Explotación de Adobe. Análisis de un PDF

Ing. Carlos Loyo

CCNA, CCFI, Auditor Lider ISO 27001

Agenda

- Hackers & Hacking
- Malware
- Metodos de ataques
  - Caso Practico: Inyección de Malware
- Informática Forense
- Procedimientos de análisis
  - Caso Practico: Análisis de Malware

Hacking

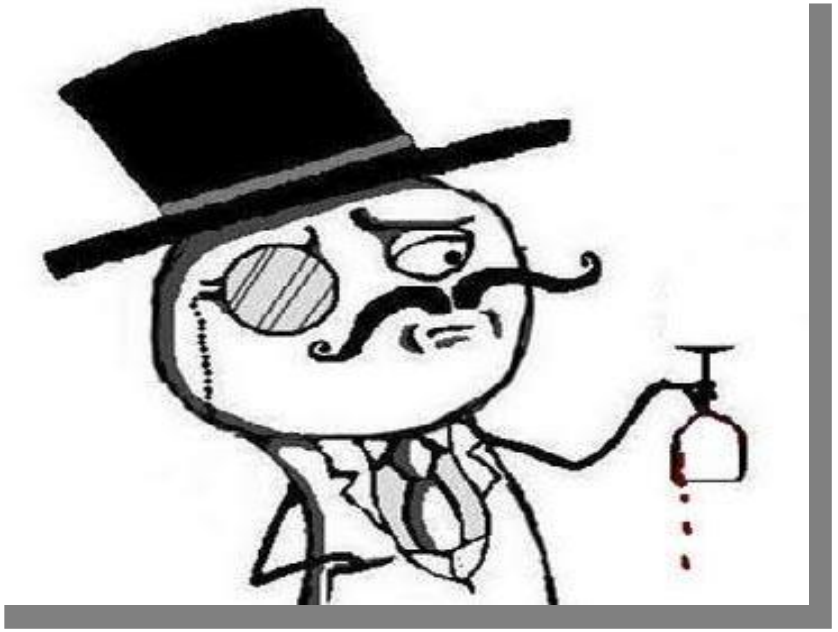
Rafael Nuñez
Alias: El RaFa
Capturado por EEUU
por acceso indebido

Carlos Loyo
Alias: No asignado
Capturado por su
Mama viendo pornografía

Hacking

Hacking


LatinHackTeam Ownz Your Box
..We Are..
infEkt - Adminp4nic - eCORE
Againts governments corruptions !!
your security.. get down !!
Follow us @LatinHackTeam @infEkt1



Hacking

- 1era programación de Malware
- Sigiloso, Avanzado y Persistente: APT
- Definición de Packer

Malware

También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Malware

Malware infeccioso: virus y gusanos

Malware oculto: Backdoor o Puerta trasera, Drive-by Downloads, Rootkits y Troyanos

Puertas traseras o Backdoors
Drive-by Downloads
Rootkits
Troyanos

Malware

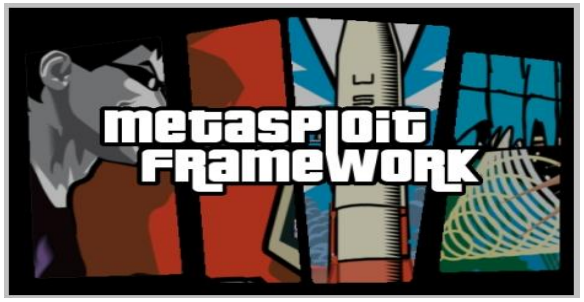
Malware para obtener beneficios

- Mostrar publicidad: Spyware, Adware y Hijacking
- Robar información personal: Keyloggers y Stealers
- Realizar llamadas telefónicas: Dialers
- Ataques distribuidos: Botnets

Metasploit

•Herramienta GNU escrita en perl y con utilizacion de diversos lenguajes de programacion como C, Python, ASM ,etc, para el desarrollo, testeo, mejora y penetracion a diversos sistemas

•Contiene una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades



Metasploit

- Payload

- Exploit

SET Social Engineering Toolkit

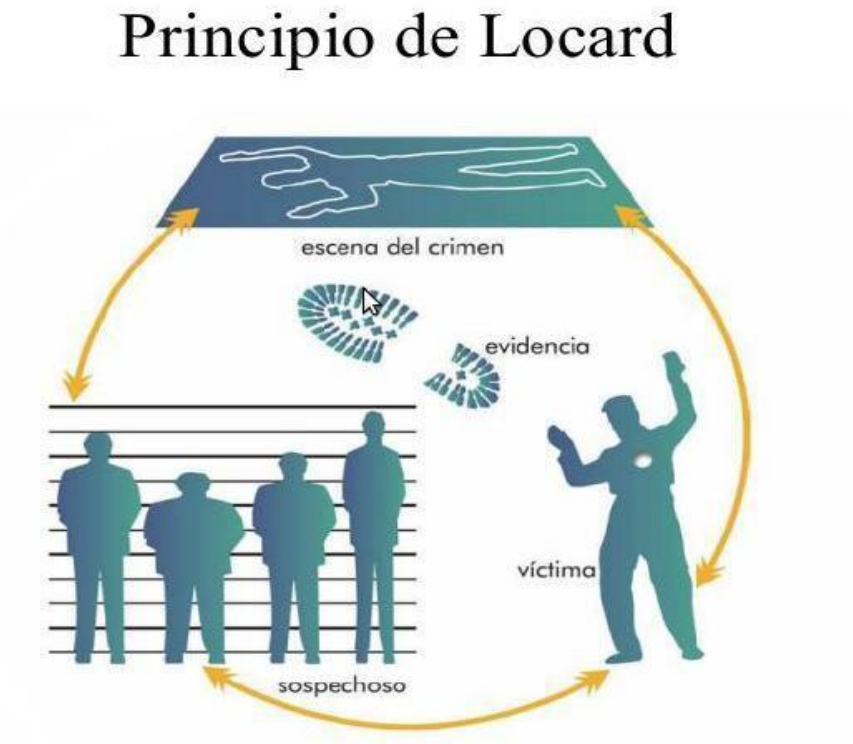
SET es una completísima suite dedicada a la ingeniería social , que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos a clonar cualquier pagina web y poner en marcha un servidor para hacer phishing en cuestión de segundos

Malware

Practica: **Propagación de Malware**

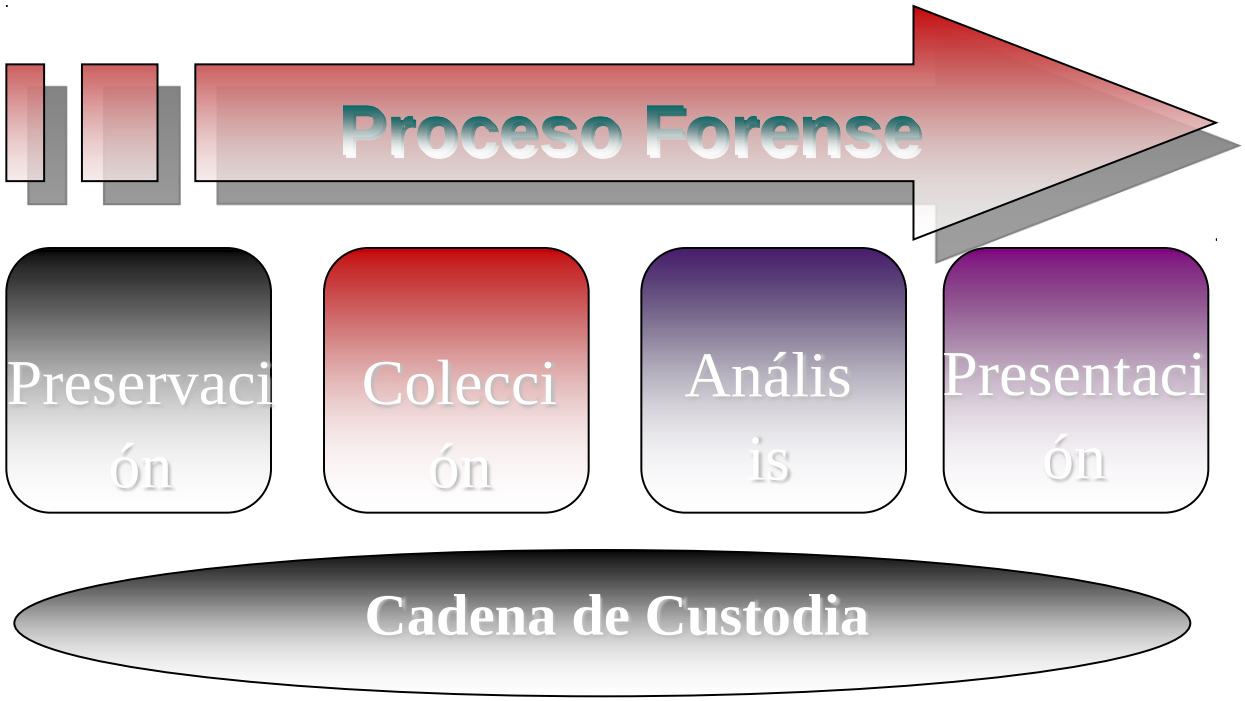
Análisis Forense

PRINCIPIO DE INTERCAMBIO DE LOCARD



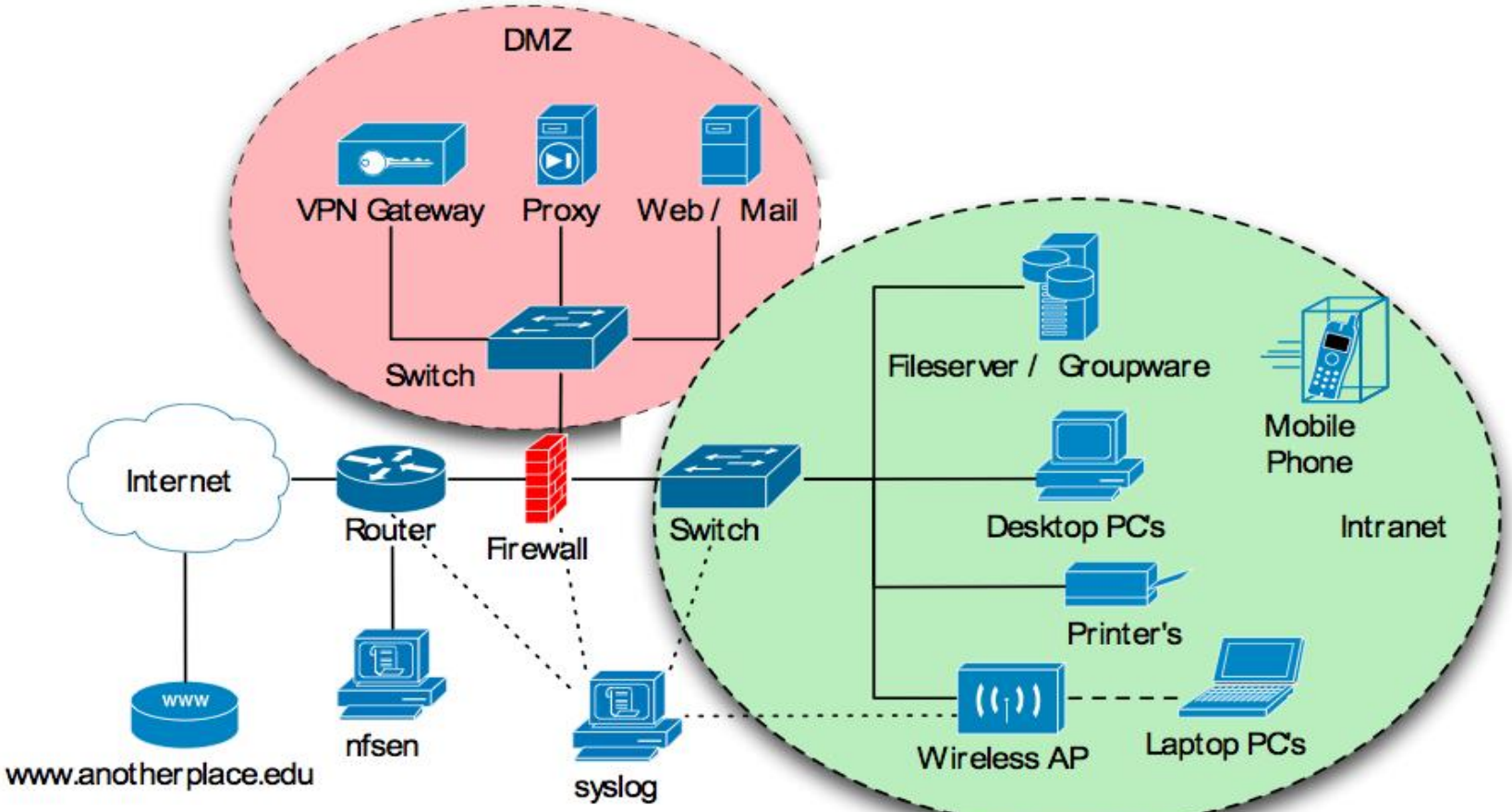
"Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto"

ETAPAS INFORMATICA FORENSE



Evidencia Digital

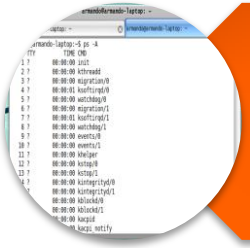
¿DONDE PUEDO ENCONTRAR EVIDENCIA?



Análisis del Malware

Escanear Puertos Abiertos

- Netstat
- Fport
- TCPView
- Nmap



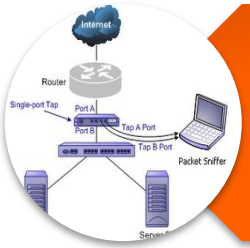
Escanear procesos Sospechosos

- PrcView
- Utilidades Linux
- MS Config
- Process Viewer

Escanear Registros Sospechosos

- Utilidades Linux
- Ficheros Windows
- Herramientas de Análisis Forense
- MS Config

Análisis del Malware



Escanear Actividades En la Red

Tcpdump
Wireshark
Xplico

Correr Escaner para Detectar Troyanos

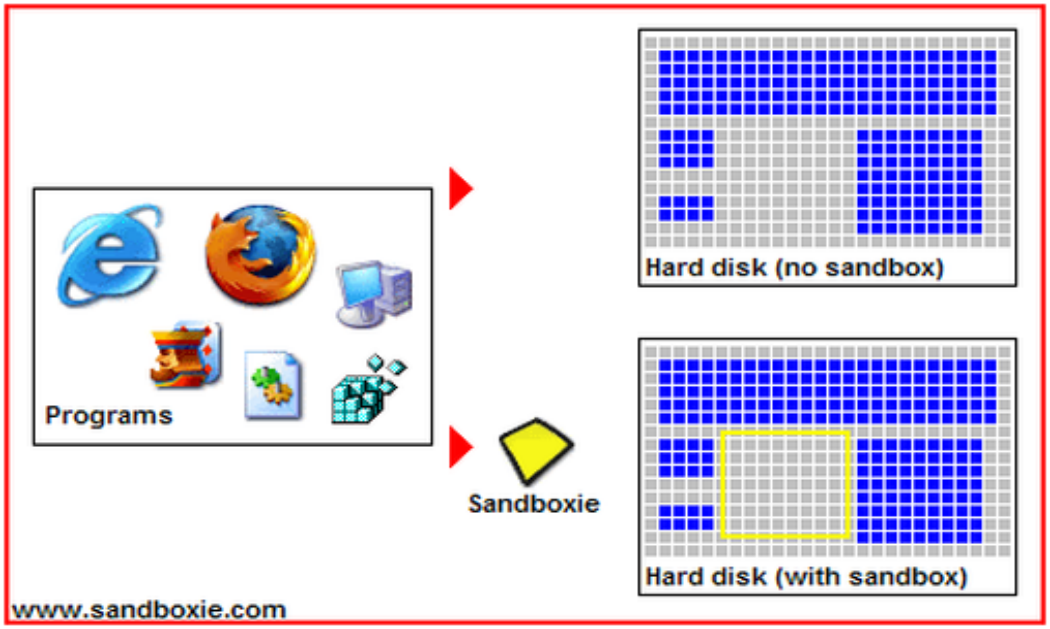
Trojan Guard
Trojan Hunter
ZoneAlarm
Anti Trojan

Análizar archivos sospechos

Autopsy
Sandbox
Encase
xxd

Análisis del Malware

Sandbox



cuckoo

PDF

PDF (sigla del inglés portable document format, formato de documento portátil)

Es un formato de almacenamiento de documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).

PDF

La estructura del fichero

- Una cabecera *(header):* Ejemplo: "%PDF“
- Un cuerpo *(body area)*
- Una tabla de referencias cruzadas *(cross-reference table)*
- *(trailer):* "%%EOF"

Ollydbg

OllyDbg es frecuentemente usado para la ingeniería inversa de programas. Es frecuentemente usado por crackers para crackear software hecho por otros desarrolladores. Es a menudo la herramienta primaria para cracking e ingeniería inversa debido a su facilidad de uso y disponibilidad. Es también útil para que los programadores se aseguren de que su programa está corriendo según lo previsto.

Malware

Practica: Análisis de Malware

GRACIAS POR SU ATENCIÓN

Que viva la Vinotinto!!!!!!

Contacto: carlosloyo23@gmail.com