Tipos de ataques informáticos

Jose Manuel Enriquez Fernandez
Alberto Villanueva Copado

¿Qué es un hacker?

- White hats :

- Black hats:

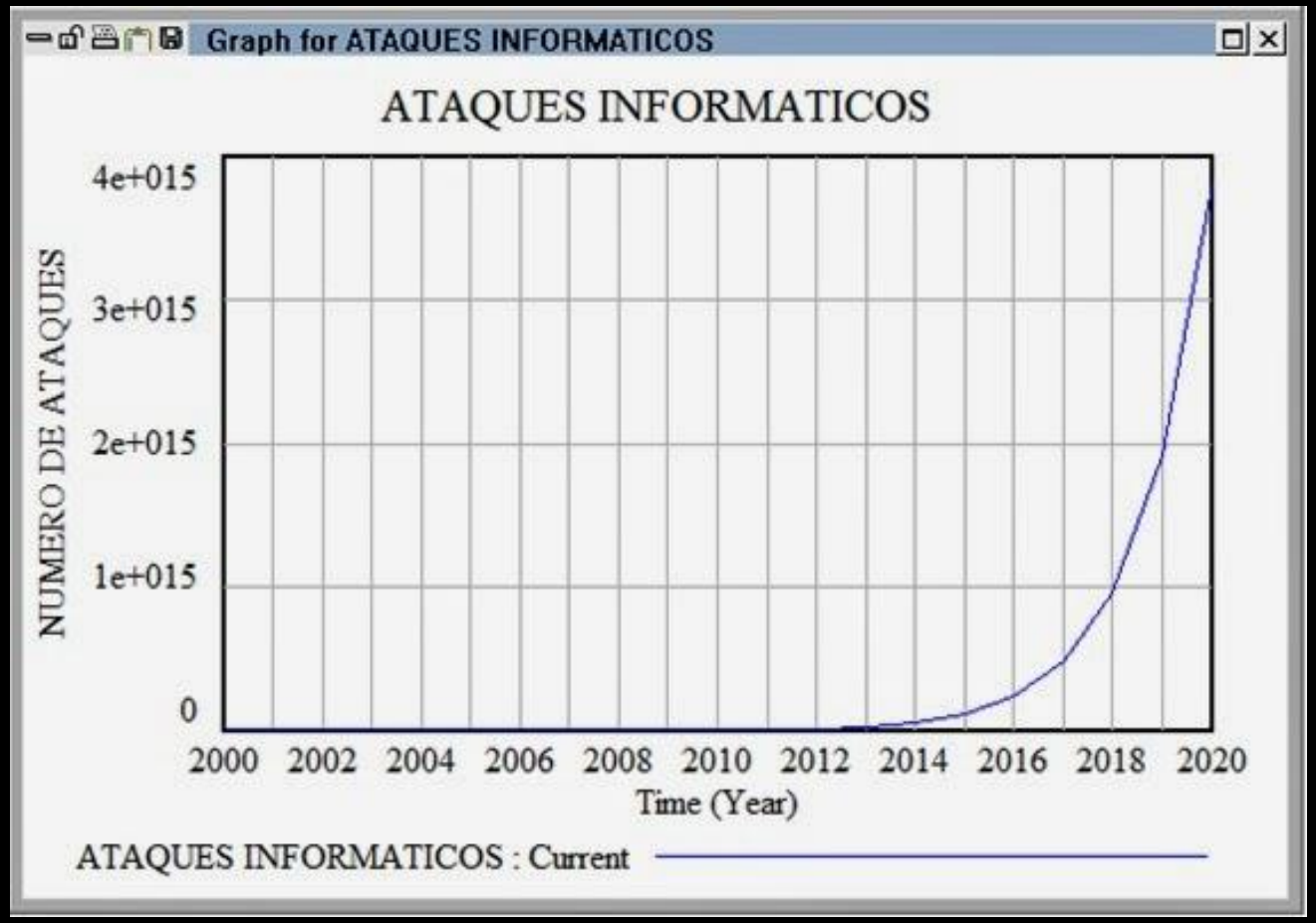
¿Qué es un ataque informático?

- Como definición formal: Un ataque informático es un intento organizado e intencionado, que puede estar causado por una o más personas, para infringir daños a la seguridad de un sistema informático o red.

- Los principales objetivos suelen ser empresas importantes o celebridades.

- Ejemplos de ataques.

Ataques informáticos en el tiempo



Herramientas

- Nmap.
- Metasploit.
- Angry IP scanner.
- Cain and Abel
- John The Ripper.
- THC Hydra.
- Burp Suite
- Ettercap.
- Wapiti.

Tipos de ataques informáticos

- Ingeniería social.
- Ingeniería social inversa.
- Trashing o cartoneo.
- Ataques de monitorización.
- Ataques de autenticación.
- Denial of Service (DoS).
- Ataques de modificación o daño.

Tipos de ataques informáticos: Ingeniería social

- Manipulación de personas para que realicen actos que habitualmente no realizan y que revelan información importante del sistema.
- La principal causa por la que ocurren es la inexperiencia de los usuarios.
- Es uno de los tipos de ataques más usados para obtener usuarios y contraseñas.

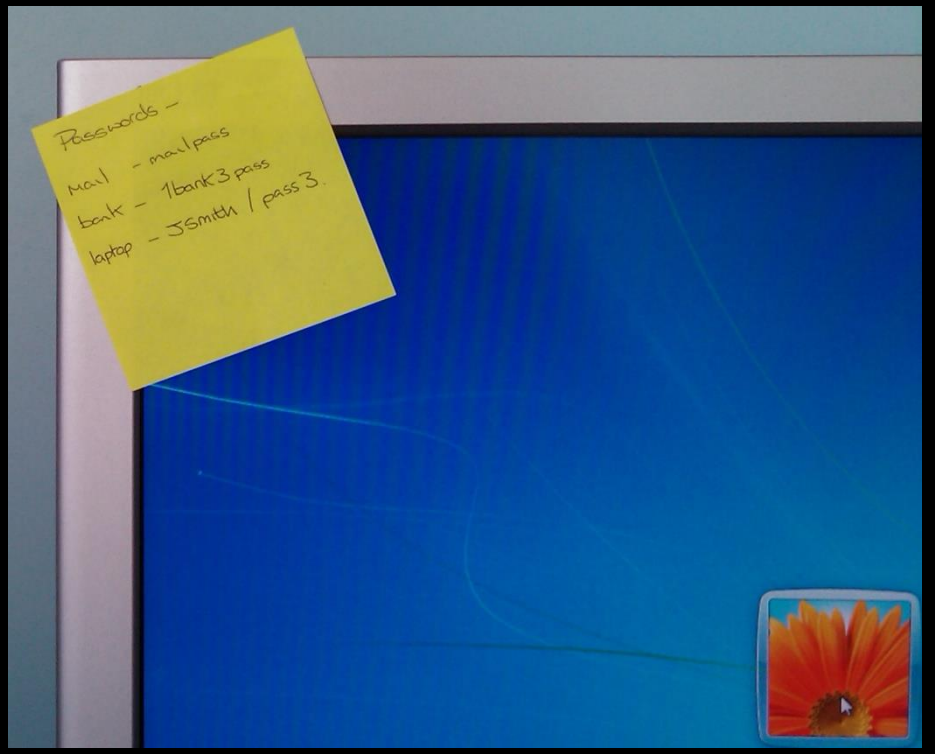
Tipos de ataques informáticos: Ingeniería social inversa

- Genera una situación inversa a la que se genera en los ataques de ingeniería social.
- Normalmente el atacante publicita su ayuda a los usuarios por un problema que el mismo ha creado.
- Este tipo de ataques necesitan más preparación y requieren que el atacante tenga un cierto contacto con el sistema.

Tipos de ataques informáticos: Trashing o cartoneo

- Es uno de los ataques más simples y suelen producirse por un integrante de la empresa a la que se ataca.

- Normalmente cuando a un usuario se le dan unos credenciales para autentificarse en un sistema, los suelen escribir y dejarlos por la mesa, el intruso se dedica a robar estos credenciales.



Tipos de ataques informáticos: Monitorización

- Shoulder Surfing: Intenta observar físicamente el usuario y la contraseña de los usuarios.

- Decoy o señuelos: Programas falsos diseñados con la misma interfaz que el orignal.

- Scanning o búsqueda: Recorre todos los puertos de una red y guarda información de los que son receptivos o de uso relevante para el atacante.

Tipos de ataques informáticos: Monitorización → Scanning

- TCP connect scanning: Forma básica de escaneo de puertos.
- TCP SYN scanning: Utilizando el protocolo Three-way-Handshake se abre "media conexión" con el servidor.
- TCP FIN Scanning-Stealth Port Scanning: Tipo de escaneo difícil de detectar. Basa su uso en el paquete FIN.
- Fragmentation scanning: Envía fragmentos ip indetectables por los firewalls, pero es fácilmente detectable por el administrador.
- Eavesdropping-Packet Sniffing: Se basa en la vulnerabilidad de capturar el tráfico de una red mediante sniffers. La dificultad de este procedimiento es colocar el sniffer.
- Snooping-Downloading: Obtienen información sin modificarla como la técnica anterior pero además la descargan en otra máquina.

Tipos de ataques informáticos: Autenticación

- Spoofing-Looping: El principal objetivo es realizar ataques haciéndose pasar por otros usuarios.

- Spoofing: Tipos de ataques que requieren el conocimiento absoluto de protocolos para aprovechar sus debilidades.

Tipos de ataques informáticos: Autenticacón → Spoofing

- IP Spoofing: Se generan paquetes de red cambiando el campo “from” del paquete.
- DNS Spoofing: Se modifican paquetes UDP intentando que el principal afectado sea el servidor DNS para incrustas direcciones ip falsas en el.
- Web Spoofing: Se crea un sitio web falso pero estéticamente similar al original.
- IP Splicing-Hijacking: El atacante suplanta la identidad de la víctima una vez se ha identificado en el sistema.
- Backdoors: Formas de entrar en un sistema que los desarrolladores usan para probarlo y se olvidan de eliminar del código.
- Exploits.
- Obtención de contraseñas: Este método comprende tanto el uso de la ingeniería social como el de algoritmos de fuerza bruta para obtener contraseñas.

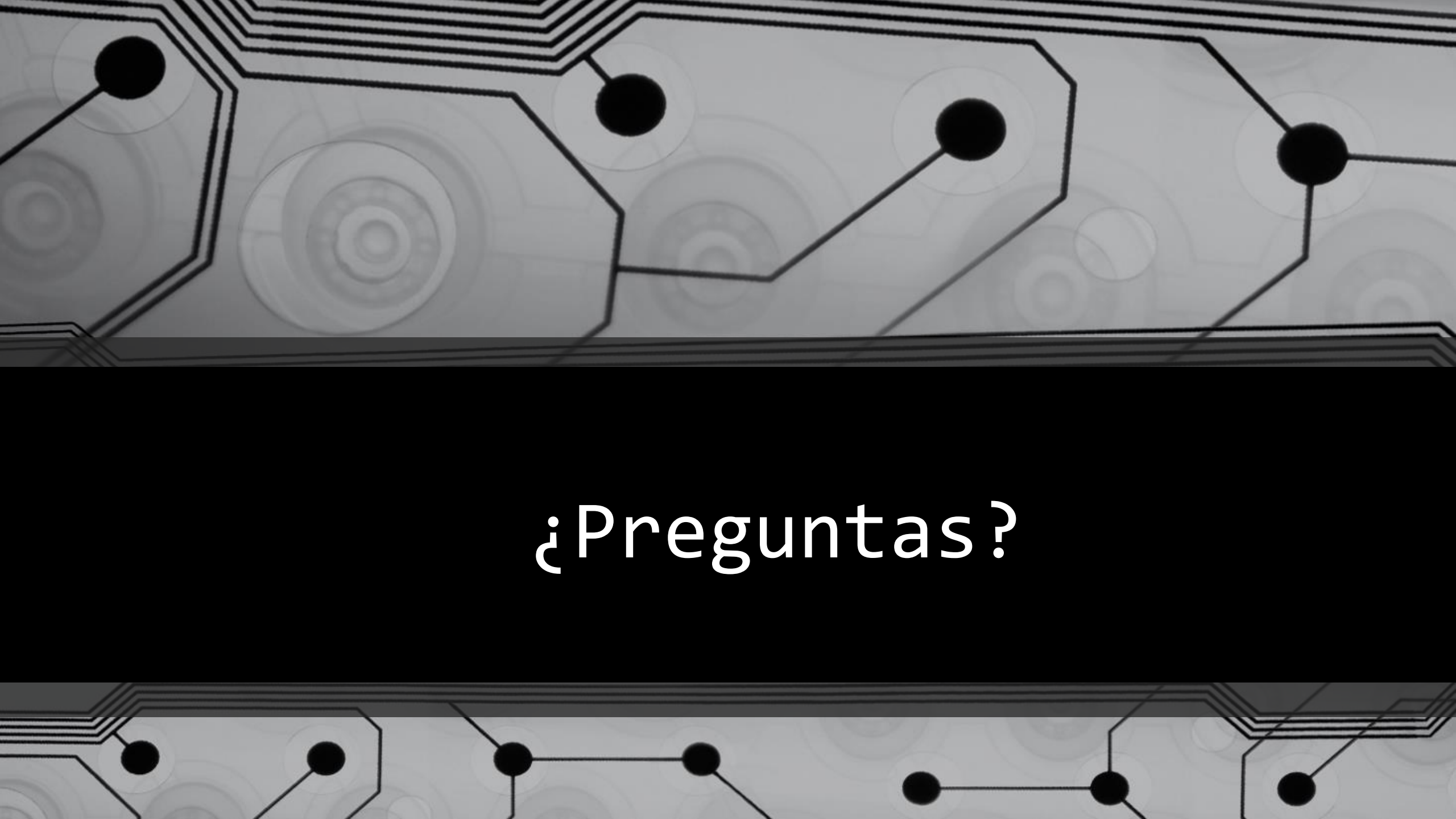
Tipos de ataques informáticos: Denial of Service

- Jamming o Flooding: La finalidad de este ataque es desactivar o saturar completamente los recursos de un sistema.
- Syn Flood: Este es el ataque más famoso de este tipo. Acaba agotando la memoria del servidor hasta que se satura por falta de la misma.
- Connection Flood: Monopoliza todas las conexiones simultáneas que admite un servidor.
- Net Flood: Consiste en saturar la línea para que solo lleguen al servidor un tipo de paquetes.
- Land attack: Aprovecha un bug en el protocolo TCP de Windows y satura el servidor con un paquete con la misma dirección origen y destino.
- Smurf: Envía un paquete broadcast con la dirección destino cambiada para que todos la acepten y respondan a la vez hacia una misma máquina.
- Supernuke: Uno de los ataques más comunes en equipos Windows que tienen abierto el puerto NetBIOS. Consiste en enviar paquetes Out of Band de forma masiva para que la máquina no pueda manejarlos.
- Teardrop I: Consiste en la modificación de fragmentos de paquetes para que se superpongan en la pila y el sistema no sea capaz de volver a montar el paquete a partir de ella.

Tipos de ataques informáticos: Modificación/Daño

- Tampering o Data Diddling: Modificación de datos o del software no autorizada.
- Ataques mediante Java Applets: En los navegadores se incluyen máquinas de java que pueden ser modificadas para extraer información del sistema.
- Ataques mediante JavaScript y VBSscript: Lenguajes usados para su ejecución en los navegadores web, pueden recopilar información.
- Ataques mediante ActiveX: Mediante el uso de certificados maliciosos y la aceptación de los usuarios.
- Vulnerabilidades de los navegadores.

Demostración


¿Preguntas?