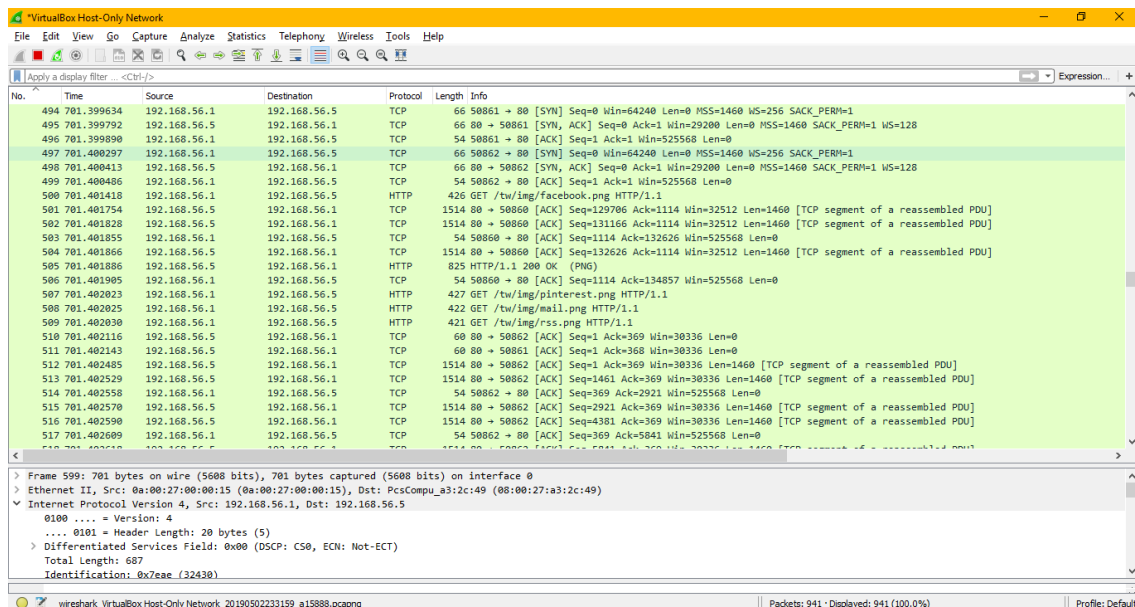


Figura 2: Paquetes enviados entre cliente y servidor

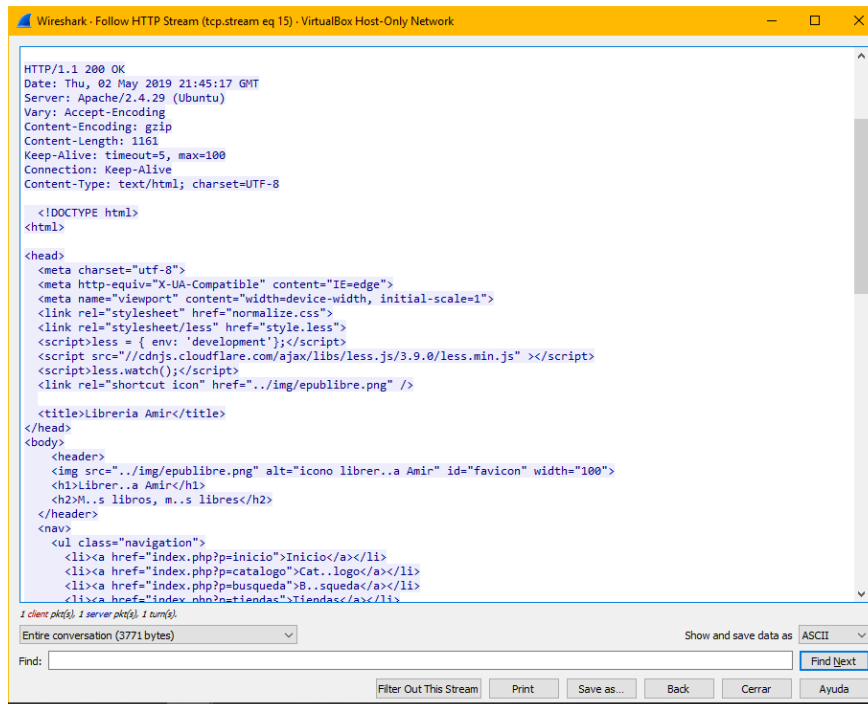


Figura 3: Ejemplo de código HTML obtenido a través de la traza HTTP

Una vez identificados los paquetes que queremos examinar por la url o la ip del servidor. Procedemos a examinar la traza HTTP donde vemos el paquete completo que contiene el contenido de la página o los datos de inicio de sesión que queremos.

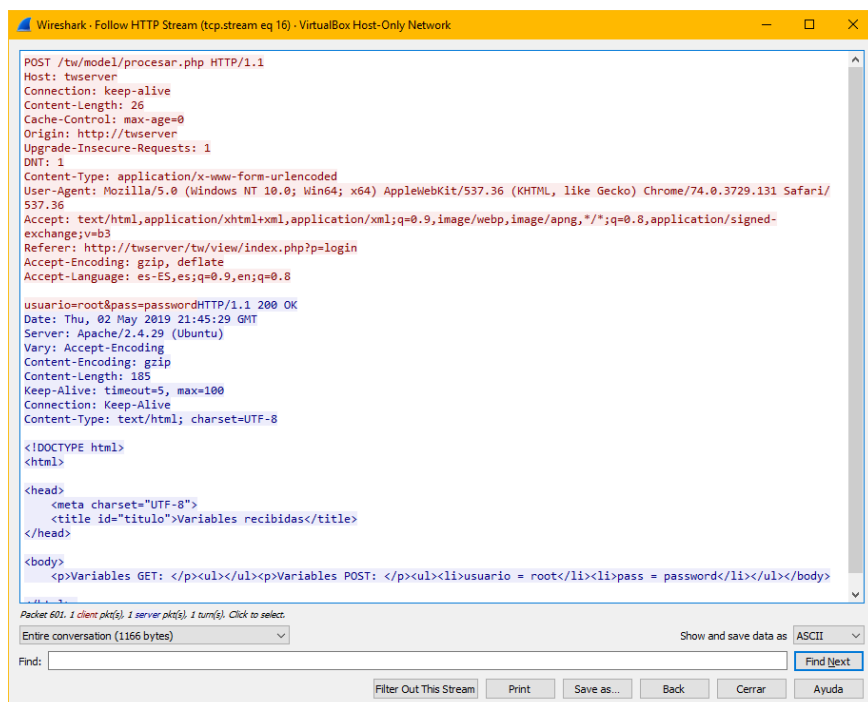


Figura 4: Datos de inicio de sesión capturados

Como vemos en la última línea hemos obtenido el usuario y la contraseña con tan solo examinar los paquetes y saber interpretar cuál de ellos son los que transportaban los datos de inicio de sesión.

¿Cómo prevenir ataques Man-In-The-Midle?

La mayoría de metodos usan un router/ servidor y no permiten que el usuario controle la seguridad de la transacción que realiza. Este método de defensa usa un sistema de cifrado fuerte entre el cliente y el servidor. En este caso, el servidor se verifica a sí mismo presentando un certificado digital y se establece un canal cifrado entre el cliente y el servidor a través del que se envía la información confidencial. Además, los usuarios pueden protegerse de estos ataques evitando conectarse a routers WiFi abiertos o usando plugins de navegador como HTTPS Everywhere o ForceTLS; los cuales establecen una conexión segura siempre que sea posible. Sin embargo, cada una de estos métodos tiene sus límites y existen ejemplos de ataques como SSLStrip o SSLSniff que pueden invalidar la seguridad de las conexiones SSL.

La tecnología PKI (public key infrastructure) puede ayudar a protegerse de algunos de los tipos de ataques mencionados anteriormente. De entre las posibles soluciones destacamos:

1. **S / MIME**: Extensiones de correo de Internet seguras / multipropósito, o S / MIME abrevia, encripta los correos electrónicos en reposo o en tránsito, asegurando que solo los destinatarios puedan leerlos y sin dejar margen para que los piratas informáticos se introduzcan y alteren nuestros mensajes. Además, S / MIME permite firmar digitalmente los correo electrónico con un Certificado digital único para cada persona.

Esto vincula la identidad virtual a nuestro correo electrónico y brinda a los destinatarios la garantía de que el correo electrónico que recibieron en realidad proviene de nosotros (a diferencia de un hacker que accede a nuestro servidor de correo).

Si bien los piratas informáticos pudieran tener acceso a los servidores de correo de las empresas para firmar digitalmente los mensajes, también necesitarían acceder a las claves privadas de los empleados, que generalmente se almacenan de forma segura en otro lugar. Estandarizar la firma digital de mensajes y educar a los destinatarios para que solo confíe en los mensajes de la empresa que se han firmado puede ayudar a diferenciar los correos electrónicos legítimos de los que se han falsificado.

2. **Certificados de autenticación:** Los piratas informáticos nunca desaparecerán, pero una cosa que podemos hacer es que sea prácticamente imposible penetrar en los sistemas (por ejemplo, redes Wi-Fi , sistemas de correo electrónico, redes internas) mediante la implementación de autenticación basada en certificados para todas las máquinas y dispositivos de los empleados. Esto significa que solo los puntos finales con certificados configurados correctamente pueden acceder a sus sistemas y redes. Los certificados son fáciles de usar (no se necesita hardware adicional para administrar o se necesita mucha capacitación del usuario) y las implementaciones se pueden automatizar para simplificar las cosas y hacer que los hackers tengan más difícil un ataque.

5. Ataque Ingeniería Social

La ingeniería social es el arte de manipular a las personas para que renuncien a la información confidencial. Los tipos de información que buscan estos delincuentes pueden variar, pero cuando los individuos son blanco, los delincuentes generalmente intentan engañarlo para que le dé su contraseña o información bancaria, o acceda a su pc para instalar en secreto el software malicioso, que le dará acceso a sus contraseñas e información bancaria, así como para darles control sobre el mismo.



Los delincuentes usan tácticas de ingeniería social porque generalmente es más fácil explotar la inclinación natural a confiar que descubrir formas de hacker tu 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).

La seguridad se trata de saber en quién y en qué confiar; saber cuándo hacerlo y cuándo no; cuándo confiar en que la persona con la que nos estamos comunicando es de hecho la persona con la que piensas que te estás comunicando; cuándo confiar en que un sitio web es o no es legítimo; cuándo confiar en que la persona que está hablando por teléfono es o no es legítima; cuando proporcionar nuestra información es o no es una buena idea.

¿Cómo Prevenir ataques de ingeniería social?

- **Ve más despacio.** Los spammers quieren que actúes primero y pienses más tarde. Si el mensaje transmite una sensación de urgencia o usa tácticas de venta de alta presión, debemos ser escépticos. Nunca debemos dejar que la urgencia influya en nuestra revisión cuidadosa.
- **Investiga los hechos.** Sospecha de cualquier mensaje no solicitado. Si el correo electrónico parece ser de una empresa que nosotros utilizamos, debemos hacer nuestra propia investigación. Usar un motor de búsqueda para ir al sitio de la compañía real, o una guía telefónica para encontrar su número de teléfono.
- **Eliminar cualquier solicitud de información financiera o contraseñas.** Si nos piden que respondamos a un mensaje con información personal, es una estafa.
- **Rechace las solicitudes de ayuda u ofertas de ayuda.** Las empresas y organizaciones legítimas no se ponen en contacto con para brindarnos ayuda. Si no solicitó específicamente la ayuda del remitente, considere cualquier oferta para 'ayudar', una estafa. Del mismo modo, si recibimos una solicitud de ayuda de una organización benéfica u organización con la que no tenemos una relación, elimínala. Para dar, busque organizaciones caritativas de buena reputación por su cuenta para evitar caer en una estafa.
- **No permitir que un enlace controle dónde acaba.** Mantén el control buscando el sitio web tú mismo usando un motor de búsqueda para asegurarnos de que terminamos donde planeamos terminar. Al pasar el ratón sobre los enlaces en el correo electrónico, se mostrará la URL real en la parte inferior, pero una buena copia falsa, puede guiarnos incorrectamente.

- **El secuestro de correo electrónico es desenfrenado.** Los piratas informáticos, los generadores de correo no deseado y los generadores de redes sociales que toman el control de las cuentas de correo electrónico de las personas (y otras cuentas de comunicación) han crecido descontroladamente. Una vez que controlan la cuenta de correo electrónico de alguien, se aprovechan de la confianza de todos los contactos de la persona. Incluso cuando el remitente parece ser alguien que usted conoce, si no espera un correo electrónico con un enlace o archivo adjunto, verifica con tu amigo antes de abrir enlaces o descargar.
- **Cuidado con cualquier descarga.** Si no conocemos al remitente personalmente pero esperamos un archivo de ellos, descargar cualquier cosa, puede ser un error.
- **Las ofertas extranjeras son falsas.** Si recibimos correos electrónicos de loterías o sorteos extranjeros, dinero de un pariente desconocido o solicitudes para transferir fondos desde un país extranjero por una parte del dinero, es una estafa.
- **Establecer los filtros de spam a niveles altos.** Cada programa de correo electrónico tiene filtros de spam. Para encontrar el suyo, busque en las opciones de configuración y establezca estos valores altos, solo recuerde revisar su carpeta de spam periódicamente para ver si el correo electrónico legítimo ha llegado accidentalmente allí. También podemos buscar una guía paso a paso para configurar los filtros de spam buscando en el nombre de su proveedor de correo electrónico.
- **Asegurar los dispositivos informáticos.** Instalar software antivirus, cortafuegos, filtros de correo electrónico y mantenerlos actualizados. Configurar los sistemas operativos para que se actualicen automáticamente. Utilizar una herramienta anti-phishing ofrecida en el navegador web, normalmente en modo de plugin, es también una gran idea.

6. OS Finger Printing

OS Fingerprinting es el proceso de recopilación de información que permite identificar el sistema operativo en el ordenador que se tiene por objetivo.

Tipos de ataques OS Finger Printing:

1. OS Finger Printing activa: El **OS Fingerprinting activo** se basa en el hecho de que cada sistema operativo responde de forma diferente a una gran variedad de paquetes malformados. De esta manera, utilizando herramientas que permitan comparar las respuestas con una base de datos con referencias conocidas, es posible identificar cuál es el sistema operativo. Nmap es una herramienta ampliamente utilizada para llevar a cabo OS Fingerprinting activo.

2. OS Finger Printing pasivo: A diferencia del activo, el **OS Fingerprinting pasivo** no se realiza directamente sobre el sistema operativo objetivo. Este método consiste en el análisis de los paquetes que envía el propio sistema objetivo a través de técnicas de sniffing. De esta forma, es posible comparar esos paquetes con una base de datos donde se tenga referencias de los distintos paquetes de los diferentes sistemas operativos y, por lo tanto, es posible identificarlos.

Tanto el OS Fingerprinting activo como el pasivo poseen diferentes cosas a favor y en contra. En el caso del activo, es mucho más directo y confiable, ya que la interacción se realiza directamente sobre el sistema operativo objetivo. Sin embargo este tipo de interacción origina tráfico de red sobre el objetivo, por lo que es posible que se generen sospechas. Caso contrario, el OS Fingerprinting pasivo es más silencioso en el sentido que no genera tráfico de red, sino que solo intercepta aquellos paquetes en la red del sistema objetivo. Sin embargo, este método puede ser más complejo a la hora de obtener un conjunto de paquetes que permitan realizar la distinción del sistema operativo con certeza.

A modo de ejemplo, se puede utilizar Nmap para realizar un OS Fingerprinting activo utilizando la opción “-O” que permite habilitar la detección del sistema operativo. En la siguiente imagen puede visualizarse la detección:

```

root@bt:~# nmap -O 192.168.2.130

Starting Nmap 6.01 ( http://nmap.org ) at 2012-10-18 11:36 ART
Nmap scan report for 192.168.2.130
Host is up (0.00025s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:2F:65:1C (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

```

Detección de sistema operativo por OS Fingerprinting activo

En el caso de OS Fingerprinting pasivo, se utilizó la herramienta P0f, la cual permite identificar el sistema operativo de los equipos de la red donde se está realizando el sniffing. Analizando el tráfico generado por el sistema objetivo y a partir de comparaciones, es posible determinar, en el mejor de los casos, la versión exacta del sistema operativo o la familia a la que pertenece. En la siguiente captura puede visualizarse que tipo de sistema operativo detectó a partir del propio tráfico generado por el sistema objetivo:

```

.-[ 192.168.2.130/1219 -> 173.194.42.20/80 (http request) ]-
|
| client    = 192.168.2.130/1219
| app       = Firefox 5.x-9.x
| lang      = Spanish
| params    = none
| raw_sig   = 1:Host,User-Agent,Accept=[image/png,image/*;q=0.8,*/*;q=0.5],Accept-Charset=[ISO-8859-1,utf-8;q=0.7,*;q=0.7],Connection=[keep-alive]
|
|-----

```

Tráfico de red HTTP (Detección User Agent)

```

.-[ 192.168.2.130/1219 -> 173.194.42.20/80 (syn) ]-
|
| client    = 192.168.2.130/1219
| os        = Windows NT kernel
| dist      = 0
| params    = generic
| raw_sig   = 4:128+0:0:1460:mss*44,0:mss,nop,nop,sok:df,id+:0
|
|-----

```

Detección de sistema operativo por OS Fingerprinting pasivo

Para poder lograr este tipo de información, se debe envenenar la red para lograr interceptar todo el tráfico y así poder analizar los paquetes enviados desde el sistema objetivo.

Desde el punto de vista de una pentester (persona que realiza el Penetration Test), el método de OS Fingerprinting pasivo es una buena técnica para obtener información relevante sin atentar contra el sigilo en el análisis. La mayor ventaja que tiene este método es que es posible utilizarlo a pesar de que los sistemas objetivos cuenten con Firewalls, sistemas IDS/IPS u otros sistemas de protección de red. Asimismo, el OS Fingerprinting pasivo no dejará rastros en los logs del sistema objetivo. Sin embargo en la mayoría de los casos el OS Fingerprinting activo será más preciso a la hora de identificar el sistema operativo debido a que es un método más invasivo y directo.

7. Conocer los puertos expuestos

Un escaneo de puertos se define como una aplicación o pieza de software específica del proceso que sirve como punto final de comunicaciones. Este punto final es utilizado por los protocolos de la capa de transporte del conjunto de protocolos de Internet, concretamente, TCP y UDP se utilizan universalmente para comunicarse en Internet. Cada puerto también se identifica con un entero sin signo de 16 bits llamado número de puerto. "En la terminología TCP / IP, un puerto es un identificador de software que corresponde a una aplicación o protocolo específico que se ejecuta en un host". Por ejemplo, Http usa el puerto 80. Los números de puerto están separados en tres rangos: Puertos conocidos, Puertos registrados y Puertos dinámicos y / o privados. En el mundo de la intrusión informática, el escaneo de puertos es una de las técnicas de reconocimiento más utilizadas para descubrir servicios "pirateables".

En la terminología cotidiana, es análogo a un ladrón caminando por un grupo de automóviles y probando las puertas de los automóviles para ver qué puertas del automóvil están abiertas. Sin embargo, un hecho importante a tener en cuenta es que el escaneo de puertos es utilizado por los administradores del sistema para diagnosticar problemas en nuestras redes. En resumen, todo escaneo de puertos es una serie de intentos de un intruso o administrador para ver qué puertos de una red están abiertos al intentar conectarse a un rango de puertos en un rango de hosts, para luego recopilar información de los puertos abiertos que responden a ver qué aplicaciones o servicios están asociados o ejecutándose en esos puertos. El escaneo de puertos se lleva a cabo mediante la implementación de software para escanear cualquiera de los 0 a 65536 puertos potencialmente disponibles en un equipo.

¿Cómo prevenir el escaneo de puertos?

Si tenemos un servidor de acceso público, el sistema será vulnerable a los escaneos de puertos. No hay una forma segura de vencer los escaneos de puertos. Los sistemas judiciales han determinado que realizar exploraciones de puertos no es ilegal. Los escaneos de puertos son ilegales solo si el atacante usa información de un escaneo de puertos para explotar una vulnerabilidad o abrir un puerto en el sistema. Entonces, la pregunta es: ¿cómo limitamos la información que nuestros sistemas proporcionarán?

Una forma de limitar la información obtenida de escaneos de puertos es cerrar los servicios innecesarios en los sistemas de destino, es decir, si está ejecutando un servidor web, http debe ser el único servicio ofrecido. En los sistemas UNIX, la forma más fácil de limitar la información proporcionada a los escáneres de puertos es editar el `/etc/inetd.conf` y comentar cualquier servicio innecesario.

También editar el `/etc/init.d` y el archivo de nivel de ejecución que el sistema está devolviendo. Eliminar los servicios innecesarios. Además, asegurarnos de que el sistema no se esté ejecutando en el modo X11. Si se está ejecutando en el modo X11, el sistema transmitirá el servicio 6000 ya sea que haya iniciado sesión o no.

Otra forma de limitar la información proporcionada a los escáneres de puertos es emplear encapsuladores TCP, cuando corresponda. Los Contenedores TCP dan al administrador la flexibilidad de permitir o denegar el acceso a los servicios en base a las direcciones IP o nombres de dominio. Las capsulas de TCP funcionan junto con el archivo `/etc/inetd.conf`. TCP Wrappers funciona invocando el `tcpd` daemon antes de proporcionar el servicio especificado. Cuando se detecta una solicitud entrante procedente de un puerto autorizado, los contenedores TCP verifican primero el archivo `/etc/hosts.allow` para ver si la dirección IP o el nombre de dominio tiene permisos para acceder al servicio. Si no se encuentra ninguna entrada, TCP Wrappers verificará el archivo `/etc/hosts.deny`. Si no se encuentra ninguna entrada allí, o si se encuentra la instrucción ALL: ALL, los Contenedores TCP ignorarán la solicitud y no permitirán que se utilice el servicio solicitado. Cuando se escanea el sistema, los contenedores TCP aún permitirán que se anuncie el servicio; sin embargo, el escáner no recibirá ninguna información adicional del puerto a menos que el escaneo provenga de un host o dominio especificado en `/etc/hosts.allow`. Cuando se escanea, el sistema mostrará el servicio como abierto. Cuando el atacante intenta explotar el puerto abierto, TCP Wrappers rechazará la conexión entrante si no proviene de un host o dominio aprobado. El inconveniente de TCP Wrappers es que no todos los servicios están cubiertos. Los servicios como http y smtp no están cubiertos, y si no están configurados

correctamente, serán susceptibles de explotación. TCP Wrappers no es susceptible a la suplantación de IP. Cuando se detecta una solicitud entrante, TCP Wrappers realizará una búsqueda DNS inversa en la dirección IP solicitante. Si la búsqueda inversa coincide con la IP solicitante, los contenedores TCP permitirán la conexión. Si la búsqueda inversa falla, TCP Wrappers supondrá que se trata de un host no autorizado y no permitirá la conexión.

Finalmente, otra forma de limitar la cantidad de información dada a los escaneos de puertos es utilizar productos como **PortSentry** ofrecido por Psionic. PortSentry detecta las solicitudes de conexión en una serie de puertos seleccionados. PortSentry es personalizable y se puede configurar para ignorar una cierta cantidad de intentos. El administrador puede seleccionar qué puertos escuchará PortSentry para las solicitudes de conexión y la cantidad de solicitudes no válidas. El administrador enumerará los puertos que su sistema no admite. Tras la detección, PortSentry empleará los contenedores TCP y realizará una entrada en el archivo `/etc/hosts.deny` para el sospechoso de intrusión. PortSentry también configurará una declaración de ruta predeterminada para el sistema infractor. La instrucción de ruta predeterminada encaminará todos los paquetes desde el sistema infractor a otro sistema o a un sistema inactivo. El resultado es que el sistema objetivo aparecerá como inexistente. En los sistemas Linux, PortSentry puede detectar todos los escaneos TCP y UDP, mientras que en los sistemas Solaris solo pueden detectar los escaneos TCP Vanilla y UDP.

8. KeyLoggers

Un keylogger puede ser un programa de software o un hardware que utiliza un atacante para registrar las pulsaciones de teclas en el teclado de un usuario. Con un Keylogger, un atacante puede conocer remotamente sus contraseñas, números de tarjetas de crédito / débito, mensajes, correos electrónicos y todo lo que escriba.

Los registradores de pulsaciones basados en software generalmente infectan el sistema en forma de un malware que un usuario podría haber descargado haciendo clic en un enlace malicioso, ya sea en línea o enviándolo por correo electrónico.

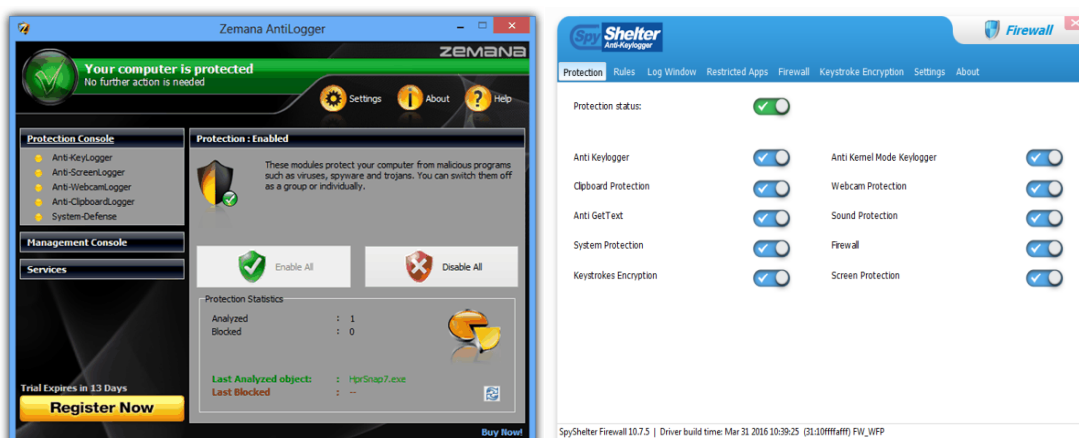
Un software de captura de teclas se ejecuta en segundo plano sin notificar al usuario y tomará nota de cada golpe de teclado y luego lo alimentará a un servidor en línea al que puede acceder el atacante.

Revisar todo el historial de registros de teclas puede brindarle a cualquiera una idea de los sitios web que visitó y la información que ingresó en ellos, lo que le da una forma fácil de acceder a la tarjeta de crédito o credenciales de banca por Internet. Los ataques de teclado son utilizados por los atacantes con intención maliciosa de monitorear las pulsaciones de teclas, siendo importante protegerse contra ellos, para que no seamos vulnerable a perder información de identificación personal, incluidas las credenciales personales o corporativas.

¿Cómo prevenir los keylogger?

Si bien hay varias herramientas disponibles para encontrar y hacer frente a los keyloggers de software, no existe un software de seguridad para identificar un keylogger hardware.

Dado que los registradores de teclas son básicamente malware, basta con un programa antivirus que proteja el PC en tiempo real, pero si deseamos protección adicional, también se pueden usar programas tales como Zemana AntiLogger y SpyShelter Stop-Logger.



La versión gratuita de Zemana solo proporciona cifrado para sus pulsaciones de teclas, lo que significa que, aunque el atacante podrá registrar sus pulsaciones de teclas, se le presentarán en un formato codificado e ilegible. La versión gratuita de SpyShelter no solo proporciona cifrado, sino que también protege el PC contra capturas de pantalla o portapapeles.

Si no deseamos utilizar un registrador de teclas, siempre se recomienda utilizar el teclado en línea disponible en los sitios web bancarios, por ejemplo, que no deja rastros de registro de teclas. Si sospechamos que las pulsaciones de teclas están siendo registradas, y

ninguno de estos softwares puede identificarlo o protegerlo de él, entonces probablemente alguien ingresó un keylogger hardware en el PC. Estos registradores de teclas hardware generalmente vienen en forma de conectores USB. Uno de los extremos está conectado al teclado y otro al USB de la PC, y aunque todo funciona sin problemas, el hardware intercepta y transmite las pulsaciones de las teclas al atacante, es revisar nuestro PC de vez en cuando.

9. ICMP Tunneling

El tunneling se usa a menudo para eludir los firewalls que no bloquean los paquetes ICMP, o para establecer un canal de comunicación cifrado y difícil de rastrear entre dos equipos sin interacción directa de la red. Un túnel ICMP establece una conexión encubierta entre dos equipos remotos (un cliente y un proxy), utilizando solicitudes de eco ICMP y paquetes de respuesta. Un ejemplo de esta técnica es tunelizar el tráfico TCP completo a través de peticiones y respuestas de ping.

¿Cómo prevenir túneles ICMP?

Resulta difícil detener la creación de túneles ICMP ya que el cortafuegos personal los infunde como mensajes de control emitidos por el sistema operativo. La encriptación y autenticación fuertes, además de la creación de túneles ICMP, empeora la situación. Por lo tanto, la solución para evitar el túnel ICMP debería:

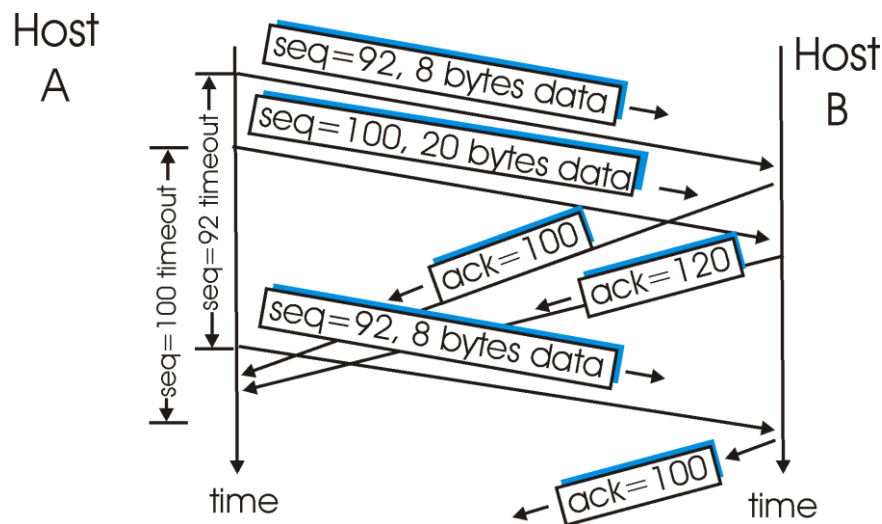
- Permitir a los administradores usar mensajes ICMP libremente.
- Permitir el paso del gran tamaño de ICMP.
- Debería funcionar incluso en el caso de una fuerte autenticación y carga útil encriptada.
- Debería funcionar incluso cuando la máquina está detrás de cortafuegos personales a nivel de aplicación.

En comparación con el modelo costoso de preservación del estado utilizado por los cortafuegos industriales, se propone un modelo simple de menos estado para evitar el efecto túnel. El modelo sin estado satisface los requisitos mencionados anteriormente. El modelo sin estado requiere un acuerdo común sobre la carga permisible de los mensajes ICMP. La política debería implementarse en la implementación del protocolo ICMP del kernel. Se debe hacer cumplir ya sea cuando un paquete ICMP sube la pila de la red o cuando baja la misma.

10. Ataque de secuencia TCP

Un ataque de predicción de secuencia TCP es un intento de predecir el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión.

En un escenario típico de ataque de predicción de secuencia TCP, un atacante pasaría algún tiempo monitorizando el flujo de datos entre dos hosts, uno de los cuales es el sistema de destino. El atacante cortaría el otro sistema (que es confiable para el objetivo) de la comunicación, tal vez a través de un ataque de denegación de servicio (DoS), dejándolos a sí mismos para tomar el lugar de ese sistema confiable, a los ojos de su objetivo.



Habiendo predicho el número de secuencia del siguiente paquete que el objetivo espera de su host de confianza, el atacante prepara un paquete con la dirección IP de origen del sistema de confianza y el número de secuencia esperado. Es seguro que este paquete llegará a su destino antes que cualquier información legítima del host confiable (que tiene un ataque DoS para mantenerlo ocupado y fuera de la imagen). El paquete del atacante se puede usar como una vía para obtener acceso al sistema de destino, terminar a la fuerza una comunicación o entregar una carga maliciosa.

¿Cómo prevenir el ataque de secuencia TCP?

En respuesta a sus propias observaciones, el Equipo de trabajo de ingeniería de Internet (IETF) emitió un estándar renovado (RFC 6528) en 2012, estableciendo un algoritmo mejorado para generar números de secuencia iniciales para las comunicaciones TCP. Está diseñado para aumentar la

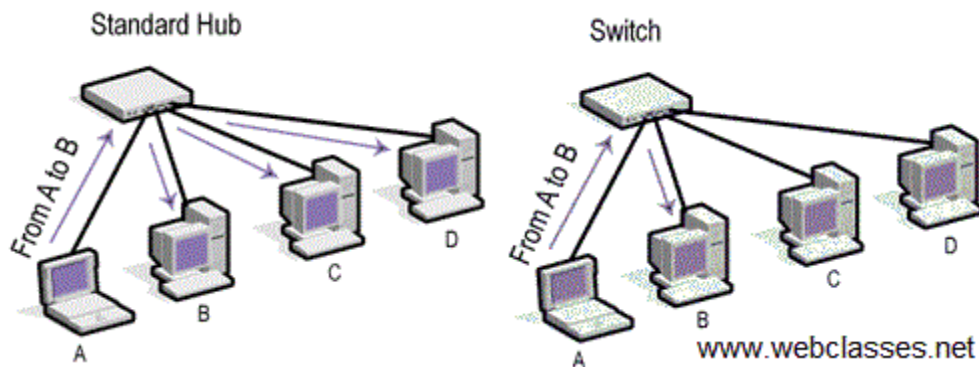
robustez de la generación del número de secuencia frente al tipo de análisis predictivo y monitoreo que permitieron a los caber atacantes un acceso tan fácil al número de secuencia bajo el antiguo régimen.

A nivel empresarial, los fabricantes de sistemas operativos respondieron a la amenaza mediante la introducción de métodos nuevos y más impredecibles de generación de números de secuencia, una medida que se logró con un éxito parcial.

Una estrategia más efectiva ha sido que las organizaciones y los administradores de red bloqueen paquetes enrutados de origen y paquetes de datos con direcciones dentro de sus propias redes. Los servicios que dependen de la autenticación basada en IP deberían, idealmente, desconectar una conexión por completo al detectar que están presentes las opciones enrutadas de origen.

11. CAM Table Overflow

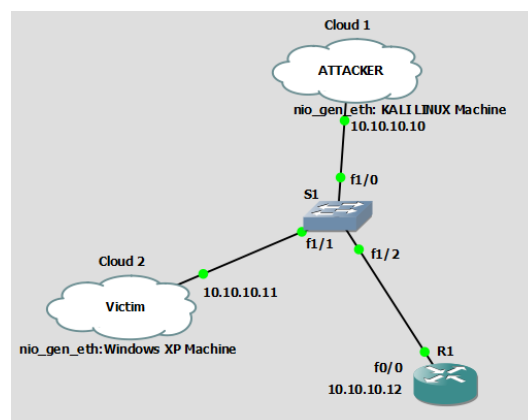
Antes de comenzar, hay un concepto básico en el campo de red que es "Switch VS Hub". La principal diferencia es cómo se transmiten los paquetes de un dispositivo "Fuente" (A) a otro "Destino" (B).



Los concentradores siempre realizan la inundación de marcos al enviar un paquete recibido desde la fuente (A) a todos los dispositivos conectados. Normalmente, todos los dispositivos eliminarán el paquete recibido, excepto el destino (B). Los conmutadores, por otro lado, tienen una tabla llamada Memoria direccionable de contenido o Content Addressable Memory (CAM) que se refiere a una tabla dinámica que asigna las direcciones MAC de los dispositivos conectados a los puertos del conmutador. Cuando el paquete se envía de A a B, el conmutador buscará en su tabla CAM el puerto que corresponde a la dirección MAC de B y solo enviará el paquete a B, que es más seguro que la técnica de inundación del concentrador.

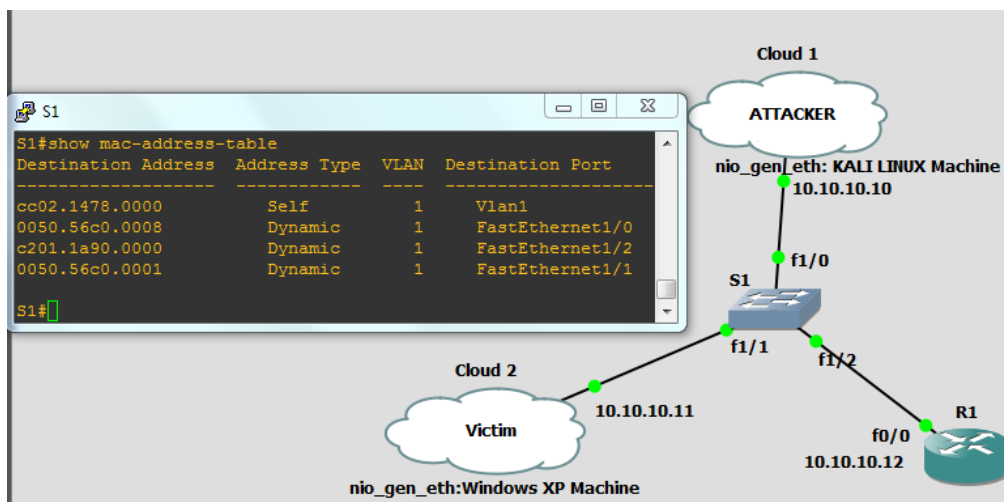
Ahora la pregunta es ¿qué pasa si esta tabla CAM está llena?

Estableceremos un entorno virtual utilizando GNS (virtualización de la red), Virtual Box o una máquina virtual con dos sistemas operativos (Kali Linux y Windows XP):



Aquí tenemos un administrador de red que ejecuta Windows XP (víctima) que intenta administrar su propio enrutador (R1) y una máquina Kali Linux (atacante) conectada en el mismo conmutador (S1).

Si emitimos el comando “**show mac-address-table**” en nuestro conmutador, veremos la tabla CAM del conmutador, que muestra el puerto y las direcciones MAC de los dispositivos que están conectados a él.



Después de pulsar enter, se generará una gran cantidad de direcciones MAC aleatorias falsas como se ve a continuación.

```

root@kali: ~/Desktop
File Edit View Search Terminal Help
9594067(0) win 512
b8:98:eb:7c:bf:ee 42:83:e8:26:ff:13 0.0.0.0.55687 > 0.0.0.0.25808: S 761779879:7
61779879(0) win 512
c2:16:80:20:da:fb 74:8f:5c:4c:d9:8a 0.0.0.0.29810 > 0.0.0.0.30351: S 519706600:5
19706600(0) win 512
7a:f7:60:55:d3:28 94:11:54:76:15:80 0.0.0.0.42368 > 0.0.0.0.64499: S 946440424:9
46440424(0) win 512
37:23:d7:b:f5:56 43:5d:45:51:38:d9 0.0.0.0.50210 > 0.0.0.0.17533: S 826711423:82
6711423(0) win 512
f7:8b:34:5c:8:6 6c:22:a0:21:fc:43 0.0.0.0.38112 > 0.0.0.0.34131: S 981290977:981
  
```

El conmutador también almacenará dinámicamente estas direcciones MAC en su tabla CAM. Ahora volveremos a emitir nuestros dos primeros comandos en nuestro conmutador para ver los cambios realizados en la tabla CAM.

```
S1#show mac-address-table count
NM Slot: 1
-----

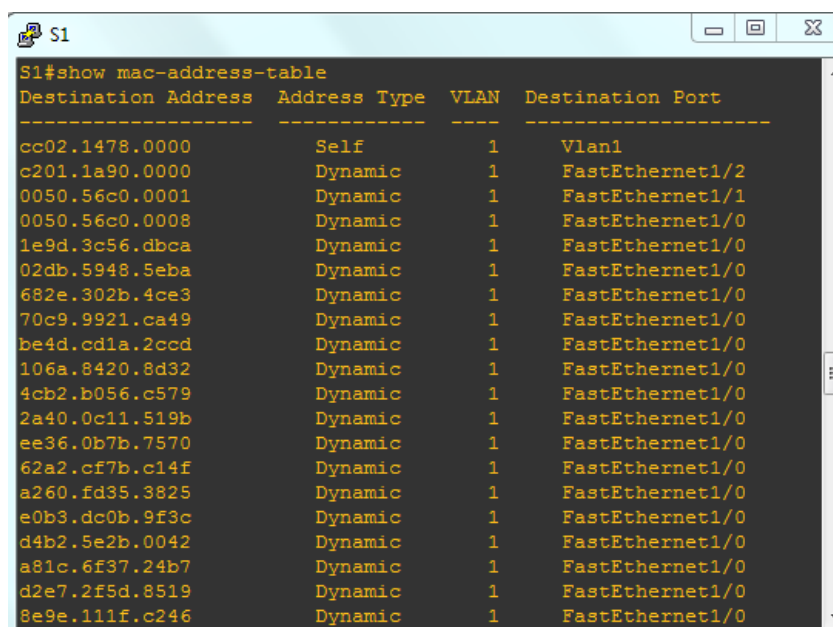
Dynamic Address Count:                6841
Secure Address (User-defined) Count:  0
Static Address (User-defined) Count:  0
System Self Address Count:            1
Total MAC addresses:                   6842
Maximum MAC addresses:                 8192

S1#show mac-address-table count
NM Slot: 1
-----

Dynamic Address Count:                7326
Secure Address (User-defined) Count:  0
Static Address (User-defined) Count:  0
System Self Address Count:            1
Total MAC addresses:                   7327
Maximum MAC addresses:                 8192
```

Aquí, el número total de direcciones MAC almacenadas aumenta cada vez que emitimos el mismo comando porque la máquina del atacante continúa generando una gran cantidad de direcciones MAC falsas.

Las nuevas entradas de la tabla CAM serán las siguientes, observamos aquí la gran cantidad de direcciones MAC asignadas al mismo puerto (interfaz FastEthernet)

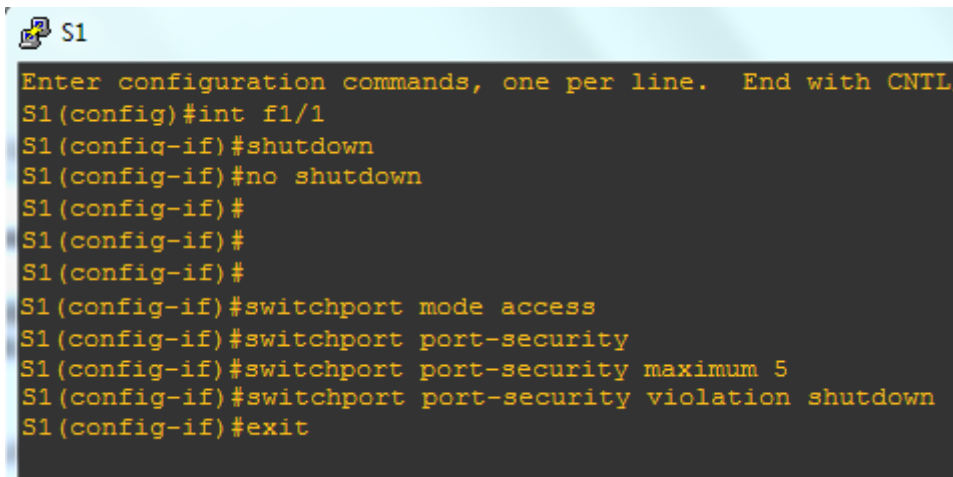


Destination Address	Address Type	VLAN	Destination Port
cc02.1478.0000	Self	1	Vlan1
c201.1a90.0000	Dynamic	1	FastEthernet1/2
0050.56c0.0001	Dynamic	1	FastEthernet1/1
0050.56c0.0008	Dynamic	1	FastEthernet1/0
1e9d.3c56.dbca	Dynamic	1	FastEthernet1/0
02db.5948.5eba	Dynamic	1	FastEthernet1/0
682e.302b.4ce3	Dynamic	1	FastEthernet1/0
70c9.9921.ca49	Dynamic	1	FastEthernet1/0
be4d.cd1a.2ccd	Dynamic	1	FastEthernet1/0
106a.8420.8d32	Dynamic	1	FastEthernet1/0
4cb2.b056.c579	Dynamic	1	FastEthernet1/0
2a40.0c11.519b	Dynamic	1	FastEthernet1/0
ee36.0b7b.7570	Dynamic	1	FastEthernet1/0
62a2.cf7b.c14f	Dynamic	1	FastEthernet1/0
a260.fd35.3825	Dynamic	1	FastEthernet1/0
e0b3.dc0b.9f3c	Dynamic	1	FastEthernet1/0
d4b2.5e2b.0042	Dynamic	1	FastEthernet1/0
a81c.6f37.24b7	Dynamic	1	FastEthernet1/0
d2e7.2f5d.8519	Dynamic	1	FastEthernet1/0
8e9e.111f.c246	Dynamic	1	FastEthernet1/0

Después de un par de minutos el conmutador está reenviando paquetes como Hub.

Ahora el conmutador está inundando cualquier paquete recibido desde cualquier puerto a todos los demás puertos, incluido el (Atacante), recibirá una copia de cada paquete enviado por el administrador (Vitim) o cualquier otra máquina al enrutador (R1) o cualquier otro dispositivo conectado a este interruptor. Al usar software como Ettercap, el atacante puede cambiar su NIC del modo de operación normal al modo promiscuo, lo que hace que el controlador pase todo el tráfico que recibe a la CPU en lugar de pasar solo las tramas que el controlador debe recibir, este modo normalmente es se utiliza para la detección de paquetes y también se conoce como el hombre en el ataque central.

Para recuperarse de este ataque, primero debemos cerrar este puerto desde el conmutador utilizando los dos comandos de apagado y no apagado en la interfaz atacada



```
S1
Enter configuration commands, one per line. End with CNTL/Z
S1(config)#int f1/1
S1(config-if)#shutdown
S1(config-if)#no shutdown
S1(config-if)#
S1(config-if)#
S1(config-if)#
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 5
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#exit
```

¿Cómo prevenir los ataques CAM Overflow?

Para evitar este tipo de ataque, cambiaremos el puerto a un puerto de acceso mediante la emisión del modo de puerto de conmutación y para aplicar la seguridad de puerto en nuestro puerto, tecleamos la seguridad de puerto de puerto de conmutación. A continuación, asignaremos el número máximo de direcciones MAC para almacenar la tabla CAM para esta interfaz que usa switchport port-security máximo 5. Finalmente elegiremos nuestra acción de violación que se aplicará cuando el usuario (atacante) intente generar más de X direcciones MAC asociadas al mismo puerto. Elegimos cerrar este puerto, ahora si el atacante intenta realizar este ataque nuevamente en dicho switch su puerto se apagará automáticamente, también se generará un registro en este que informa al administrador que el (atacante) MAC la dirección en este puerto estaba tratando de atacarnos y el estado del puerto ahora está abajo/cerrado.

12. Ataques a Aplicaciones Web

Las Aplicaciones Web, al igual que los equipos físicos u otro tipo de software, también presentan vulnerabilidades que pueden ser explotadas. A continuación se explican algunas de las más conocidas, ejemplos de cómo funcionan y al igual que con el resto de ataques, soluciones para protegernos ante estas amenazas:

- **Inyección SQL:** La inyección SQL se trata de infiltración de código intruso en una aplicación a la hora de realizar operaciones en una base de datos. Esta vulnerabilidad tiene origen en la incorrecta comprobación o filtrado de variables utilizadas en un programa que genera código SQL (como es el caso de las aplicaciones web que en la mayoría de los casos tienen una base de datos SQL para almacenar la información). Este error no es tanto un problema de configuración de un servidor web, sino que se trata más bien de un error de programación al desarrollar la aplicación.

Según la OWASP (Open Web Application Security Project) la inyección SQL se encuentra en el top 10 de vulnerabilidades explotadas actualmente, en concreto la inyección (de cualquier tipo) se encuentra en el top 1 de vulnerabilidades.

La vulnerabilidad se puede producir automáticamente cuando un programa "arma descuidadamente" una sentencia SQL en tiempo de ejecución, en cualquier caso, siempre que el programador necesite y haga uso de parámetros a ingresar por parte del usuario, a efectos de consultar una base de datos; ya que, justamente, dentro de los parámetros es donde se puede incorporar el código SQL intruso.

Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el ordenador.

Para solucionar de una forma simple este problema se han creado diferentes funciones que sirven para escapar los caracteres utilizados principalmente en las bases de datos para crear consultas y no son necesarias para introducir datos por parte del usuario. Por ejemplo, en PHP se usa la función `mysqli_real_escape_string()`.

Ejemplo de inyección SQL

Para esta demo vamos a utilizar la aplicación web DVWA (Damn Vulnerable Web Application) que se trata de un entorno diseñado específicamente para ser vulnerable y para que los profesionales de la seguridad dispongan de un lugar donde practicar el pentesting en un entorno legal y para que los desarrolladores web entiendan mejor los procesos de securización de las aplicaciones web.

En este caso haremos un par de ejemplos de inyección SQL y veremos lo que se puede conseguir a través de él.

En primer lugar examinamos el código para ver que tipo de vulnerabilidades podemos explotar.

Low SQL Injection Source

```
<?php
if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];

    // Check database
    $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysqli_query($GLOBALS["__mysqli_ston"], $query ) or die( '

```
' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : (($___mysqli_res =

 // Get results
 while($row = mysqli_fetch_assoc($result)) {
 // Get values
 $first = $row["first_name"];
 $last = $row["last_name"];

 // Feedback for end user
 echo "<pre>ID: {$id}
First name: {$first}
Surname: {$last}</pre>";
 }

 mysqli_close($GLOBALS["__mysqli_ston"]);
}
?>
```


```

Para esta consulta SQL podemos ver como no se realiza ningún escape de caracteres y se inserta el contenido de la variable directamente en la consulta por lo que podemos inyectar cualquier código SQL que queramos y obtener datos que deberían ser privados.

CONSULTA 1

En este primer ejemplo vamos a obtener los nombres de usuario de todas las personas registradas en el sistema, para ello introduciremos el siguiente código:

```
' or ' 1=1
```

Vulnerability: SQL Injection

User ID:

ID: ' or ' 1=1
First name: admin
Surname: admin

ID: ' or ' 1=1
First name: Gordon
Surname: Brown

ID: ' or ' 1=1
First name: Hack
Surname: Me

ID: ' or ' 1=1
First name: Pablo
Surname: Picasso

ID: ' or ' 1=1
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/SDP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-okul/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)

Damn Vulnerable Web Application (DVWA) v1.10 *Development*

Como la condición `1=1` siempre se cumple vamos a obtener todos los datos almacenados en esa tabla en concreto.

CONSULTA 2

En este caso vamos a obtener el nombre de la base de datos:

```
' or 1=1 union select null, database() #
```

The screenshot shows the DVWA interface with the 'SQL Injection' vulnerability selected. The 'User ID' field contains the payload: `' or 1=1 union select null, database() #`. The results show the following output:

```
ID: ' or 1=1 union select null,database() #
First name: admin
Surname: admin

ID: ' or 1=1 union select null,database() #
First name: Gordon
Surname: Brown

ID: ' or 1=1 union select null,database() #
First name: Hack
Surname: Me

ID: ' or 1=1 union select null,database() #
First name: Pablo
Surname: Picasso

ID: ' or 1=1 union select null,database() #
First name: Bob
Surname: Smith

ID: ' or 1=1 union select null,database() #
First name:
Surname: dvwa
```

The 'More Information' section lists several links for further reading on SQL Injection:

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_injection
- <http://bobby-tables.com/>

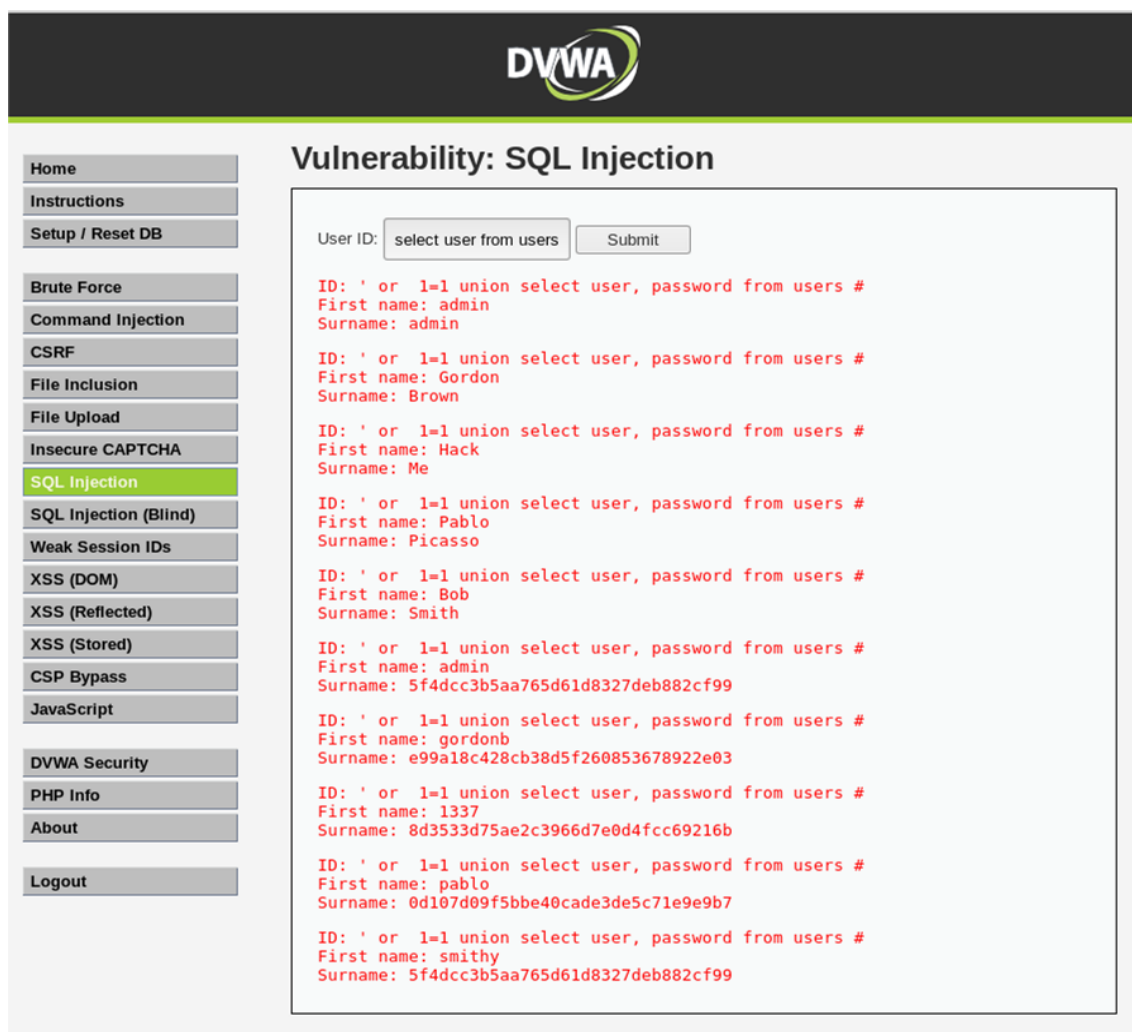
The footer of the application shows: 'Damn Vulnerable Web Application (DVWA) v1.10 *Development*'.

Como podemos observar, obtenemos los mismos datos que anteriormente, pero en la última línea se nos muestra el nombre de la base de datos del sistema.

CONSULTA 3

En este último ejemplo, tras realizar unos pasos previos que no veremos hemos obtenido el nombre de las tablas de la base de datos (gracias en parte al nombre que hemos obtenido anteriormente) y los campos de las mismas. Ahora vamos a proceder a obtener el usuario y su contraseña asociada con el siguiente código:

```
' or ' 1=1 union select user, password from users #
```



DVWA

Vulnerability: SQL Injection

User ID:

```
ID: ' or ' 1=1 union select user, password from users #
First name: admin
Surname: admin

ID: ' or ' 1=1 union select user, password from users #
First name: Gordon
Surname: Brown

ID: ' or ' 1=1 union select user, password from users #
First name: Hack
Surname: Me

ID: ' or ' 1=1 union select user, password from users #
First name: Pablo
Surname: Picasso

ID: ' or ' 1=1 union select user, password from users #
First name: Bob
Surname: Smith

ID: ' or ' 1=1 union select user, password from users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' or ' 1=1 union select user, password from users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' or ' 1=1 union select user, password from users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' or ' 1=1 union select user, password from users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' or ' 1=1 union select user, password from users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Como podemos observar obtenemos la contraseña, pero está hasheada. Sin embargo no tiene mayor inconveniente que pasarlas por una de las cientos de herramientas para descryptar que existen, asociándole su nombre de usuario que también hemos conseguido.

SOLUCIÓN

SQL Injection

Impossible SQL Injection Source

```
<?php
if( isset( $_GET[ 'Submit' ] ) ) {
    // Check Anti-CSRF token
    checkToken( $_REQUEST[ 'user_token' ], $_SESSION[ 'session_token' ], 'index.php' );

    // Get input
    $id = $_GET[ 'id' ];

    // Was a number entered?
    if( is_numeric( $id ) ) {
        // Check the database
        $data = $db->prepare( 'SELECT first_name, last_name FROM users WHERE user_id = (:id) LIMIT 1;' );
        $data->bindParam( ':id', $id, PDO::PARAM_INT );
        $data->execute();
        $row = $data->fetch();

        // Make sure only 1 result is returned
        if( $data->rowCount() == 1 ) {
            // Get values
            $first = $row[ 'first_name' ];
            $last = $row[ 'last_name' ];

            // Feedback for end user
            echo "<pre>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</pre>";
        }
    }
}

// Generate Anti-CSRF token
generateSessionToken();
?>
```

Para solucionar estos problemas de seguridad la propia aplicación nos muestra el código resultante de una correcta programación, utilizando en este caso PHP y PDO para realizar la consulta, evitando de esta forma cualquier tipo de inyección SQL posible.

Sigamos hablando del resto de ataques a aplicaciones web:

- **Cross-Site Request:** La falsificación de solicitudes entre sitios, también conocida como ataque con un solo clic o sesión y abreviado como CSRF ("sea-surf") o XSRF, es un tipo de exploit malicioso de un sitio web mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. A diferencia de los scripts de sitios cruzados (XSS), que explota la confianza que un usuario tiene para de un sitio en particular, CSRF explota la confianza que un sitio tiene en el navegador de un usuario.
- **Ataque de envenenamiento de cookies:** Los ataques de envenenamiento de cookies implican la modificación de los contenidos de una cookie (información personal almacenada en el equipo de un usuario web) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de cookies, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad.

- **Robo de cookies:** Este tipo de ataques se realizan mediante scripts del lado del cliente como JavaScript. Cuando el usuario hace clic en un enlace, el script buscará la cookie almacenada en la memoria del ordenador para todas las cookies activas y las enviará (al parecer, los correos electrónicos) al atacante.
- **Ataques de phishing:** Phishing es el proceso criminalmente fraudulento de intentar adquirir información sensible como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una entidad confiable en una comunicación electrónica.
- **Web Defacement:** La desfiguración del sitio web es un ataque a un sitio web que cambia la apariencia visual del sitio. Estos son típicamente el trabajo de los crackers del sistema, que entran en un servidor web y reemplazan el sitio web alojado con uno propio. Lo más probable es que este tipo de ataques se hagan intencionalmente para arruinar la reputación de la compañía que ha alojado este sitio web.
- **Buffer Overflow:** El desbordamiento de búfer es una anomalía en la que un proceso almacena datos en un búfer fuera de la memoria que el programador reservó para ello. Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. Esta vulnerabilidad es completamente un error del Programador.
- **Navegación forzada:** La exploración forzada es un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace referencia, pero que aún son accesibles. Por ejemplo, directorios como config, backup, logs a los que se puede acceder pueden revelar mucha información sobre la aplicación en sí, contraseña, actividades, etc.
- **División de respuesta HTTP:** Un atacante pasa datos maliciosos a una aplicación vulnerable, y la aplicación incluye los datos en un encabezado de respuesta HTTP. Este ataque en sí no causa ningún daño, pero daría lugar a otros ataques sensibles como XSS.
- **Defectos de inyección:** Las fallas de inyección permiten a los atacantes retransmitir código malicioso a través de una aplicación web a otro sistema. Estos ataques incluyen llamadas al sistema operativo a través de llamadas al sistema, el uso de programas externos a través de comandos del shell, así como llamadas a bases de datos de backend a través de SQL (es decir, inyección de SQL).

Los scripts completos escritos en Perl, Python y otros lenguajes pueden ser inyectados en aplicaciones web mal diseñadas y ejecutado. Cada vez que una aplicación web utiliza un intérprete de cualquier tipo, existe el peligro de un ataque de inyección. Cada vez que una aplicación web utiliza un intérprete de cualquier tipo, existe el peligro de un ataque de inyección.

¿Cómo prevenir los ataques a aplicaciones web?

Existen diferentes métodos y herramientas que los desarrolladores modernos de aplicaciones web usan para proteger un sitio web. Existen soluciones para ataques específicos y mejores prácticas que se pueden utilizar de forma continua para proteger las aplicaciones y los usuarios. Las revisiones de código, los programas de recompensa de errores y los escáneres de código deberían implementarse durante todo el ciclo de vida de la aplicación. Las revisiones de códigos pueden ayudar a detectar códigos vulnerables al principio de la fase de desarrollo, los escáneres de códigos dinámicos y estáticos pueden hacer comprobaciones automáticas de vulnerabilidades, y los programas de bonificación de errores permiten a los tester/hacker profesionales encontrar errores en el sitio web.

Las soluciones específicas de ataque incluyen:

- Usar procedimientos almacenados con parámetros que se parametrizan automáticamente.
- Implementando CAPTCHA o incitando a los usuarios a responder preguntas. Esto asegura que un formulario y una solicitud sean enviados por un humano y no por un bot.
- Y lo más importante, utilizar un **cortafuegos de aplicación web (WAF)** para supervisar la red y bloquear posibles ataques.

Ninguno de estos métodos puede reemplazar al otro, cada uno aporta su propio valor a la tabla y agrega protección contra ciertos escenarios de ataque. No puede encontrar todas las vulnerabilidades mediante revisiones de código o programas de bonificación de errores, ni solo mediante un cortafuegos de aplicación web ya que ninguna herramienta está 100% segura. Se debe usar una combinación de todos estos métodos para proteger las aplicación y a sus usuarios.

13. Virus y Worms

Un **virus informático** es un programa informático que puede copiarse e infectar un ordenador. El término "virus" también se usa comúnmente pero erróneamente para referirse a otros tipos de malware, incluidos, entre otros, los programas de adware y spyware que no tienen la capacidad reproductiva. Un virus verdadero puede propagarse de un equipo a otro (en algún tipo de código ejecutable) cuando su host se lleva a l equipo de destino; por ejemplo, porque un usuario lo envió a través de una red o Internet, o lo llevó en un medio extraíble, como una unidad USB.

Por otro lado un **Worm o Gusano** informático es un programa informático de malware autoreplicante. Utiliza una red informática para enviar copias de sí mismo a otros nodos (ordenadores en la red) y puede hacerlo sin intervención del usuario. Esto se debe a deficiencias de seguridad en el equipo de destino. A diferencia de un virus, no es necesario que se una a un programa existente. Los gusanos casi siempre causan al menos algún daño a la red, al consumir ancho de banda, mientras que los virus casi siempre corrompen o modifican archivos en un equipo específico.

14. Malware, Adware y Spyware

1. Malware: es una forma corta de software malicioso. El malware no es lo mismo que el software defectuoso, es decir, el software que tiene un propósito legítimo pero contiene errores dañinos. El malware incluye virus informáticos, gusanos, caballos de Troya, spyware, adware deshonesto, software delictivo, la mayoría de los rootkits y otro software malicioso y no deseado.

¿Cómo prevenir el Malware?

- a) **Instalar software Anti-Virus / Anti-Malware:** Este consejo puede ser evidente. Sin embargo, he visto muchos PCs, especialmente PCs personales, que no tienen protección antivirus / malware. Esta protección es un primer paso imprescindible para mantenernos libres de virus.
- b) **Mantener el software antivirus actualizado:** Tener software de protección es el primer paso; mantenerlo es el segundo. El software antivirus gratuito es mejor que nada, pero tenga en cuenta que no es la mejor solución. Microsoft proporciona un paquete de seguridad "gratis". Es gratis si tiene Windows en su máquina, se le concede acceso. Muchos usuarios no conocen este programa, pero en realidad es una protección decente.

- c) **Ejecuta escaneos regulares programados del antivirus:** Esto también puede parecer obvio, pero muchos de nosotros nos olvidamos de hacer esto. Configurar el software de elección para que se ejecute a intervalos regulares. Es preferible una vez por semana, pero no debemos esperar mucho más entre escaneos. Es difícil trabajar en el equipo mientras se está ejecutando el software antivirus. Una solución es ejecutar el software por la noche cuando no se está usando el PC. Sin embargo, a menudo apagamos nuestros ordenadores por la noche, por lo que el escaneo nunca se ejecuta. Configurar el software antivirus para que se ejecute en una noche específica, y siempre dejar el PC encendido ese día. Asegurarnos de que no se apague automáticamente o entre en modo de hibernación.
- d) **Mantener el sistema operativo al día:** Ya sea que esté ejecutando Windows, Mac OS X, Linux o cualquier otro sistema operativo, mantenerlo actualizado. Los desarrolladores de SO siempre emiten parches de seguridad que arreglan y completan las filtraciones de seguridad. Estos parches ayudarán a mantener un sistema seguro. Del mismo modo, mantener un software antivirus actualizado. Los virus y el malware se crean de forma continua. Si nuestro software de escaneo es tan bueno como nuestra base de datos. También debe ser lo más actualizado posible.
- e) **Asegurar la red:** Muchos de nuestros equipos se conectan a nuestros archivos, impresoras o Internet a través de una conexión Wi-Fi. Debemos asegurarnos de que se requiere una contraseña para acceder y que la contraseña es fuerte. Nunca debemos transmitir por una conexión Wi-Fi abierta. Usaremos cifrado WPA o WPA2. Ya que el WEP no es lo suficientemente fuerte ya que los expertos lo pueden romper en minutos. También es una buena idea no difundir su SSID (el nombre de su red Wi-Fi) e importante también, proporcionar un SSID de invitados que use una contraseña diferente.
- f) **Piensa antes de hacer clic:** Evitar los sitios web que proporcionan material pirateado. No abrir un archivo adjunto de correo electrónico de alguien o una empresa que no conocemos. No hacer clic en un enlace en un correo electrónico no solicitado. Siempre colocar el cursor sobre un enlace (especialmente uno con un acortador de URL) antes de hacer clic para ver hacia dónde nos lleva realmente el enlace. Si tenemos que descargar un archivo de Internet, un correo electrónico, un sitio FTP, un servicio de intercambio de archivos, etc., buscarlo antes de ejecutarlo. Un buen software antivirus lo hará de forma automática, pero debemos asegurarnos de que se está haciendo.
- g) **Mantener la información personal segura:** Esto es probablemente lo más difícil de hacer en Internet. Muchos hackers accederán a nuestros archivos no mediante la fuerza bruta, sino a través de la ingeniería

social. Recibirán suficiente información para acceder a nuestras cuentas en línea y obtendrán más de nuestros datos personales. Continuarán de una cuenta a otra hasta que tengan suficiente información que les permita acceder a nuestros datos bancarios o simplemente robar nuestra identidad. Debemos tener cuidado con los tableros de mensajes y las redes sociales. Bloquear todas nuestras configuraciones de privacidad y evitar usar nuestro nombre real o identidad en los foros de debate.

- h) **No usar Wi-Fi abierto:** Cuando nos encontremos en la cafetería local, la biblioteca y especialmente el aeropuerto, no debemos usar el Wi-Fi abierto (sin contraseña ni cifrado) "gratuito". Pensémoslo. Si puede acceder sin problemas, ¿qué puede hacer un individuo malicioso entrenado?
- i) **Haz una copia de seguridad de los archivos:** Lo mejor que puede hacer es hacer una copia de seguridad de los archivos, todos ellos. Idealmente, tendremos nuestros archivos (sus datos) en al menos tres lugares: en el lugar donde trabaja en ellos, en un dispositivo de almacenamiento por separado y otro fuera del sitio de trabajo. Debemos mantener nuestros archivos en el PC, hacer una copia de seguridad de ellos en un disco duro externo y luego hacer una copia de respaldo en una ubicación diferente.
- j) **Usa múltiples contraseñas fuertes:** Nunca use la misma contraseña. Por lo general, utilizamos la misma dirección de correo electrónico o nombre de usuario para todas nuestras cuentas. Si se usa la misma contraseña para todo, o en muchas cosas, y la misma se "rompe", solo demorará unos segundos a un hacker para entrar en la cuenta. Usa minúsculas, mayúsculas, números y símbolos en la contraseña. Haz una contraseña fácil de recordar pero difícil de adivinar.

2. Adware (o software respaldado por publicidad): es cualquier paquete de software que reproduce, muestra o descarga publicidades en un equipo automáticamente después de instalar el software o mientras se usa la aplicación. Las funciones de publicidad se integran o se incluyen con el software, que a menudo está diseñado para indicar qué sitios de Internet visita el usuario y para presentar la publicidad pertinente a los tipos de productos o servicios que allí aparecen.

3. Spyware: es un tipo de malware que se instala en los equipos y recopila pequeñas porciones de información a la vez sobre los usuarios sin su conocimiento. La presencia de spyware generalmente está oculta para el usuario y puede ser difícil de detectar. Normalmente, el spyware se instala secretamente en el PC personal del usuario. A veces, sin embargo, los spyware como key loggers son instalados por el propietario de un PC

compartido, corporativa o pública a propósito para monitorizar en secreto a otros usuarios.

15. Troyanos

Un caballo de Troya o troyano es un tipo de malware que a menudo se camufla como software legítimo. Los ciberdelincuentes y los hackers pueden emplear los troyanos para intentar acceder a los sistemas de los usuarios. Normalmente, algún tipo de ingeniería social engaña a los usuarios para que carguen y ejecuten los troyanos en sus sistemas. Una vez activados, los troyanos pueden permitir a los cibercriminales espiarte, robar tus datos confidenciales y obtener acceso por una puerta trasera a tu sistema. Estas acciones pueden incluir las siguientes:

- Eliminación de datos
- Bloqueo de datos
- Modificación de datos
- Copia de datos
- Interrupción del rendimiento de ordenadores o redes de ordenadores

A diferencia de los virus y los gusanos informáticos, los troyanos no pueden multiplicarse.

¿Cómo pueden afectar a un equipo los troyanos?

Los troyanos se clasifican en función del tipo de acciones que pueden realizar en el ordenador:

- **Puerta trasera (Backdoor):** Un troyano backdoor (de puerta trasera) proporciona el control remoto del ordenador infectado a los ciberdelincuentes. Estos troyanos permiten al ciberdelincuente hacer todo lo que desee en el ordenador infectado, como enviar, recibir, iniciar y eliminar archivos, mostrar datos y reiniciar el ordenador. Los troyanos backdoor (de puerta trasera) a menudo se utilizan para unir un conjunto de ordenadores infectados para formar un botnet o una red zombi que se puede utilizar con objetivos delictivos.
- **Exploit:** Los exploits son programas que contienen datos o código que se aprovechan de una vulnerabilidad del software de aplicaciones que

se ejecuta en el ordenador.

- **Rootkit:** Los rootkits están diseñados para ocultar ciertos objetos o actividades en el sistema. A menudo, su objetivo principal es evitar la detección de programas maliciosos con el fin de ampliar el periodo en el que los programas pueden ejecutarse en un ordenador infectado.
- **Trojan-Banker (Troyano Bancario):** Los programas Trojan-Banker, o troyanos bancarios, están diseñados para robar tus datos bancarios de sistemas de banca online, sistemas de pago electrónico y tarjetas de débito o crédito.
- **Trojan-DDoS:** Estos programas realizan ataques DoS (denegación de servicio) contra una dirección web específica. Mediante el envío de una gran cantidad de solicitudes (desde tu ordenador y otros ordenadores infectados), el ataque puede saturar la dirección de destino y originar una denegación de servicio.
- **Trojan-Downloader:** Los programas de descarga de troyanos, Trojan-Downloader, pueden descargar e instalar nuevas versiones de programas maliciosos en el ordenador, incluidos troyanos y adware.
- **Trojan-Dropper:** Los hackers utilizan estos programas para instalar troyanos y virus, o bien para evitar la detección de programas maliciosos. No todos los programas antivirus pueden analizar todos los componentes incluidos en este tipo de troyano.
- **Trojan-FakeAV:** simulan la actividad de software antivirus. Están diseñados para extorsionar al usuario a cambio de la detección y eliminación de amenazas, aunque estas no existan realmente.
- **Trojan-GameThief:** Este tipo de programas roba los datos de la cuenta de usuario de los jugadores online.
- **Trojan-IM:** Los programas Trojan-IM roban los datos de inicio de sesión y las contraseñas de los programas de mensajería instantánea, como ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype, etc.
- **Trojan-Ransom:** Este tipo de troyano puede modificar los datos del ordenador para que no funcione correctamente o no puedas utilizar datos específicos. El cibecriminal solo restaurará el rendimiento del ordenador o desbloqueará los datos una vez que hayas pagado el dinero

"de rescate" que solicita.

- **Trojan-SMS:** Estos programas pueden costarte dinero en forma de envío de mensajes desde el dispositivo móvil a números de teléfono con tarificación especial.
- **Trojan-Spy:** Los programas Trojan-Spy pueden espiar cómo utilizas el ordenador. Por ejemplo, mediante el seguimiento de los datos que introduces a través del teclado, la realización de capturas de pantalla o la obtención de una lista de aplicaciones en ejecución.
- **Trojan-Mailfinder:** Estos programas pueden recopilar las direcciones de correo electrónico del ordenador.

¿Cómo saber si un troyano está acampando en tu ordenador?

Los troyanos, aunque pretendan pasar inadvertidos, pueden dejar varias señales de su estancia en nuestro ordenador .

Si nuestro equipo presenta alguno de estos síntomas, puede que tenemos un troyano alojado en el:

- Pantalla o ventanas emergentes con mensajes poco usuales. No hay duda: bien existe software espía instalado en el PC, bien ha sido infectado por un falso antivirus.
- Comportamientos sospechosos del navegador: el navegador de internet accede por sí solo a determinados sitios que no solicitamos, se abren y cierran ventanas solas. Es un signo inequívoco de infección. Muchas de las amenazas están diseñadas para redirigir tráfico a determinados sitios que el usuario no ha elegido.
- Problemas con las conexiones. No puedes conectarte a internet o la conexión es mucho más lenta que la habitual; El malware podría estar estableciendo diferentes sesiones de conexión, lo que sin duda nos robará ancho de banda y hará que naveguemos muy despacio o que incluso se convierta en una tarea casi imposible.
- Lentitud en el Sistema Operativo, bloqueos continuos o se reinicia el sistema sin que se conozcan las causas, programas que inesperadamente comienzan su ejecución o la concluyen.
- El antivirus desaparece. Otra de las características de muchas amenazas informáticas es la deshabilitación del sistema de seguridad que hayas instalado.

¿Cómo proteger un equipo frente a un troyano?

Entre otras soluciones, las más efectivas son:

- Instalar un antivirus original (puede ser gratuito) y tenerlo siempre actualizado.
- Actualizar las aplicaciones y el sistema operativo.
- Desconfiar siempre de correos electrónicos con remitentes desconocidos.
- No sigas enlaces ni ejecutes adjuntos si no estás 100% seguro de su origen.
- Descargar siempre las aplicaciones de los 'markets' oficiales, no solo las de banca móvil, ya que en amenazas como esta el troyano no se esconde en una aplicación que simula ser del banco, sino en una utilidad de software genérica, como por ejemplo aquella que permite ver vídeos en formato Flash.

Bibliografía

1. <https://latam.kaspersky.com/blog>
2. <https://www.welivesecurity.com>
3. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
4. https://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
5. https://www.youtube.com/watch?v=KmbMtiOfTnQ&list=PLqDeWqLgG5nWE69_NgONpzWfJO7rmB0fo&index=9
6. <https://www.bbva.com>
7. www.stackoverflow.com/questions/3410505/sniff-http-packets-for-get-and-post-requests-from-an-application
8. <https://www.wireshark.org/lists/wireshark-users/200902/msg00129.html>