Servidores Web de Altas Prestaciones

Prevención de Ataques

Número de trabajo: 12
Horas dedicadas: 37

Autores
Miguel Ángel Pérez Díaz
Sergio Aguilera Ramírez
Christian Vigil Zamora

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

Índice

1. INTRODUCCIÓN

En la actualidad, resulta complicado hacerse la idea de que una persona no tenga conexión a internet. Está más que claro que internet ha supuesto una gran cantidad de innovaciones para la sociedad, pero no todo el mundo lo usa con una finalidad positiva.

A su vez, cada vez más empresas se suman al proceso de digitalización, a fin de llegar a un público más amplio, extender sus ventas mediante el comercio online, etc. La digitalización para una empresa supone alojar sus datos en internet, debiendo ser lo suficientemente protegidos para evitar que puedan ser robados.

Tal y como comentábamos, internet puede ser usado para una finalidad negativa y ahí es donde tiene cabida el tema de nuestro trabajo, la prevención de ataques. A día de hoy, los ciberdelincuentes están en su momento más álgido, realizando ataques tanto de tipo personal: robo de datos confindenciales, robo de dinero, suplantación de identidad... como ataques a empresas con la finalidad de tirar abajo su funcionamiento y robar datos sensibles entre otros.

Todos estos tipos de ataques tienen un nombre y en medida de lo posible, existen ciertas técnicas y patrones a seguir para prevenir sufrir dichos ataques, sea el ámbito que sea. Aunque este mundo nunca tiene fin, mientras se investiga para descubrir técnicas de prevención de ataques actuales, los ciberdelicuentes trabajan en nuevas formas de atacar y así sucesivamente.

2. ANTECEDENTES O PRELIMINARES

En esta primera sección comenzaremos detallando algunos conceptos premilinares con el objetivo de mejorar la comprensión de las proximas secciones, así como comentar los diferentes servicios/productos/sistemas que hemos encontrado parecidos al tema que nos conscierne.

Como hemos comentado en la introducción, los ataques informáticos ocurren con una frecuencia altísima día a día, siendo originados desde cualquier parte del mundo gracias a la conexión de internet. Ya conocemos la frecuencia con la que ocurren ataques, pero ¿a qué nos referimos cuando hablamos de ataques informáticos?. Bien, aunque no existe una definición universal, numerosos organismos de prestigio han proporcionado la suya:

- **Instituto Español de Estudios Estratégicos**
  "*Actos que los delincuentes informáticos llevan a cabo como parte de sus actividades delictivas virtuales*"
- **Auditool**
  "*Un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red*"

- **Real Academia de Ingeniería**
  "*Forma de ciberguerra o ciberterrorismo donde, combinado con ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a la misma*"

Ya sabemos en que consiste un ataque informático y tal como nos podemos imaginar, llevan existiendo desde los inicios de internet. En el apartado próximo, comentaremos cuáles son los ataques que se dan con más frecuencia en la actualidad, así como técnicas de prevención ante ellos, pero claro, dichas técnicas de prevención como es de esperar tienen antecedentes dado que los ataques llevan existiendo mucho tiempo.

La herramienta usada por excelencia para prevenir los ataques es el **antivirus**. El hecho de ser la más usada se debe a que no requiere conocimientos avanzados de informática, por lo tanto la mayoría de usuarios se bastan de herramientas de éste estilo y nada más. Un antivirus es un programa dedicado a detectar virus, bloquearlos y eliminarlos. A día de hoy son capaces también de detectar malware, spyware...

Por supuesto, los ciberdelicuentes se adaptan a las nuevas medidas de prevención e inventan nuevos ataques, por lo que a día de hoy el antivirus puede considerarse un antecedente, ya que ha dado lugar a técnicas de prevención más complejas, las cuáles requieren un nivel de usuario más avanzado en la informática.

3. DESARROLLO Y/O ANÁLISIS

3.1. Contexto

Una vez introducidos anteriormente algunos de estos conceptos más generales, en esta sección profundizaremos más en los diferentes ataques informáticos que pueden se producir hoy día en cualquier dispositivo electrónico. Trataremos de ofrecer una clasificación en base a estos ataques, a la misma vez que ofrecemos diferentes técnicas de prevención para cada uno de ellos.
Para llevar a cabo la tarea de prevención debemos seguir una serie de pasos tales como:

1. **Identificar aquello que debemos proteger.** Inicialmente es necesario tratar de identificar los diferentes elementos que pueden verse afectados en caso de un ataque como pueden ser:
   - *Usuarios y contraseñas*
   - *Información sensible de la empresa o usuario*
   - *Datos de tarjetas de crédito*
   - *Credenciales*
2. **Identificar aquellos sucesos que pueden ocurrir.** Una vez identificados los elementos que debemos proteger es necesario tratar de identificar las consecuencias

que pueden llegar a ocurrir sobre estos elementos cuando un intruso entra en el sistema y se propone a lanzar un ataque. En este paso asociaremos los diferentes tipos de ataques que vamos a estudiar con sus respectivas consecuencias:

- **Ataque Man in the Middle :** Consiste en una persona que es capaz de situarse en el medio de dos comunicaciones y robar la información que se envía. Puede ser tanto online como offline.

  Otro ejemplo de ataque Man in the Middle es el que se lleva a cabo en los navegadores. Lo que hacen los atacantes es insertar código malicioso en el sistema de la víctima y actúa como intermediario. El objetivo aquí es ir recopilando todos los datos que se introducen en el navegador, las páginas visitadas, etc.

- **Ataque DoS :** Los ataques de denegación de servicio son ataques cuyo objetivo es inhabilitar el uso de un sistema informático. La base principal del funcionamiento de estos ataques consiste en enviar gran cantidad de peticiones de diferentes tipos a un mismo punto para que el servidor o la red a la que se envía no soporte la cantidad de paquetes recibidos y como consecuencia se produzca una interrupción del servicio proporcionado.

- **Keyloggers :** Se trata de un programa software o hardware utilizado por los usuarios atacantes, permitiéndoles conocer las teclas que son pulsadas por el usuario afectado. Los ataques más utilizados hoy en día son los basados en software, ya que presentan una mayor facilidad de utilización respecto a los de tipo hardware, que para su utilización es necesario el acceso físico al dispositivo. De ambos modos, el atacante puede conocer de forma remota las contraseñas, correos electrónicos, número de cuenta y multitud de información privada de un usuario.

  Principalmente, estos malware se transfieren a través de correos electrónicos, páginas web inseguras, descargar indeseadas o simplemente forman parte de una apliación. Los ataques keyloggers se ejecutan en segundo plano, por lo que el usuario afectado no se percata de lo que sucede.

3. **Identificar las vulnerabilidades.** Este paso tiene como propósito identificar todas las vulnerabilidades técnicas o escenarios que permitan la ejecución de las amenazas identificadas en los pasos anteriores.Tenemos que tener en consideración que hay que identificar y registrar todas las vulnerabilidades potenciales independientemente de que estén o no incluidas en el caso de uso de la institución que estamos analizando

Entre las principales vulnerabilidades que normalmente solemos encontrar:

- *Total acceso a la web y uso de correos electrónicos.*
- *Controles de antivirus y firewall del sistema deficientes.*
- *Deficiente configuración de seguridad.*
- *Deficiente monitorización de seguridad.*
- *Débil segmentación de la red.*
- *Políticas de contraseñas frágiles.*
- *Información no cifrada.*

4. **Evaluar el grado de vulnerabilidad.** Esta tarea implicará la identificación de controles de seguridad (por ejemplo, el cifrado de bases de datos que contienen información sensible) y su evaluación de eficiencia. Este proceso permitirá tener una idea del grado de vulnerabilidad actual de la institución y la facilidad con que las múltiples amenazas se podrían materializar.

Una vez identificado todo aquello que debemos proteger, las principales vulnerabilidades del sistema y los ataques que pueden producirse debemos tratar que aplicar ciertas medidas para prevenir estos ataques.

En esta nueva subsección trataremos de comentar las principales medidas de prevención sobre los diferentes ataques que anteriormente hemos comentado.

3.2. Ataques Man in the middle

En este apartado vamos a exponer diversas medidas/técnicas de prevención de ataques Man in the Middle. Por lo general, los ataques Man in the Middle son aquellos en los que el atacante utiliza un intermediario para realizar el ataque al usuario final. Las medidas básicas para contrarrestar este tipo de ataques son la utilización de sitios web que tengan implementadas conexiones cifradas a través de SSL/TSL, aunque con esto no estaríamos protegidos ante las vulnerabilidades en el lado del cliente, la utilización de la verificación en dos pasos para los distintos sitios web, como por ejemplo las cuentas de Google o las de Facebook, en último lugar, podemos hacer uso de redes VPN, donde realizamos una conexión virtual punto a punto a través de un túnel que intensifica la dificultad del ciberdelincuente para entrar en esta conexión. Algunas otras prevenciones son:

- No usar redes públicas para operación de gran importancia (implementar redes privadas VPN)
- Inicios de sesión seguros, a través de HTTPS, TLS, etc.
- Redes wifi divididas
- Instalar sistemas de detección de intrusos, IDS, con el objetivo de monitorar nuestra red y informar de procesos que modifiquen en significacia el flujo del tráfico.

Una de las herramientas más utilizadas para aumentar la seguridad contra este tipo de ataques es Etherwall basada en el envenenamiento de caché ARP. A su vez, esta herramienta sirve para prevenir otros tipos de ataques como sniffing, hijacking, DNS spoofing, etc. Las principales características de esta herramienta son la ejecución en modo demonio del sistema, el filtrado de paquetes ARP, la protección punto a punto y punto a multipunto, la protección se realiza en tiempo real, tiene integrado un sistema de registro de log y un sistema de alerta temprana, dar soporte de redes estáticas y dinámicas, así como soporte para ethernet inalámbrico y por cable de interfaz.
Esta herramienta consta de tres algoritmos básicos:

1. **Filtrado de paquetes ARP:** solo permite la entrada de paquetes procedentes del router. Para aceptar paquetes de otros hosts el usuario puede hacer una lista de hosts, que se ubicará en la ruta /etc/etherwall/allow.conf", desde los que se permitirá la entrada de paquetes.
2. **Protección punto a punto:** este algoritmo mantiene la comunicación entre dos hosts y proporciona una dirección válida de manera que siempre se mantendrá la estabilidad de la conexión.
3. **Protección punto a multipunto:** este algoritmo es similar al de protección punto a punto, pero permitiendo la conexión entre dos o mas hosts.

3.3. Ataques DoS

En esta subseción trateremos de comentar algunas de las medidas de prevención más importantes para los ataques de denegación de servicio (DoS). Para este tipo de ataques implementar medidas preventivas será imprescindible ya que, en caso contrario, solamente sabremos que hemos sido víctimas de este ataque cuando el servicio deje de funcionar.

A continuación vamos a detallar algunas de estas medidas de prevención, pero enfocadas a distintos ámbitos:

3.3.1. Medidas de protección en la red interna

Cuando la página web se encuentra en la red interna de la empresa se han de incorporar elementos de protección perimetral para protegerlo. Entre otras medidas:

- Ubicar **el servidor web en una zona desmilitarizada** (entre cortafuegos), también llamada DMZ, evitando así que un intruso pueda acceder a la red interna si vulnera el servidor web.
- Implementar **un sistema de detección y prevención de intrusiones (IDS/IPS)** que monitorizan las conexiones y nos alerta si detecta intentos de acceso no autorizados o mal uso de protocolos.
- Utilizar un dispositivo o software con funcionalidad mixta (antivirus, cortafuegos y otras), como un UTM que permite gestionar de manera unificada la mayoría de ciberamenazas que pueden afectar a una empresa.

El uso combinado de estos elementos, que pueden ser tanto software como hardware, y su correcta configuración, reducirá las posibilidades de sufrir un ataque de denegación de servicio.

3.3.2. Medidas de protección en el hosting

En caso de que se haya contratado un hosting debes informarte sobre las medidas de seguridad que ha implementado el proveedor. Tendrás que comprobar que son como las del apartado anterior. Algunos proveedores ofrecen estas medidas de seguridad en el panel de administración del alojamiento web. Verifica con el proveedor quién será el encargado de su configuración y administración.

3.3.3. Ancho de banda

Esta puede que sea la forma de protección más básica, pero no por ello la menos eficaz. Independientemente de que el servicio web se encuentre dentro de la organización o subcontratado se ha de contar con el mayor ancho de banda posible. De esta forma, se podrán gestionar mejor los picos de tráfico que causan las denegaciones de servicio.

3.3.4. Redundancia y balance de carga

La redundancia consiste en tener el activo duplicado en más de un servidor y el balanceado de carga permite que se asigne a un servidor u otro en función de la carga de trabajo que esté soportando. Esta medida reduce los riesgos de sufrir uno de estos ataques, ya que al tener más de un servidor se reducirá la posibilidad de que se detenga debido a la sobrecarga. Además, aporta otras ventajas como la tolerancia a los fallos, ya que si un servidor cae, el total del trabajo lo asumiría el otro servidor.

3.3.5. Soluciones de seguridad basadas en la nube

Una de las soluciones que cualquier servicio web considerado crítico debe tener es un cortafuegos de aplicación o WAF por sus siglas en inglés Web Application Firewall. Los proveedores de seguridad web basados en la nube pueden ser de gran ayuda a la hora de evitar y mitigar los efectos de un ataque de denegación de servicio. Los WAF, que ofrecen las soluciones basadas en la nube, actúan como intermediarios entre nuestro servicio web y los usuarios, interponiéndose también a ciberdelincuentes o bots. Ante cualquier indicio de ataque, el WAF actuará y evitará que las conexiones maliciosas lleguen al sitio web, evitando así las denegaciones de servicio

3.3.6. Sistemas actualizados

Algunos de los ataques de denegación de servicio tienen su origen en sistemas desactualizados, pues estos son en esencia más vulnerables. Mantener el software (servidores, gestores de contenidos web, etc.) actualizado es esencial para evitar cualquier tipo de ataque. Los ataques DoS no son una excepción.
También, hay que reducir la superficie de ataque lo máximo posible, por lo que cualquier servicio que no sea estrictamente necesario para el correcto funcionamiento de la web debe ser desinstalado. Cuanto menor sea la superficie de ataque, menor será la posibilidad de sufrir uno

3.4. Keyloggers

En este apartado, nos centraremos en las distintas técnicas/herramientas para prevenir los ataques de tipo Keyloggers. Existen diferentes métodos de prevención para estos ataques, el método más utilizado comunmente por los usuarios es la instalación de un antivirus que ofrezca protección en tiempo real a nuestro ordenador, el gran inconveniente es que en la mayoria de casos estos antivirus comerciales no son lo bastantes eficaces para impedir dichos ataques. En relación a esta posible vulnerabilidad, aquellas entidades, confederaciones o personas con un alto interés de protección, utilizan otros métodos más especializados en este tipo de ataques, como pueden ser las herramientas Zemana Antilogger, Ghostpress y SpyShelter Stop-Logger. Los métodos anteriores se basan en el cifrado por pulsación de teclas y en la continua analización de actividades sospechosas en el sistema de nuestro ordenador, proporcionando una mayor seguridad sobre el robo de información de nuestra computadora.

3.4.1. Zemana Antilogger

Es un programa que permite reconocer, prevenir y bloquear el robo de identidad en línea y herramientas de estafa financiera. Zemana es una herramienta poderosa y fácil de usar, cuya funcionalidad es monitorizar el sistema en tiempo real para prevenir intentos de grabación y robo de los datos privados, asegurando así que los datos se transmitan de forma segura sin ser interceptados por el atancante. De forma general, el mecanismo que utiliza este programa es el cifrado de la pulsación de la tecla, proporcionando la información de descifrado en sitio destino, ya sea sitios web, bancos, etc. Este programa a diferencia de las demás herramientas de anti-logging, protege nuestra información no solo del navegador, sino de todas las aplicaciones que usamos en nuestra computadora.

Figura 1: Zemana Antilogger

3.4.2. Ghostpress

Ghostpress es una aplicación diseñada para evitar ataques basados en Keyloggers, se encuentra de forma gratuita para todos los usuarios. Esta aplicación fue creada por Henrick Schiffer. Ghostpress a diferencia de las demás teconologias de prevención de ataques, oculta las teclas y pulsaciones en su totalidad, es decir, no lleva a cabo ninguna técnica de intercambiado de teclas, rastreo de anomalias, etc. Esta herramienta al igual que Zemana es fácil de usar y posee una gran flexibilidad de configuración para enfocar la protección en únicamente en la ocultación de las pulsaciones. Una de las funcionalidades con la que cuenta este programa es la protección contra las falsificaciones que se basan en la imitación del estilo de escritura, donde el atacante pretende hacerse pasar por el usuario, aunque una de las formas más simples que lleva a cabo para evitar estas falsificaciones es establecer un límite de tiempo de escritura.

Figura 2: Ghostpress

3.4.3. SpyShelter Anti-Logger

SpyShelter al igual que las herramientas expuestas anteriormente, esta capacitado para detectar y detener cualquier tipo de malware, así como los más complejos a la hora de prevenir. Esta herramienta, protege todos los módulos que componene nuestro sistema operativo, con el objetivo de proteger la información privilegida. La funcionalidad de SpyShelter, de forma similar que Zemana Antilogger, supervisa en tiempo real nuestra computadora en busca de amenazas, cuando este detecta alguna posible amenaza, bloquea de forma inmediata dicha amenaza e informa al usuario de la misma. A su vez, cuenta con un mecanismo de encriptación de pulsaciones del teclado para otorgar un mayor nivel de protección al sistema. Además, esta herramienta tiene integrado un sistema de seguridad que permite proteger nuestro sistema durante conexiones HTTP, HTTPS, SMTP etc. Asimismo, detecta las solicitudes entrantes y salientes, para sí poder analizar con cautela cada una de estas solicitudes detectanto posibles anomalías, esto es conocido como protección de cortafuegos bidireccional.

Figura 3: SpyShelter Stop-Logger

4. EXPERIMENTACIÓN

En esta sección trataremos de aplicar los conocimientos anteriormente expuestos sobre las diferentes formas de prevenir ataques. Como ya hemos mencionado en secciones anteriores, existen muchísimos ataques diferentes donde cada uno tiene un comportamiento diferente dentro de nuestro sistema.

Para nuestro trabajo hemos decidido centrarnos en algunos de ellos, donde una vez expuesto en qué consisten y sus diferentes medidas de prevención, vamos a poner en práctica alguna de estas medidas para así comprobar su funcionamiento en el ámbito real.

4.1. Experimento 1: Ataque y prevención Keylogger

Empezaremos realizando una prueba con el ataque *Keylogger* en donde trataremos de prevenir dicho ataque mediante uno de los softwares anteriores: *SpyShelter*.

Para realizar esta prueba se ha instalado el software y se ha generado un ejecutable con Python en donde trataremos de simular este ataque. Este script recogerá y mostrará por pantalla cada tecla que pulsemos desde el teclado:

```python
from pynput.keyboard import Listener


def captura(key):
    tecla = str(key)
    tecla = tecla.replace("'","")
    print("Evento: ",tecla)

with Listener(on_press=captura) as c:
    c.join()
```

Figura 4: Script captura de teclado Python

Una vez tenemos el script preparado y SpyShelter instalado en nuestro sistema, vamos a tratar de probar el funcionamiento de este último a la hora de captar y prevenir pérdidas de información a través del ataque Keylogger.

En principio dejamos la protección desactivada y ejecutamos el script para captar las pulsaciones de las teclas:

Figura 5: Protección desactivada

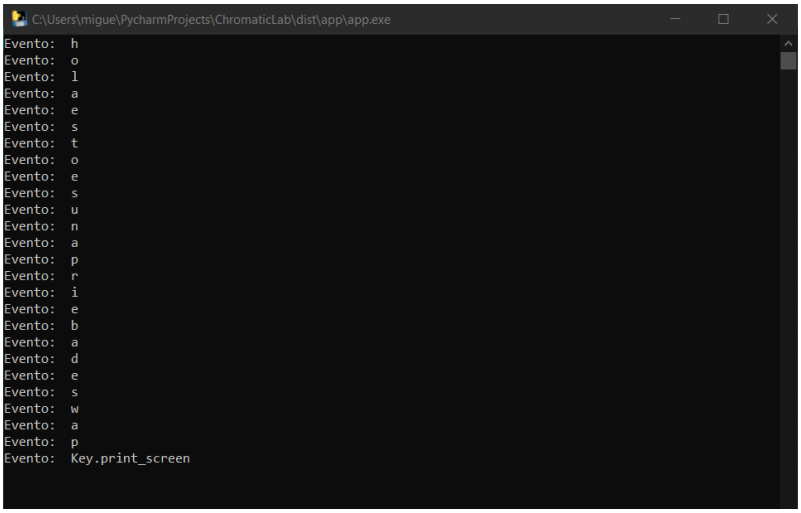

Figura 6: Captación de teclas

Como podemos apreciar al tener la protección desactivada se captan y se muestran por pantalla todas las teclas que hemos pulsado en ese momento. Tras esto vamos a tratar de activar la protección y observar qué ocurre en este caso.

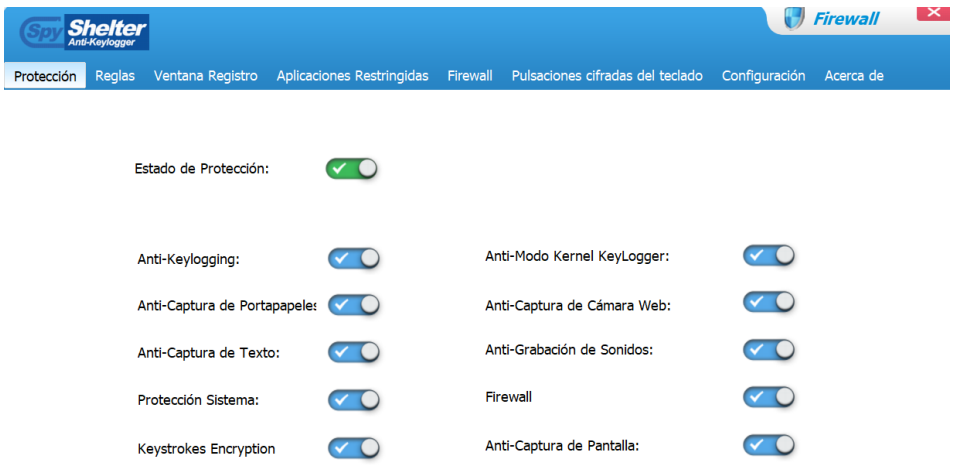

Figura 7: Protección activada

Como podemos ver en el menú superior de SpyShelter existe una opción de *Pulsaciones cifradas de teclado*, esta opción nos permite en caso de conseguir captar las pulsaciones del teclado, que éstas estén cifradas y no sean legibles por un usuario externo, así en caso de robo de información pueden saber que estamos pulsando teclas pero no saben cuáles son al estar cifradas.

Si una vez activada la protección intentamos ejecutar el script anterior, nos encontramos con el siguiente mensaje:

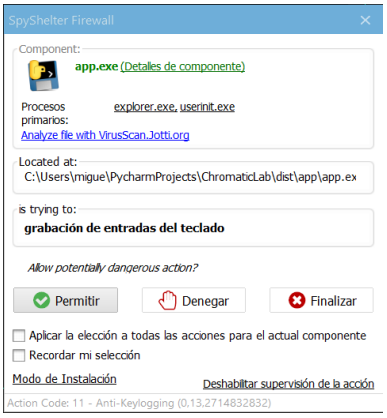

Figura 8: Alerta de SpyShelter

Podemos observar como SpyShelter nos muestra una advertencia de programa malicioso el cuál está tratando de grabar las entradas del teclado. Aquí el software ya nos está advirtiendo que algo no puede ir bien, si tras esto pulsamos en aceptar y ejecutamos el programa Keylogger podemos obtener la siguiente respuesta:

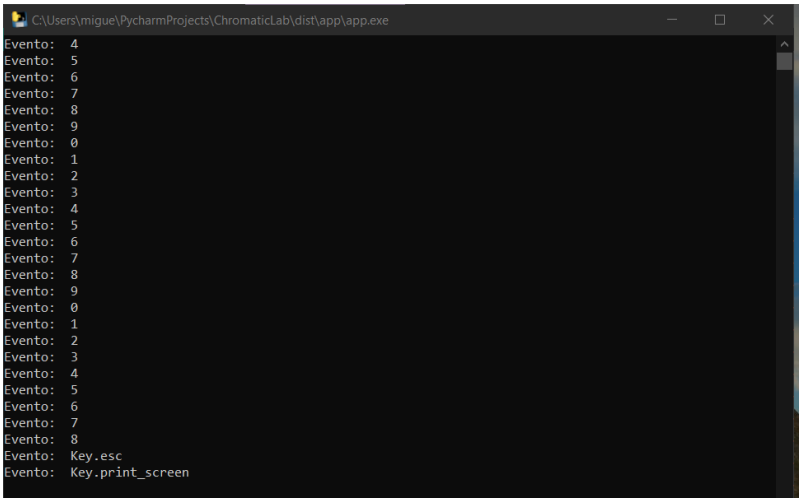

Figura 9: Captación del teclado - cifrado

En este caso a diferencia del anterior podemos ver que aunque captura los eventos del teclado, éstos son cifrados y no es capaz de obtener su verdadero valor. De esta forma al pulsar cualquier letra obtenemos esa respuesta en forma de número, estos números no tienen relación con la tecla pulsada, ya que si pulsamos la letra L sucesivamente podemos encontrar una secuencia de respuesta : 1,2,3,4,5,6,7, etc. De esa forma cada pulsación aunque sea en la misma tecla obtiene un valor diferente.

Ante la dificultad de mostrar esto con capturas, en este enlace se muestra el vídeo que verifica el experimento realizado: `https://www.youtube.com/watch?v=juZJgQuRNUw`

4.2. Experimento 2: Ataque y prevención DoS

En este segundo experimento, vamos a lanzar un ataque DoS a un servidor de Ubuntu, dicho servidor ha sido creado a través de una máquina virtual. Este ataque se basa en lanzar un número relativamente alto de peticiones a un puerto en concreto, en nuestro caso vamos a atacar el puerto 80, que corresponde al servicio apache2 (HTTP).

Para ello, hemos utilizado un script bash basado en pentBox (pentmenu). De forma general, pentBox es un suite de seguridad orientado a test de penetración que pone a prueba sitios web, además de escanear puertos, crear honeypot de forma rápida, etc. En nuestro caso, hemos utilizado el tipo de ataque *slowloris*, cuyo funcionamiento es mantener abiertas una gran cantidad de conexiones al servidor web destino y durante un periodo de tiempo alto, teniendo como resultado la caida del servidor, con un bajo uso de ancho de banda. Además, éste provoca una baja repercursión sobre servicios y puertos que no están relacionados de forma directa con el objetivo del ataque. Asimismo, cabe destacar que el script permite realizar más tipos de ataques DoS a parte del utilizado.

En primer lugar, vamos realizar el ataque sobre el servidor comentado anteriormente, provocando la caida de la página web de ejemplo creada. En la Figura 10 podemos ver el menú del que dispone el script utilizado. Tras seleccionar el ataque correspondiente (7 – slowLoris), especificamos la información necesaria, como la dirección IP del servidor, siendo ésta 192.168.56.101, el puerto por el que se va a lanzar las peticiones (80), el número total de peticiones a enviar, donde se han indicado 700 peticiones, así como el tiempo de espera entre petición (5 segundos), y por último indicamos que no se va a utilizar ningún tipo de protocolo de seguridad.

Figura 10: Ataque DoS

Una vez lanzado el ataque, podemos ver como las peticiones se van enviando de forma incremental al servidor (Figura 11) hasta llegar a la cantidad indicada, aunque por lo que hemos podido comprobar, el servicio se cae a alrededor de las 150 peticiones.

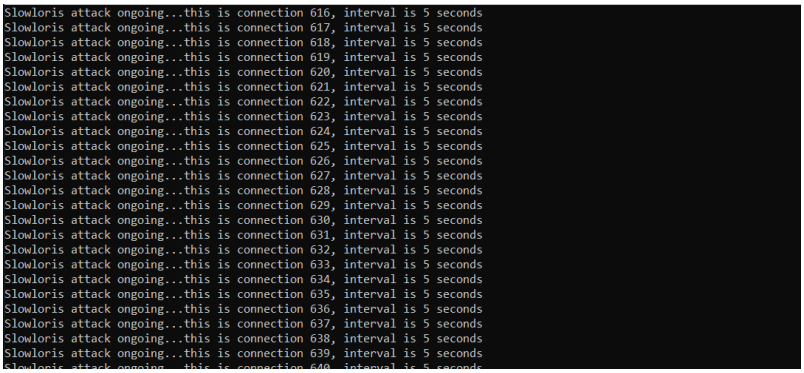

Figura 11: Envio de peticiones

El resultado del ataque se puede verificar simplemente comprobando a través del navegador web (google chrome) que la página web del servidor en un principio funciona correctamente y que una vez lanzado el ataque, a una cierta cantidad de peticiones, cuando recargamos la página web en el navegador, ésta indica que no es posible acceder a dicha dirección (Figura 12).

Ante la dificultad de mostrar esto con capturas, en este enlace se muestra el vídeo que verifica el experimento realizado: `https://www.youtube.com/watch?v=ufVd2RmM_pE`

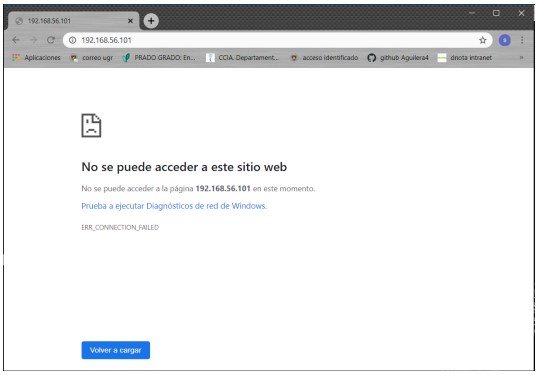

Figura 12: Caida del servicio

En relación con nuestro trabajo de prevención de ataques, el mécanismo para detener/prevenir llevado a cabo para este tipo de ataques es repartir la carga entre 2 o más servidores mediante un balanceador. En nuestro caso, este balanceo se va a realizar sobre dos servidores, por lo que ahora vamos a lanzar el ataque a la máquina balanceadora, teniendo en cuenta que los servidores cuentan con un cortafuegos que únicamente aceptan peticones del balanceador.

Para que el experimento tenga una base robusta y relativamente coherente, las cantidades de peticones lanzadas y el tiempo entre petición van a ser las mismas que las utilizadas para el ataque anterior (Figura 13). Por otro lado, la dirección del balanceador es 192.168.56.110.

```
1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) TCP SYN Flood       5) UDP Flood          9) Distraction Scan
2) TCP ACK Flood       6) SSL DOS           10) Go back
3) TCP RST Flood       7) Slowloris
4) TCP XMAS Flood      8) IPsec DOS
Pentmenu>7
Using netcat for Slowloris attack....
Enter target:
192.168.56.110
Target is set to 192.168.56.110
Enter target port (defaults to 80):
80
Using Port 80
Enter number of connections to open (default 2000):
700
Choose interval between sending headers.
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
5
use SSL/TLS? [y]es or [n]o (default):
n
```

Figura 13: Ataque DoS al balanceador

Tras lanzar el ataque, podemos comprobar como en ningún momento el sitio web deja de funcionar, por lo que podemos concluir que este mecanismo es capaz de prevenir el ataque. Cabe destacar, que para un número mayor de peticiones el balanceador termina cayendose. Asimismo, una posible solución es aumentar nuestra granja web horizontal o verticalmente, adentrandonos en temas de escabilidad de servidores. Ante la dificul-

tad de mostrar esto con capturas, en este enlace, `https://www.youtube.com/watch?v=Os2o44h2Xm4`, se muestran los videos que verifican el experimento.

5. CONCLUSIONES

Como hemos comentado, los ataques informáticos están viviendo un momento de auge absoluto y todo apunta a que en los próximos años va a ir a más. Nosotros hemos hecho hincapié en tres de los más principales; **Man in the Middle, DoS y Keyloggers**.

Hay bastante más, los *Malware* por ejemplo están presentes en una gran cantidad de páginas web, aunque sus técnicas de prevención son algo más sencilla generalmente, bastando con instalar extensiones en el navegador en muchos casos. El *Phishing* es otro de los ataques con más presencia en la actualidad, ataque por el cual intenta suplantar tu itendidad, ya sea robándote tus credenciales bancarias, contraseñas de perfiles, etc.

Bien, estos dos tipos de ataques no los hemos incluído puesto que consideramos que la concienciación del usuario a la hora de navegar por internet es crucial a la hora de prevenir gran cantidad de éstos. Si un usuario se preocupa en verificar que el sitio al que está accediendo es seguro y no descarga archivos de dudosa procedencia, además de contar con antivirus y extensiones de navegador, probablemente no se infecte de malware nunca. Por otro lado, si un usuario presta especial atención a los correos que recibe, comprobando que provienen de orígenes de confianza, la probabilidad de sufrir phishing disminuye.

En cambio, como hemos demostrado en la experimentación, los ataques DoS o Keyloggers son mucho más difíciles de detectar a simple vista. En la experimentación realizada con Keylogger se ha podido ver que cada tecla pulsada, era registrada, siendo invisible para el usuario. Por otro lado, con la experimentación de DoS la única forma que el usuario tiene a simple vista de percibir que está siendo atacado es cuando el servicio se cae, momento en el que ya es tarde para actuar.

En nuestro caso, para prevenir el ataque Keylogger hemos usado la herramienta SpyShelter, en la que no sólo hemos configurado para que sea detectado el ataque sino que también se cifren las teclas pulsadas, de forma que la información robada sea inútil. Por otro lado, para prevenir el ataque DoS hemos optado por un balanceo de carga entre los diferentes servidores, de forma que las masivas peticiones no se atienden en un sólo servidor sino que se reparten, evitando así que el servicio caiga.

A modo de conclusión, vemos que si bien herramientas como el antivirus o las extensiones de navegador pueden ser útil para prevenir cierto tipos de ataques, existen otros muchos ataques que son imparables para esas herramientas y cuyas técnicas de prevención requieren de un nivel de informática algo más avanzado que el que tiene la inmensa mayoría de la población a día de hoy. Por lo tanto, consideramos que llega a ser preocupante

la falta de conciencia por parte de la sociedad ante los ataques informáticos, porque recordemos que en éste 'juego' no hay ganador, por muchas técnicas de prevención que se descubran, siempre van a aparecer nuevos ataques.

6. BIBLIOGRAFÍA

- SpyShelter
  https://www.techulator.com/resources/13324-Review-of-SpyShelter-Stop-Logger-An-effi
  aspx
- Ghostpress
  https://www.redeszone.net/2016/05/23/ghostpress-una-sencilla-herramienta-protegerno
- Zemana Antilogger
  https://www.techspot.com/downloads/5413-zemana-antilogger.html
- Ataque Man in the Middlehttps://technologyforgippsland.com.au/cyber-security/
  man-in-the-middle-attack
- Riesgos y medidas de prevención
  https://www.infobae.com/america/tecno/2019/11/21/8-especialistas-en-seguridad-infor
- Phishing
  https://www.phishprotection.com/content/phishing-prevention/
- SQL Injection
  https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-inject
- Prevención
  https://www.researchgate.net/profile/Cesar_Vallejo_De_La_Torre/publication/
  328007416_Sistemas_de_Prevencion_de_Intrusos_IDS_en_la_Gestion_de_la_
  Informacion/links/5bb296fba6fdccd3cb8137a0/Sistemas-de-Prevencion-de-Intrusos-IDS-e
  pdf
- Ataque Dos
  https://e-archivo.uc3m.es/bitstream/handle/10016/29630/TFG_Javier_Bautista_
  Rosell.pdf?sequence=1&isAllowed=y
- Ataque Man in the Middle
  https://www.redeszone.net/tutoriales/seguridad/ataques-man-in-the-middle-evitar/
- Programas anti-keylogger
  https://mundowin.com/5-mejores-programas-anti-keylogger-gratuitos-que-protegeran-lo
  de Keylogger
- Ataque DoS
  https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion