Desarrollo de herramienta honeypot de implantación y uso ágil

Aplicación a la detección y análisis de amenazas en la red de la U.G.R

Juan Luis Martin Acal

Antecedentes

2010 Centro de Servicios Informáticos y Redes de Comunicaciones **(C.S.I.R.C)**

Se inicia el desarrollo del nuevo sistema de gestión de incidencias del Área de Seguridad Informática.

Inicialmente existían **3 vías** de comunicación de incidencias:

1. Correo desde **[IRIS-CERT].**
2. Correo desde **[C.I.C.A].**

   En la práctica solo es un reenvío de las incidencias procedentes que registraba el equipo C.E.R.T de Red Iris.

3. Detección mediante **un único sensor**, de tipo **honeypot**, vigilando **una única subred**.

Antecedentes

- El sensor **consistía en:**
  - Un equipo físico
    - Típica **torre de escritorio.**
    - Uso especifico.
      - **Enteramente dedicado a la labor de detección.**
    - Hardware **obsoleto.**
      - Aunque funcionalmente se no requería más.
  - Sistema operativo **Linux Debian (versión obsoleta).**

    Software:
    - **Nephentes (evolución abandonada en 2009).**
    - Scripts de envío **de notificaciones mediante** sendmail al correo de seguridad.

Problemática

- **Implantación**
  - **Ineficiente en escabilidad y recursos, multiplicaban por cada sensor.**
    - **Espacio** en la sala servidores.
    - **Tomas a la red.**
    - **Consumo eléctrico.**
    - **Consumo de recursos hardware**.
  - Ante **fallo crítico del hardware** la única solución “rápida” era **pasar el disco duro a otra máquina.**
  - Ante **fallo crítico del software**, había que **reconstruir el sensor:**
    - Instalación del sistema y configuración del mismo.
    - Instalación de todo el software.
    - Comprobaciones de funcionamiento correcto.
- **Esto suponía varios días de respuesta ante cualquier adversidad surgida.**

Problemática

- **Funcionalidad.**
  - **Comunicación** de las incidencias era **ineficiente.**
    - **Sobrecarga del correo del Área de Seguridad**. Mientras se prologase la amenaza en el tiempo se enviaban correos.
    - La **consulta en detalle** de la incidencia y no solo que ip y fecha, requería una consulta **tediosa** de **logs muy fragmentados o inmensos.**
    - Nephentes **no soporta** por si mismo **base de datos.**
      - **Almacenamiento local en texto plano.**
      - **No había comunicación con la base de datos Oracle que da almacenamiento al que seria el nuevo sistema de gestión.**
  - **El "mantenimiento" (rm –f /losLogs) era manual.**

Problemática

- **Análisis de la información**.
  - **Analizar información** en esas condiciones era una **pesadilla.**
  - **Imposible** hacer **estadísticas ni análisis de incidentes** que no fueran relativamente **recientes.**
    - **No era apto para** la extracción de datos relativos **a calidad del área**.
- No había capacidad de **“pillar en caliente”** la ocurrencia de un incidente.
  - **La información que se extrae durante desarrollo** del incidente, **es la piedra rosetta**.
    - **Adquirimos no solo detección, también conocimiento de la amenaza. SIN ESTO NO HAY CERT REAL.**
    - El **potencial y el alcance del riesgo** se ven **minimizados** drásticamente.

Justificación

Este trabajo a dado **solución a la anterior problemática** y a **suministrado información de las amenazas presentes en la red de la U.G.R para mejora en la calidad de respuesta del C.S.I.R.C**, además de ampliar los conocimientos dentro del propio área de seguridad en dicha materia.

Características de la herramienta honeypot

Virtualización:

- Eficiente en el uso de recursos.
- Sustitución y migración en minutos.

Comunicación:

- El almacenamiento local de la información es en base de datos SQLite **(se implemento para kippo)**.
- Cada 24 horas se centraliza toda la información en la base de datos Oracle del C.S.I.R.C.
  - Se filtra información esencial.
  - Se geolocaliza la ip del atacante.
- Monitorización de lo que esta detectando el honeypot.

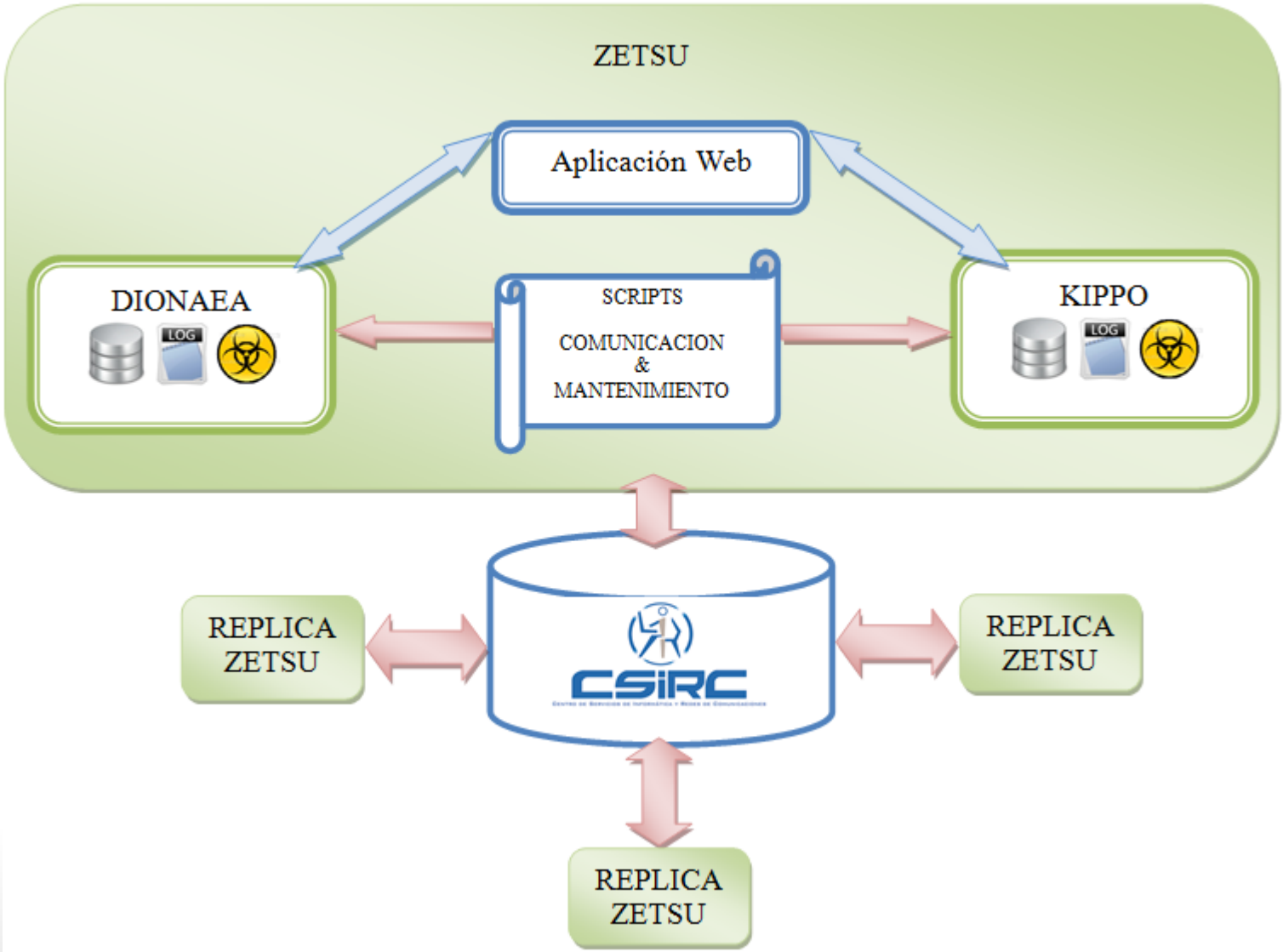
Mantenimiento

- No se requiere almacenamiento permanente de logs.
- Cada semana el malware recopilado es eliminado o migrado.
- Inicialmente es borrado de la zona de aislamiento pero es fácil migrarlo a una “sandbox” para análisis forense.

Esquemático

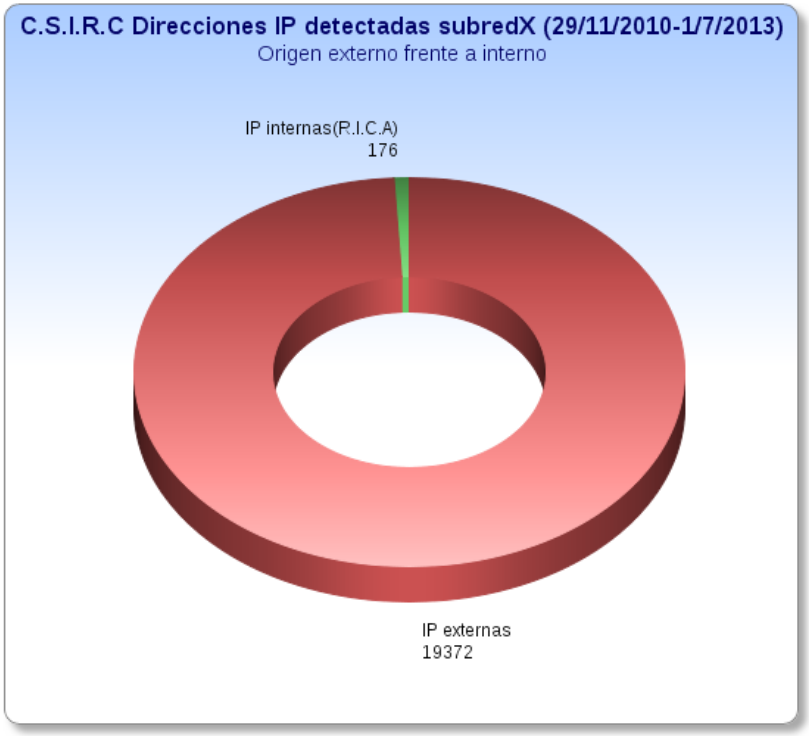
Acción programada

Interacción humana



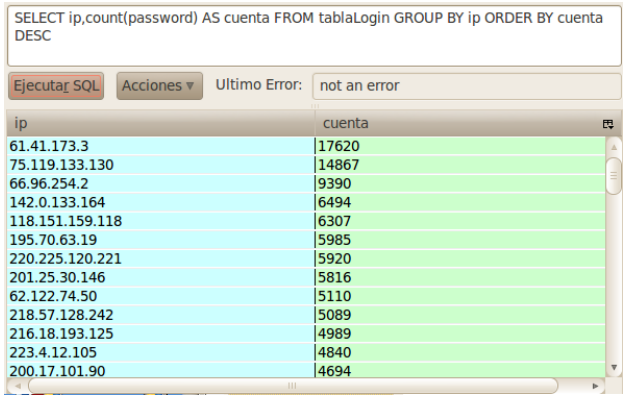
Análisis de la información

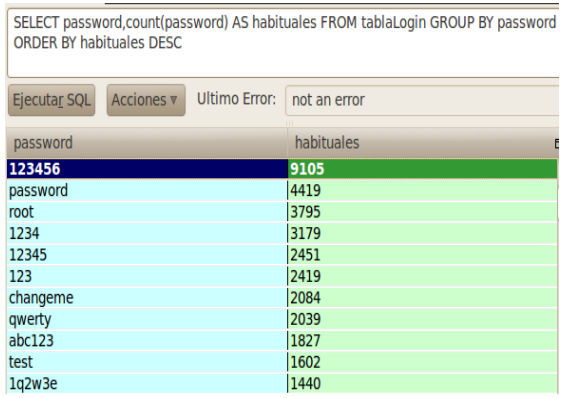
Procedencia de las amenazas

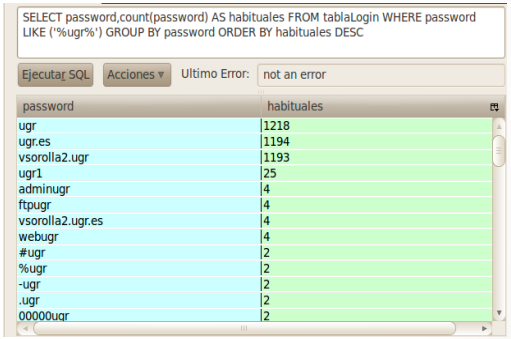


Análisis de la información

Naturaleza de las amenazas





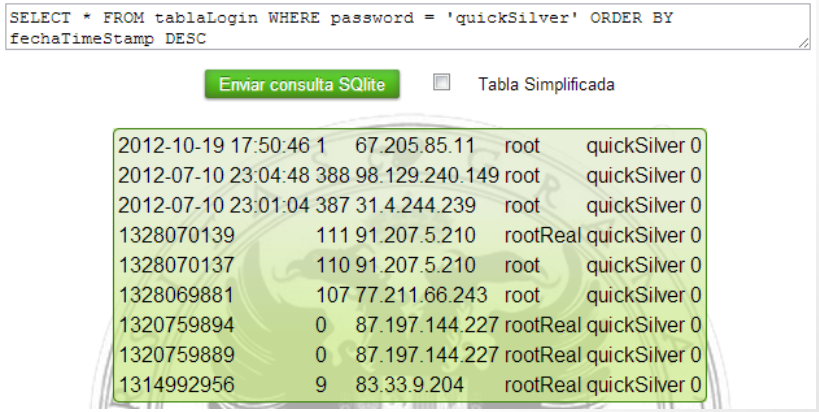


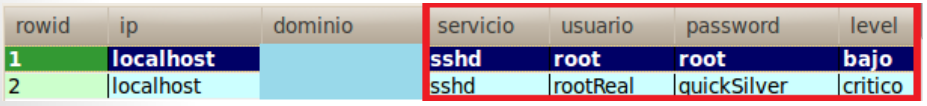
Es fundamental distinguir entre:

-Escaneo y búsqueda de vulnerabilidades

-Intrusión básica.

-Intrusión “avanzada” (Superar retos).





PAISES CON MAS DE 1000 ATAQUES - TOP 35 – 29/11/2010 14/7/2013	
CHINA	354.356
ESPAÑA (FALSO, NO ESTAN FILTRADAS PRUEBAS INTERNAS)	115.906
ESTADOS UNIDOS DE AMÉRICA	33.604
ALEMANIA	12.421
REPÚBLICA DE COREA	7.063
CANADÁ	5.688
ARGENTINA	4.813
FEDERACIÓN DE RUSIA	4.532
- NO REGISTRADO	4.437
KOREA, REPUBLIC OF	3.614
BRASIL	3.536
TAIWAN	3.314
INDIA	3.284
FRANCIA	2.850
TURQUÍA	2.780
REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE	2.433
TAILANDIA	2.368
GRECIA	2.155
JAPÓN	2.155
INDONESIA	1.944
PAÍSES BAJOS	1.944
PALESTINIAN TERRITORY	1.914
UCRANIA	1.910
RUSSIAN FEDERATION	1.843
NIGERIA	1.829
POLONIA	1.747
COLOMBIA	1.715
JAPAN	1.566
BRAZIL	1.317
VIET NAM	1.298
ITALY	1.248
FRANCE	1.171
GERMANY	1.140
HONG KONG	1.077
TURKEY	1.019

-El número de ataques externos es elevadísimo.
-Su análisis engañoso.
-Se ha de conocer la naturaleza del ataque y del atacante.

OBTENEMOS ASÍ CONOCIMIENTO Y NO SOLO ESTADISTICOS

```
SELECT * FROM tablaLogin WHERE fechaTimeStamp BETWEEN '1368836685.0' AND
'1369009485.0' and resultado = '1' ORDER BY fechaTimeStamp DESC
```

Enviar consulta SQlite Tabla Simplificada

```
2013-05-19 15:59:28 267 85.214.246.127   root p@ssw0rd 1
2013-05-19 15:31:12 191 175.195.182.182 root p@ssw0rd 1
2013-05-19 02:24:45 32   95.77.175.43      root p@ssw0rd 1
2013-05-19 02:22:08 31   218.89.136.139   root p@ssw0rd 1
2013-05-18 05:22:49 927 95.76.102.230    root p@ssw0rd 1
2013-05-18 02:27:31 734 94.102.3.151     root p@ssw0rd 1
```

- IP address : **95.77.175.43**
- Country : RO
- State/Province : BUCURESTI
- City : BUCHAREST

EL INTRUSO

- IP address : **85.214.246.127**
- Country : DE
- State/Province : BERLIN
- City : BERLIN

ACERTO a la primera
NO toco nada

- IP address : **175.195.182.182**
- Country : KR
- State/Province : SEOUL-TUKPYOLSI
- City : SEOUL

SOLO PASO DICCIONARIO

- IP address : **218.89.136.139**
- Country : CN
- State/Province : SICHUAN
- City : CHENGDU

SOLO PASO DICCIONARIO

- IP address : **218.89.136.139**
- Country : CN
- State/Province : SICHUAN
- City : CHENGDU

SOLO PASO DICCIONARIO

- IP address : **95.76.102.230**
- Country : RO
- State/Province : BUCURESTI
- City : BUCHAREST

ACERTO a la primera
Segunda visita en tres meses

- IP address : **94.102.3.151**
- Country : TR
- State/Province : SINOP
- City : SINOP

SOLO PASO DICCIONARIO

Análisis de la información

Procedencia Interna

SHA256: 41bdde2c2c47f5db00656199587d24fda4e3935704921e6639161db22ca19757

Nombre: 446f2511da70b11490a0e8814a6baeef

Detecciones: 38 / 42

Fecha de análisis: 2012-04-26 16:56:54 UTC (hace 1 año, 2 meses)

Antivirus	Resultado	Actualización
AhnLab-V3	Trojan/Win32.Buzus	20120423
AntiVir	TR/Agent.kdv.37949	20120424
Antiy-AVL	Trojan/Win32.Menti.gen	20120424
Avast	Win32:Kolab-MX [Trj]	20120423
AVG	Worm/Pakes.AFE	20120423
BitDefender	Trojan.Generic.KDV.376981	20120424

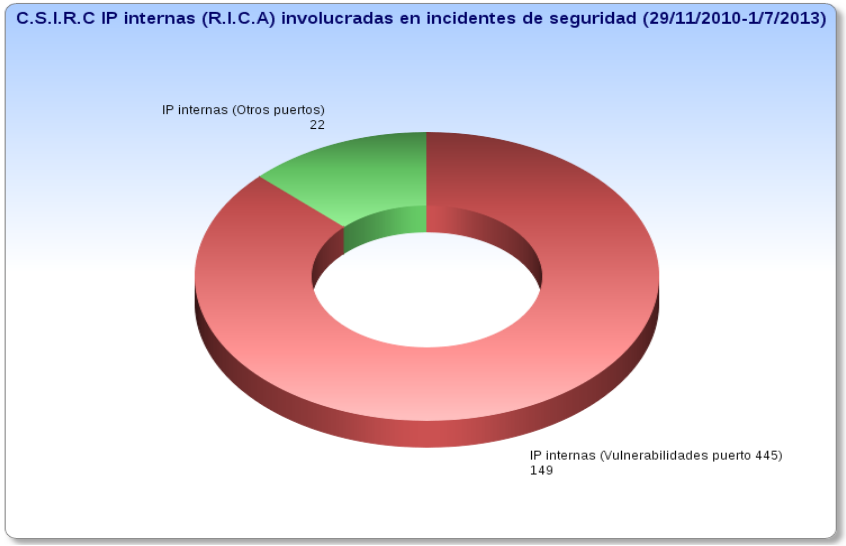
SHA256: 0c3e7029fd2208410f0d8e10ffefdc10494bb78b440e0275cd001428fc5b2815

Nombre: adbe735664247021d3d2d515da10b1a4

Detecciones: 36 / 42

Fecha de análisis: 2012-04-28 13:01:49 UTC (hace 1 año, 2 meses)

Antivirus	Resultado	Actualización
AhnLab-V3	Trojan/Win32.Scar	20120428
AntiVir	TR/Dropper.Gen	20120428
Antiy-AVL	Trojan/Win32.Scar.gen	20120428
Avast	Win32:Downloader-KUV [Trj]	20120428
AVG	Generic25.ACEP	20120428
BitDefender	Trojan.Generic.KDV.380634	20120428




```
SELECT * FROM dcerpcserviceops WHERE dcerpcserviceop = '22' ORDER BY
dcerpcserviceop DESC
```

Enviar consulta

22 22 31 NetPathCanonicalize MS08-67

```
SELECT * FROM downloads WHERE connection = '122568' OR connection = '122411'
ORDER BY download DESC
```

Enviar consulta

6357 122568 http://146.185.246.117/t.exe adbe735664247021d3d2d515da10b1a4
6344 122411 http://146.185.246.117/ii.exe 446f2511da70b11490a0e8814a6baeef

Conclusiones

NOTA: En fecha de redacción de este trabajo y durante el tiempo de elaboración del mismo casi la totalidad de dichas medidas han sido o están implantándose de manera exitosa.

- **Administración**

  -Una política cuidadosa de elección de las credenciales.

  -Correcta configuración de seguridad en sistemas operativos y la aplicación de reglas de cortafuegos (Áreas de Sistemas de Investigación y Área de Sistemas de Gestión).

  -Actualización y parcheado periódico de las imágenes que son cargadas en la red administrativa (Área de Micro Informática) y de aulas (Área de Aulas).

- **Redes**

  -Aislamiento mediante VPN o subredes privadas de los servicios en producción que sean de uso privado del servicio de informática.

  -Capado del acceso desde redes públicas, como son la VPN y la red inalámbrica, a subredes que no abastezcan de servicios públicos.

  -Proveer de mecanismos técnicos que permitan la utilización eficiente de las técnicas de seguridad activa, como es el registro y consulta eficiente de los históricos de conexión.

- **Seguridad**

  -Gestión automatizada del registro y tratamiento de incidencias de seguridad tanto de origen interno como externo. Siempre con soporte humano para la toma final decisiones.

  -Auditorias periódicas de seguridad mediante test de penetración.

  - No basta con detectar la amenaza, hay que adelantarse y documentar para la corrección por parte de las áreas implicadas de dicha amenaza.

  -Ampliación del conocimiento del área hacia campos como el análisis de malware (Byte Forensic).

  - Con la detección de la amenaza la eficacia es solo parcial. Es necesario el estudio profesional de la misma para la evaluación real de su alcance.

Muchas gracias por su atención