



# 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.
- Ettercap.
- Metasploit.
- Angry IP scanner.
- Cain and Abel
- John The Ripper.
- Burp Suite



# 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

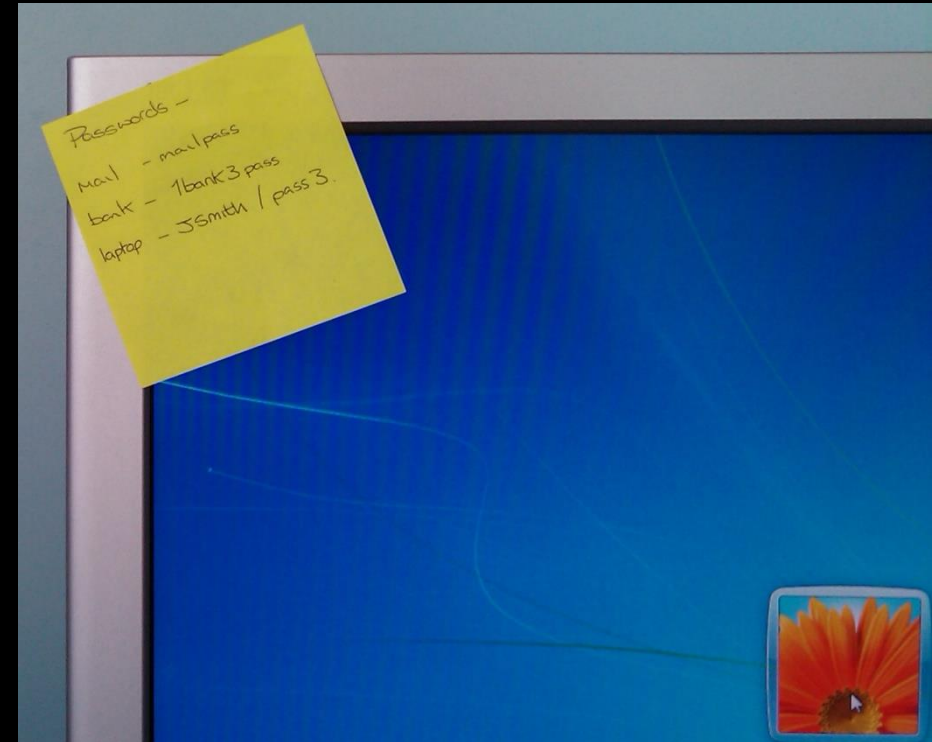


- Genera una situación inversa a la que se genera en los ataques de ingeniería social.
- Normalmente el atacante publicita su ayuda a los usuarios por un problema que el mismo ha creado.
- Este tipo de ataques necesitan más preparación y requieren que el atacante tenga un cierto contacto con el sistema.



# 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 es atacada.
- Normalmente cuando a un usuario se le dan unos credenciales para autenticarse 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 original.
- 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:

## Autenticación → 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 incrustar 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.
- Gps.
- Email.

# Tipos de ataques informáticos: Denial of Service

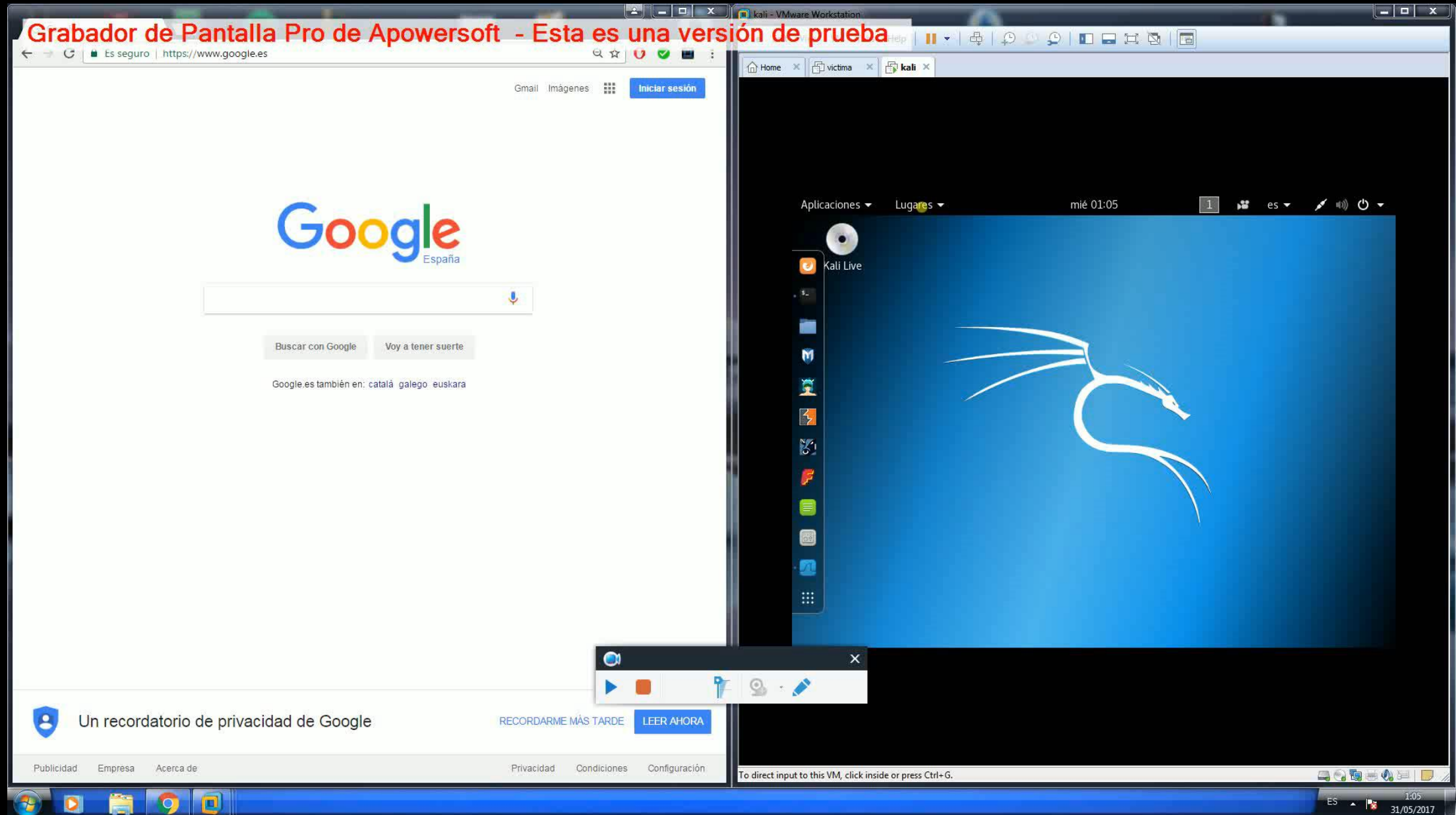
- Syn Flood: Este es el ataque más famoso de este tipo. Acaba agotando la memoria del servidor hasta que se satura por falta de la misma.
- ICMP Flood: Monopoliza todo el ancho de banda de un servidor.
- UDP Flood: Lanza paquetes UDP contra distintos puertos.
- Smurf: Envía un paquete broadcast con la dirección destino cambiada para que todos la acepten y respondan a la vez hacia una misma máquina.

# 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 VBScript: 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?