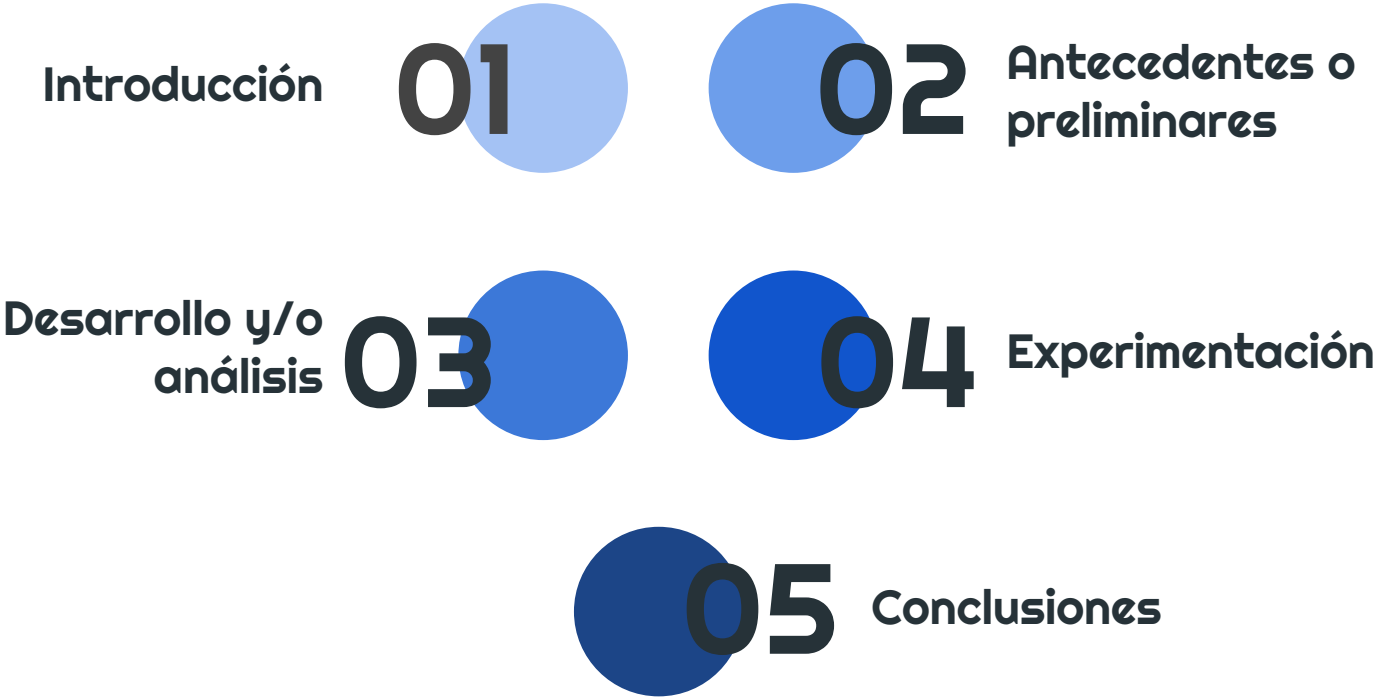
Prevención de ataques

Integrantes

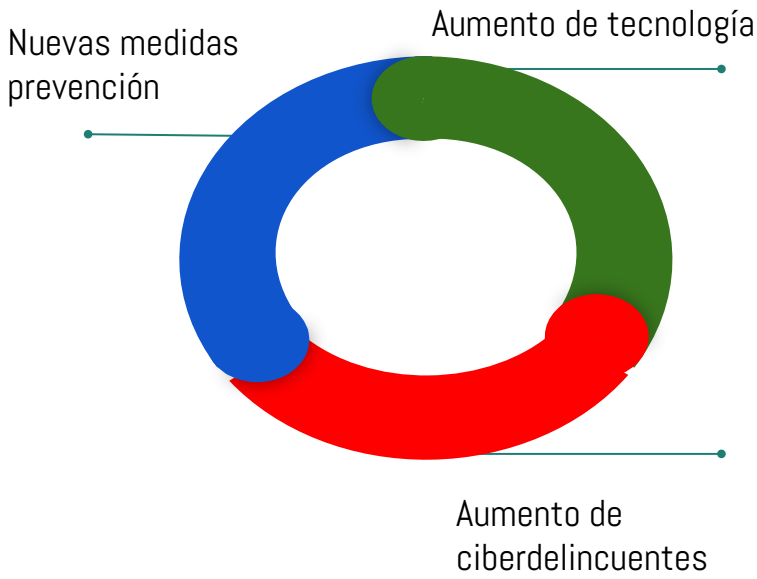
EL GRUPO ESTÁ COMPUESTO POR :

- SERGIO AGUILERA RAMÍREZ
- MIGUEL ANGEL PÉREZ DÍAZ
- CHRISTIAN VIGIL ZAMORA


Introducción
01
02
Antecedentes o preliminares
Desarrollo y/o análisis
03
04
Experimentación
05
Conclusiones

01 Introducción

- Conexión a internet muy generalizada actualmente, tanto empresas como familias, pero no todo el mundo lo utiliza para la misma intención.
- Cada vez más empresas optan por la digitalización para llegar a un público más amplio, esto supone alojar datos en Internet.
- A día de hoy la tecnología sigue aumentando considerablemente, lo que supone un aumento de ciberdelincuentes tratando de acceder a cualquier tipo de dato.
- Por tanto cada vez es más necesario prevenir estos tipos de ataques y evitar que los atacantes puedan acceder a nuestros sistemas.



02

Antecedentes o preliminares

ATAQUE INFORMÁTICO

Un intento organizado e intencionado causado por una o más personas para infringir daños o problemas a un sistema informático o red.

La herramienta más utilizada y generalizada, y que puede considerarse un antecedente es el **ANTIVIRUS**, ya que ha dado lugar a técnicas de prevención más complejas, las cuales requieren un nivel de usuario más avanzado en la informática.

¿PERO QUÉ ES UN ANTIVIRUS?

Se trata de un programa dedicado a detectar virus, bloquearlos y eliminarlos. A día de hoy son capaces también de detectar malware, spyware...

03

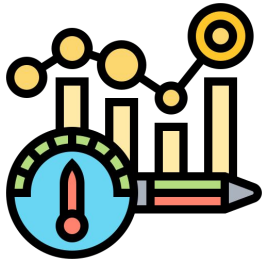
Desarrollo y/o análisis

Pasos para realizar la tarea de prevención

Identificar aquello que debemos proteger

Identificar aquellos sucesos que pueden ocurrir

Identificar las vulnerabilidades

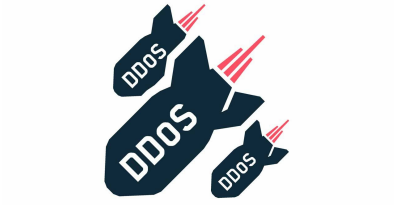


Evaluar el grado de vulnerabilidad

Principales ataques

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.



Ataque DoS

Consiste en enviar gran cantidad de peticiones a un mismo punto para que el servidor no soporte la cantidad de paquetes recibidos y en consecuencia se caiga el servicio.

Keylogger

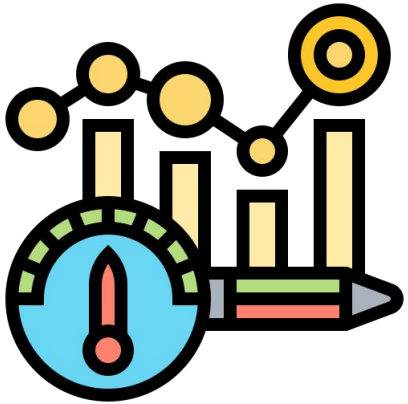
Se trata de un programa software o hardware utilizado por los usuarios atacantes, permitiéndoles conocer las teclas que son pulsadas por el usuario afectado

Identificación de las vulnerabilidades

- Total acceso a la web y uso de correos
- Control de antivirus y firewall deficiente
- Deficiente configuración de seguridad
- Deficiente monitorización de seguridad
- Débil segmentación de red
- Políticas de contraseñas frágiles
- Información no cifrada

Evaluar el grado de vulnerabilidad

- Identificación de los controles de seguridad y su evaluación eficiente.
- Permitirá tener una idea del grado de vulnerabilidad actual de la institución y la facilidad con que las múltiples amenazas se podrían materializar



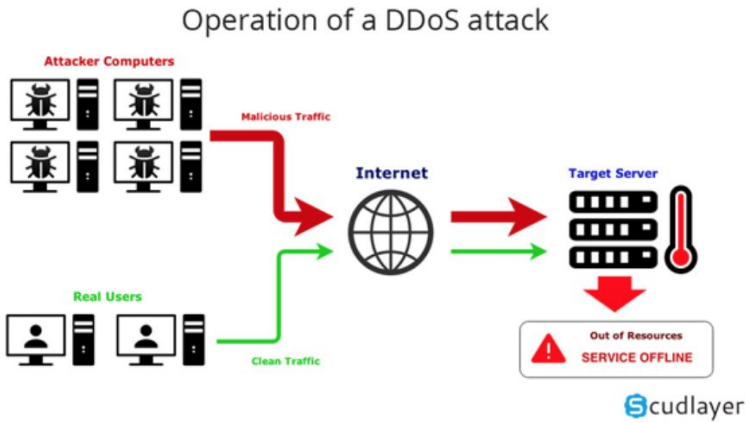
Técnicas de prevención de ataques

- Man in the middle
- DoS
- Keyloggers

Prevención ataque MitM

- Redes privadas VPN
- Inicios seguros, HTTPS, TLS
- Redes wifi divididas
- Sistemas IDS
- Herramienta Etherwall

Prevención ataques DoS



- Medidas de protección en la red interna
- Medidas de protección en el hosting
- Ancho de banda
- Redundancia y balance de carga
- Soluciones de seguridad basadas en la nube
- Sistemas actualizados

Prevención de ataques keyloggers

Zemana Anti-Logger

- Fácil de usar
- Poderosa
- Monitorización en tiempo real
- Cifrado de pulsación de tecla
- Protege la información tanto del navegador como las aplicaciones de la computadora.

Ghostpress

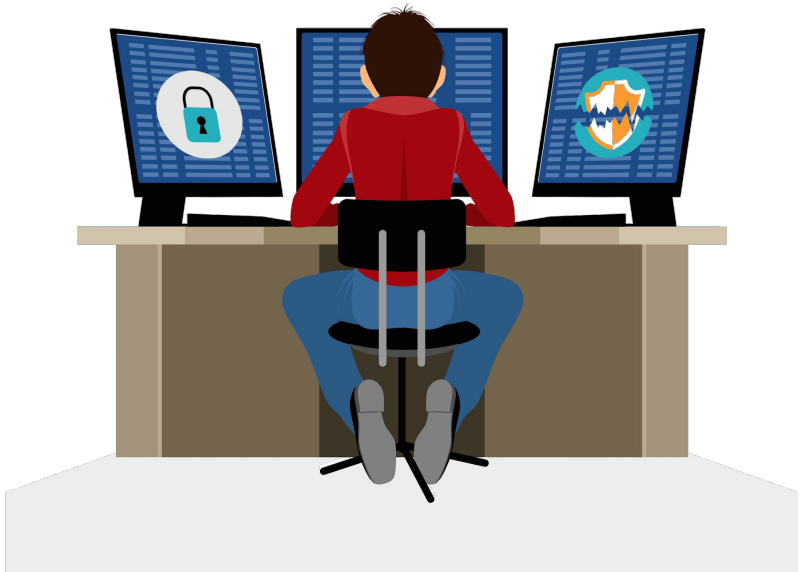
- Gratuita
- Ocultación de teclas y pulsaciones en su totalidad
- Fácil de usar
- Flexibilidad de configuración en la protección

Shelter Anti-keylogger

- Detecta y detiene cualquier tipo de malware
- Protege todos los módulos del sistema
- Monitorización en tiempo real
- Bloqueo de amenazas y aviso al usuario
- Sistema de encriptación de pulsaciones
- Integra un sistema de seguridad para conexiones HTTTP, HTTPS, etc.
- Analiza solicitudes entrantes y salientes

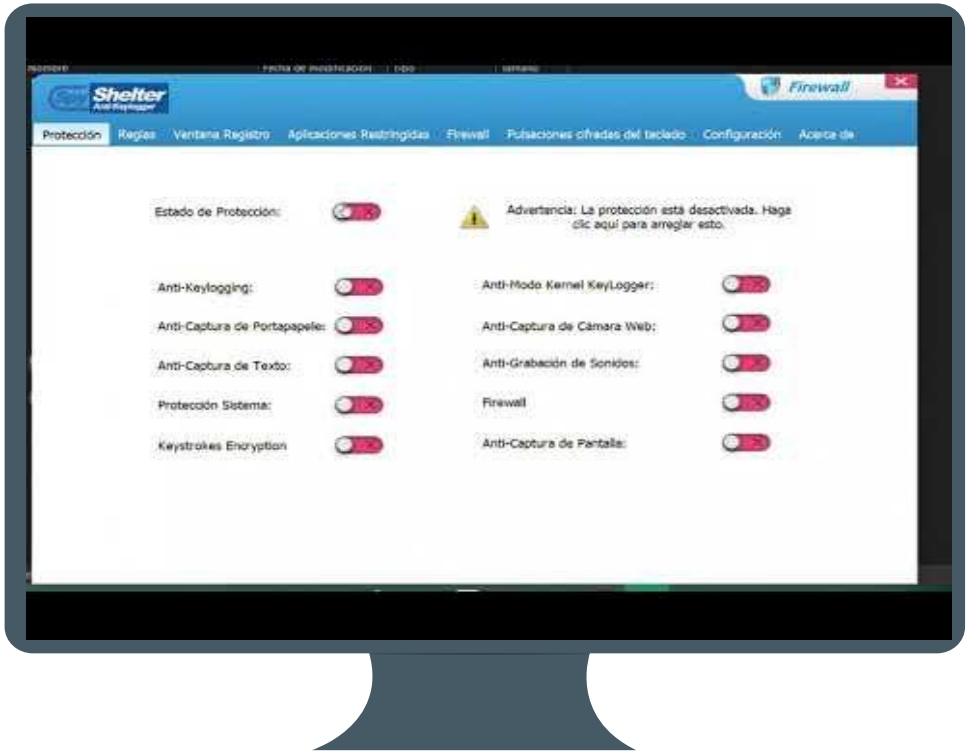
04

Experimentación



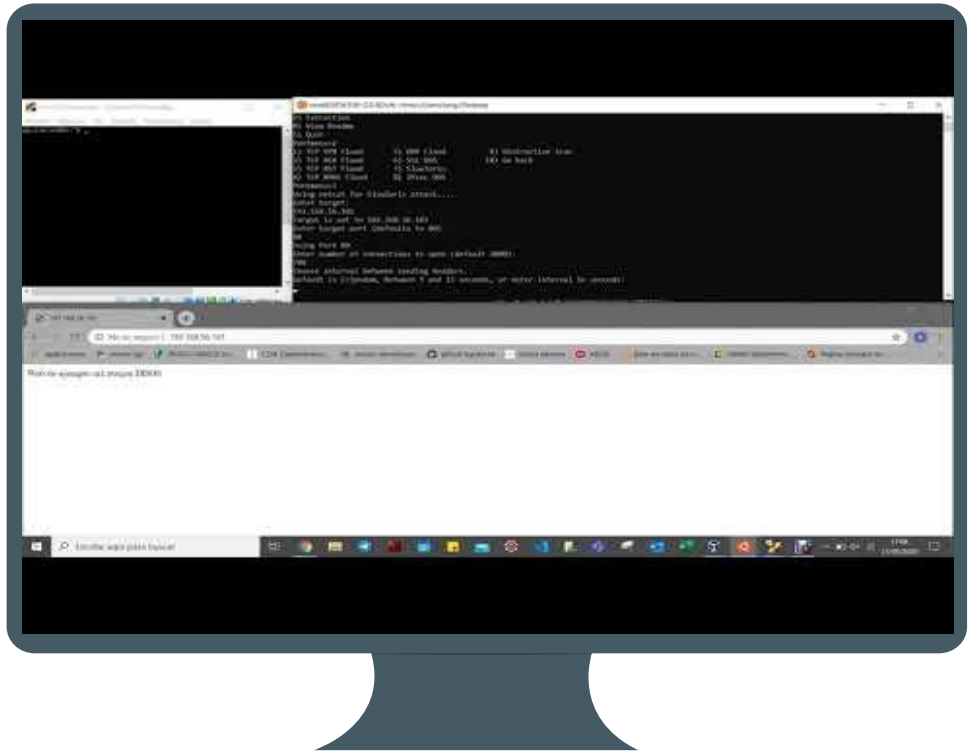
Demostración Keyloggers

- Vamos a realizar un ataque keylogger sobre nuestro sistema.
- El objetivo de dicho ataque es capturar la secuencia de teclas pulsadas mientras esté activo el ataque.
- Para prevenirlo, hemos instalado SpyShelter, herramienta usada para detectar el ataque.
- Además de activar la función de cifrar las teclas, para no revelar información.



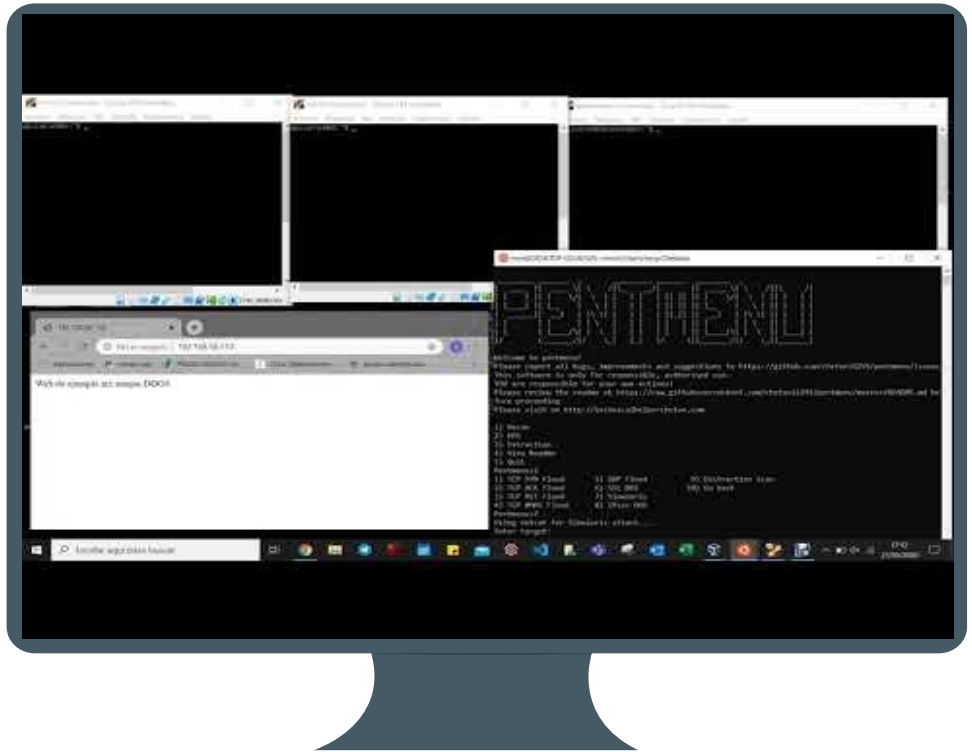
Demostración DoS

- Se va a realizar un ataque DoS a un servidor de Ubuntu, alojado en una máquina virtual.
- En nuestro caso, se lleva a cabo sobre el puerto 80, ya que se van a realizar numerosas peticiones HTTP en paralelo.
- La consecuencia de dicho ataque es la caída temporal del servicio sino se previene de forma correcta.



Demostración DoS

- Para prevenir el efecto tan grave que supone un ataque DoS, hemos optado por un balanceador de carga.
- Es decir, las peticiones que llegan son atendidas de forma alternativa por los dos servidores que componen la granja web.
- De ésta forma conseguimos que el servicio no llegue a saturarse y no sufra una caída.



05 Conclusiones

- Ciertos ataques como Malware o Phishing pueden ser prevenidos con un uso responsable de Internet
- Otros ataques como los que hemos trabajado requieren conocimiento más profundo sobre la materia
- Antivirus y extensiones del navegador herramientas más extendidas
- + Prevención → + Ataques

Gracias!

Cualquier duda:
sergioaguilera@correo.ugr.es
christianvz@correo.ugr.es
mapd0004@correo.ugr.es