GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Dossier de apoyo a profesores

Espacios de Ciberseguridad

Jornadas de Profesores

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Jornadas de ciberseguridad 6

1.1. Acerca de INCIBE 6
1.2. Características de las Jornadas 6
1.3. Descripción de las temáticas 7

2. índice de materiales 9

2.1. Presentaciones de los talleres 9
2.2. Herramientas 11

3. Máquinas virtuales 23

3.1. Utilización de máquinas virtuales 23

3.1.1. Máquinas virtuales de los alumnos 23

3.1.2. Máquinas virtuales del formador 23

3.2. Instalación de software de virtualización 24
3.3. Creación de una máquina virtual 25
3.4. Importación de máquinas virtuales 27

3.4.1. Importación de máquinas virtuales vulnerables 28

3.5. Configuración de red de las máquinas virtuales 29

4. configuración del entorno 31

4.1. Requisitos de la red 31

5. configuración de los entornos de pruebas 32

5.1. Mi ordenador es un zombi 32

5.1.1. Configuración de red 32

5.1.2. Máquinas virtuales necesarias 33

5.2. Programación segura de sitios Web 33

5.2.1. Configuración de red 33

5.2.2. Máquinas virtuales necesarias 34

5.3. Fundamentos del análisis de sitios Web 34

5.3.1. Configuración de red 34

5.3.2. Máquinas virtuales necesarias 35

5.4. Fundamentos del análisis de sistemas 35

5.4.1. Configuración de red 35

5.4.2. Máquinas virtuales necesarias 36

5.5. Análisis de malware en Android 36

5.5.1. Configuración de red 36

5.5.2. Máquinas virtuales necesarias 37

5.6. Seguridad Wifi 37

5.6.1. Configuración de red 37

5.6.2. Máquinas virtuales necesarias 38

5.7. Espionaje y Cibervigilancia 38

5.7.1. Configuración de red 38

5.7.2. Máquinas virtuales necesarias 39
5.8. Forense en Windows 39
5.8.1. Configuración de red 39
5.8.2. Máquinas virtuales necesarias 39
6. principales problemas 40
6.1. Resolución de problemas de virtualización 40
6.2. Resolución de problemas de la red 41
6.3. Potenciales problemas con los entornos 41

ÍNDICE DE FIGURAS

Figura 1. Suite aircrack-ng 11
Figura 2. Emulador en Android Studio 12
Figura 3. Edición de clases en Android Studio 12
Figura 4. Herramienta APK Tools 12
Figura 5. Diferentes opciones de APK Tools 13
Figura 6. Beef 13
Figura 7. Burp suite 14
Figura 8. Aplicación DVWA 15
Figura 9. Herramienta FOCA 15
Figura 10. Malware educativo Flu 16
Figura 11. Herramienta GeoSetter 16
Figura 12. Java decompiler 17
Figura 13. Escáner NMap 17
Figura 14. Escáner OpenVas 18
Figura 15. Process Explorer 18
Figura 16. Process Monitor 19
Figura 17. Herramienta Recuva 19
Figura 18. Herramienta SilentEye 20
Figura 19. Suite Sysinternals 20
Figura 20. Navegador Tor Browser 21
Figura 21. Capturador de tráfico Wireshark 22
Figura 22. Página principal de VirtualBox 24
Figura 23. Descarga de VirtualBox 24
Figura 24. Creación de nueva máquina virtual 25
Figura 25. Configuración de sistema operativo 25
Figura 26. Asignación de memoria RAM 26
Figura 27. Configuración de disco duro virtual 26
Figura 28. Importar máquina virtual 27
Figura 29. Selección de máquina virtual a importar 27
Figura 30. Confirmación de la importación 28
Figura 31. Pantalla durante la importación 28
Figura 32. Máquina virtual Metasploitable2 29
Figura 33. Acceso a configuración de la máquina virtual 29
Figura 34. Acceso a la configuración de red 30
Figura 35. Configuración de la red en modo puente 30
Figura 36. Entorno del taller Mi ordenador es un zombi 32
Figura 37. Entorno del taller Programación segura de sitios Web 33
Figura 38. Entorno del taller Fundamentos del análisis de sitios Web 34
Figura 39. Entorno del taller Fundamentos del análisis de sistemas 36

Figura 40. Entorno del taller Análisis de malware en Android 37
Figura 41. Entorno del taller Seguridad Wifi 38
Figura 42. Entorno del taller Espionaje y cibervigilancia 38
Figura 43. Error con compatibilidad USB 40
Figura 44. Error con drivers vboxdrv 40

1. JORNADAS DE CIBERSEGURIDAD

La creciente evolución de Internet y de las tecnologías de la información ha causado un aumento de los riesgos asociados al uso de la tecnología. Esto queda patente en que cada vez son más comunes los casos de fugas de información sensible, de intrusiones en sistemas internos de empresas o de robos de datos de particulares debido a sistemas o servicios de tratamiento de información inseguros.

Dicha evolución ha hecho que las empresas aumenten su conciencia sobre el riesgo al que están expuestos sus sistemas de información, por lo que cada vez es más común la realización de revisiones de seguridad y auditorías por parte de hackers éticos y expertos en seguridad. Estos expertos tienen como objetivo comprobar la seguridad de los sistemas, servicios y aplicaciones desde el punto de vista de un atacante. Es por ello que deben conocer las principales técnicas de seguridad existentes, así como formarse continuamente sobre nuevas estrategias de explotación de sistemas y vulnerabilidades.

Debido al marco anterior y a la rápida evolución de la tecnología, cada vez existe una mayor demanda de profesionales con conocimientos en ciberseguridad actualizados, por lo que los programas de formación son fundamentales para tal fin.

1.1. Acerca de INCIBE

El Instituto Nacional de Ciberseguridad de España, INCIBE, es una sociedad dependiente del Ministerio de Industria, Energía y Turismo, MINETUR, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, SETSI. INCIBE es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española, RedIRIS, y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, desde INCIBE se lideran diferentes actuaciones para la ciberseguridad a nivel nacional e internacional; basando su actividad en la investigación, la presentación de servicios y la coordinación con los agentes que tengan competencias en la materia.

1.2. Características de las Jornadas

Las Jornadas “Espacios de Ciberseguridad” nacen como una herramienta de captación y generación de talento en ciberseguridad, orientadas a estudiantes de enseñanzas medias, con el fin de satisfacer dicha demanda desde la base.

Este programa de formación, promovido por INCIBE, tiene las siguientes características principales:

- **Temáticas:** ocho talleres independientes entre sí, de manera que sea posible impartir cualquier temática sin requisitos de impartición previos.
- **Enfoque:** con un alto componente práctico y con el apoyo teórico suficiente para entender los diferentes ejercicios propuestos.

- **Duración:** aproximadamente tres horas, pero variable en función de los conocimientos previos de los alumnos.
- **Público objetivo:** estudiantes de enseñanzas medias (bachillerato y formación profesional) con conocimientos de informática a nivel usuario.
- **Asistentes:** dimensionado para grupos reducidos de no más de 30 alumnos idealmente.
- **Entorno:** simulación de un entorno de pruebas real pero controlado, en el cual los alumnos son capaces de poner en práctica técnicas de seguridad sin riesgo.
- **Evaluación:** las temáticas están diseñadas de manera que permitan evaluar a los alumnos con ejercicios destinados para tal fin.
- **Dinámica:** el diseño de los talleres intercala partes teóricas con ejercicios prácticos, de manera que los alumnos no pierdan la atención durante el taller.
- **Aplicabilidad:** las diferentes temáticas tratan aspectos relativos a diferentes nichos profesionales dentro del sector de la ciberseguridad.

1.3. Descripción de las temáticas

- **Mi ordenador es un zombi**

Se abordarán diferentes conceptos relacionados con el malware y las redes botnets. Entre otros temas, se estudiarán los diferentes tipos de malware, el ciclo de vida de una botnet (infección y creación), medidas de evasión de sistemas antivirus, técnicas de anonimato del botmaster y medidas de protección ante este tipo de ataques.

- **Programación segura de sitios Web**

Se identificarán los principales elementos a tener en cuenta para desarrollar aplicaciones web seguras, así como la importancia de implementar medidas y controles de seguridad desde la fase de diseño. En este sentido, se analizarán los principales vectores de ataque y cómo mitigar su riesgo, tanto a nivel de desarrollo de código como de configuración de servidores.

- **Fundamentos del análisis de sitios Web**

Se analizarán los aspectos de seguridad, vectores de ataque y técnicas de intrusión básicas a nivel de aplicación. Para ello, se toma como referencia el top 10 de vulnerabilidades OWASP, viendo a nivel teórico los vectores de ataque más comunes y realizando ejemplos prácticos de explotación de dichas vulnerabilidades.

- **Fundamentos del análisis de sistemas**

Se detallarán las diferentes técnicas de análisis de las redes de ordenadores y de las infraestructuras que soportan las aplicaciones web. Concretamente, los alumnos aprenderán a identificar, analizar y explotar las principales vulnerabilidades de los servicios soportados por un servidor, así como los protocolos principales que suelen utilizar.

- **Análisis de malware en Android**

Se estudiarán las técnicas y estrategias fundamentales en el análisis de malware en dispositivos Android, entrando en detalle teórico y práctico sobre las principales técnicas de análisis estático y dinámico de aplicaciones, así como las herramientas utilizadas para tal fin y diferentes técnicas de protección ante este tipo de ataques.

- **Seguridad Wifi**

En esta temática se identificarán los fundamentos de las comunicaciones inalámbricas, así como la seguridad de las diferentes configuraciones y dispositivos característicos de redes Wi-Fi. Por otro lado, se estudiará la fortaleza de los diferentes cifrados que emplean los estándares, y recomendaciones para incrementar la seguridad al usar este tipo de redes.

- **Espionaje y cibervigilancia**

Se estudiarán las técnicas de recolección de información pública mediante el uso de fuentes abiertas en Internet y la importancia de controlar nuestros datos Para ello se analizarán los diferentes motores de búsqueda generalistas o específicos y otras herramientas que pueden ser utilizadas para tal fin, focalizando en el riesgo de pérdida de privacidad en la red.

- **Forense en Windows**

Se analizarán las principales técnicas de análisis forense en sistemas Windows, así como las técnicas de análisis de datos tanto volátiles como no volátiles. El temario se focaliza en el análisis forense como fase del ciclo de respuesta ante incidentes, detallando los diferentes procedimientos de recolección de evidencias y custodia de las mismas.

2. ÍNDICE DE MATERIALES

2.1. Presentaciones de los talleres

Para la impartición de las Jornadas se ofrecen una serie de presentaciones que el profesor podrá emplear libremente, cada una de ellas tiene las siguientes secciones:

- **Apartado introductorio común a todas las temáticas:** Es preciso destacar que todas las presentaciones comienzan con un contenido común compuesto por los siguientes apartados:
  - **Introducción a INCIBE**: con una breve introducción de qué es INCIBE, sus principales líneas de actuación y detalle de las actividades realizadas en el área de "I+D+i y Promoción del Talento" donde se engloba esta iniciativa.
  - **Introducción a la ciberseguridad**: se trata de forma global temas como la evolución de las Tecnologías de la Información, casos notorios de fallos de seguridad, riesgos para los Sistemas de información, diferentes tipos de hackers que existen y principales mecanismos de defensa.
- **Presentación "Mi ordenador es un zombi":**
  - Objetivos del curso
  - Malware
  - Botnets
  - Práctica: Construyendo una botnet
    - Creación
    - Infección
    - Explotación
    - Detección y desinfección
  - Contramedidas
- **Presentación "Programación segura de sitios Web":**
  - Objetivos del curso
  - Contexto
  - Introducción a la seguridad Web
  - Principios de la seguridad
  - Mitigación de vulnerabilidades en aplicaciones web
  - Mitigación de vulnerabilidades en servidores
  - Práctica: Aplicación web vulnerable
- **Presentación "Fundamentos del análisis de sitios Web":**
  - Objetivos del curso
  - Introducción
  - Fundamentos de comunicaciones
  - Análisis de vulnerabilidades
  - Explotación de vulnerabilidades
  - Seguridad en aplicaciones web
  - Práctica: Aplicación web vulnerable

- **Presentación "Fundamentos del análisis de sistemas":**
  - Objetivos del curso
  - Contexto
  - Introducción a redes y sistemas
  - Análisis de puertos
  - Análisis de vulnerabilidades
  - Explotación de vulnerabilidades
  - Post-explotación de vulnerabilidades
  - Práctica: Explotando un sistema

- **Presentación "Análisis de malware en Android":**
  - Objetivos del curso
  - Introducción
  - Aplicaciones
  - Seguridad en Android
  - Malware
  - Vulnerabilidades
  - Contramedidas
  - Práctica: Analizando un malware

- **Presentación "Seguridad Wifi":**
  - Objetivos del curso
  - Contexto
  - Introducción a las redes inalámbricas
  - Cifrado de las comunicaciones y control de acceso.
  - Ataques a redes Wi-Fi
  - Seguridad en clientes Wi-Fi
  - Práctica: Seguridad en cifrado WEP

- **Presentación "Espionaje y cibervigilancia":**
  - Objetivos del curso
  - Contexto
  - Introducción al espionaje y Cibervigilancia
  - Métodos de obtención de información
  - Deep web
  - Evasión de restricciones online
  - Actividades prácticas

- **Presentación "Forense en Windows":**
  - Objetivos del curso
  - Contexto
  - Introducción al análisis forense
  - Tratamiento de la evidencia
  - Conceptos básicos
  - Análisis de datos volátiles en Windows
  - Análisis de datos no volátiles en Windows
  - Actividades prácticas

2.2. Herramientas

Para la realización de las prácticas de los talleres, se emplean las siguientes herramientas gratuitas y disponibles en la red; mostradas por orden alfabético:

- **AirCrack:** Aircrack-ng es una suite de software de seguridad inalámbrico que se utiliza en la temática de Seguridad WiFi. Consiste en un analizador de paquetes de red, un crackeador de redes WEP y WPA/WPA2-PSK y otro conjunto de herramientas de auditoría inalámbrica entre las que destacan:
  - Aircrack-ng (descifra la clave de los vectores de inicio).
  - Airodump-ng (escanea las redes y captura vectores de inicio).
  - Aireplay-ng (inyecta tráfico para elevar la captura de vectores de inicio).
  - Airmon-ng (establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores).

  - **Temáticas en las que se emplea**:
    - Seguridad Wifi.

  - **URL de descarga**: *Herramienta instalada por defecto en Kali Linux*

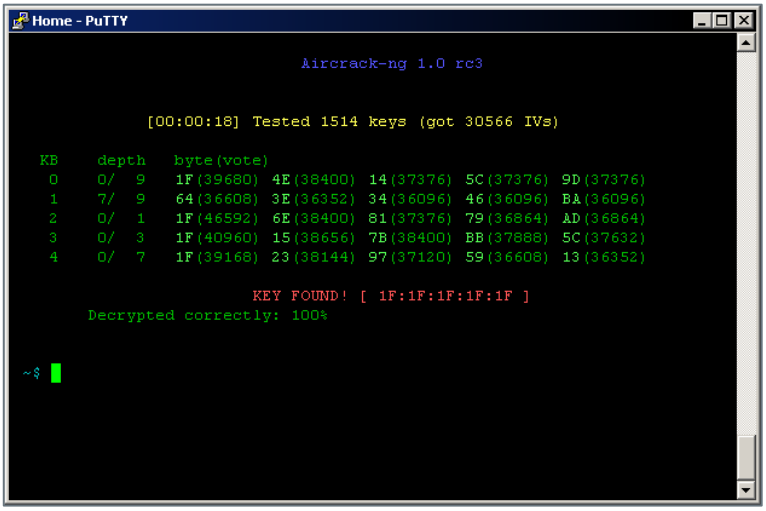

Figura 1. Suite aircrack-ng

- **Android Studio:** Es un entorno de desarrollo integrado para la plataforma Android. Reemplazó a Eclipse como el IDE oficial para el desarrollo de aplicaciones para Android.

  - **Temáticas en las que se emplea**:
    - Análisis de Malware en Android.

- **URL de descarga**: http://developer.android.com/sdk/index.html

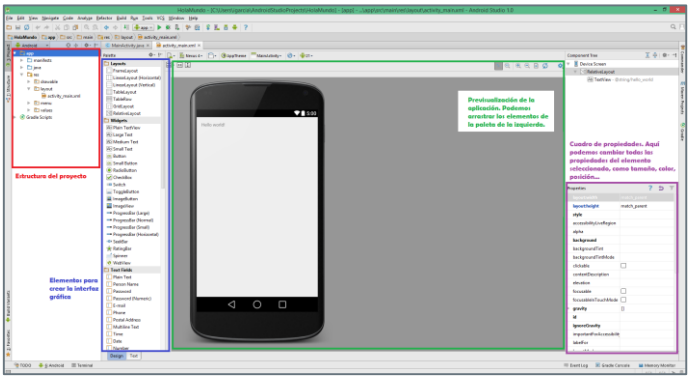

Figura 2. Emulador en Android Studio

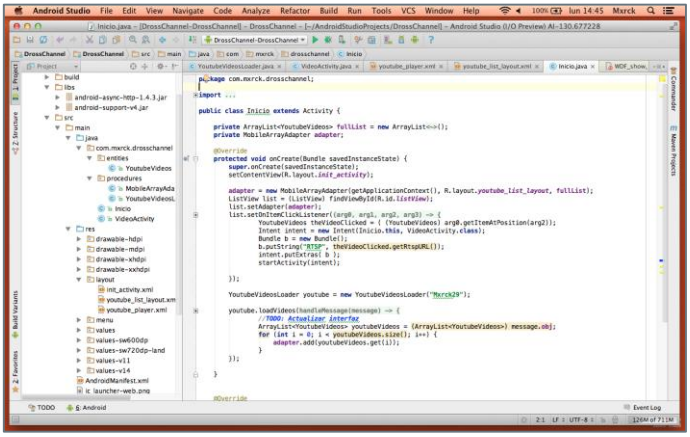

Figura 3. Edición de clases en Android Studio

- **Apktools:** Permite descomprimir apks, editarlos y volverlos a comprimir. También permite de una manera rápida desempaquetar un archivo apk, para poder editarlo directamente.

  - **Temáticas en las que se emplea**:

    - Análisis de Malware en Android.

  - **URL de descarga**: http://ibotpeaches.github.io/Apktool/

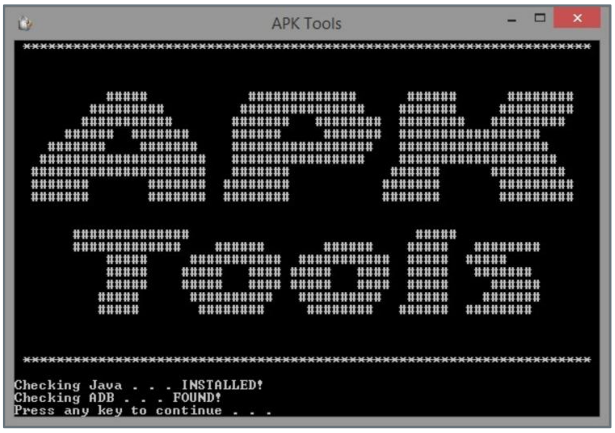

Figura 4. Herramienta APK Tools

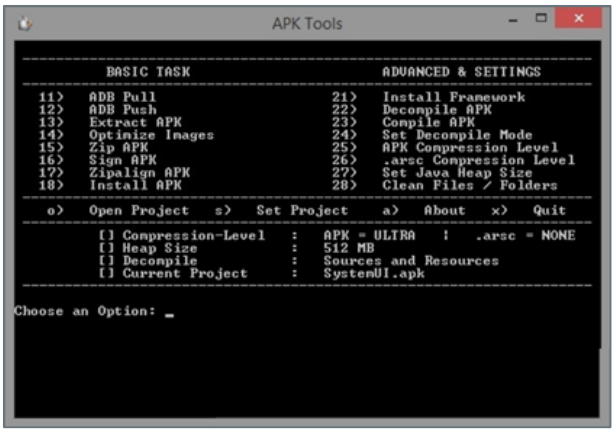

Figura 5. Diferentes opciones de APK Tools

- **Beef:** De las siglas en inglés *Browser Exploitation Framework*, Beef es una herramienta de pruebas de penetración que permite tomar el control de navegadores Web.

    - **Temáticas en las que se emplea:**
        - Mi ordenador es un zombie

    - **URL de descarga**: *Herramienta instalada por defecto en Kali Linux*

Figura 6. Beef

- **Burp:** Burp Suite es una herramienta para realizar el análisis de seguridad de aplicaciones Web.

    - **Temáticas en las que se emplea**:
        - Programación segura de sitios Web

- **URL de descarga**: *Herramienta instalada por defecto en Kali Linux*

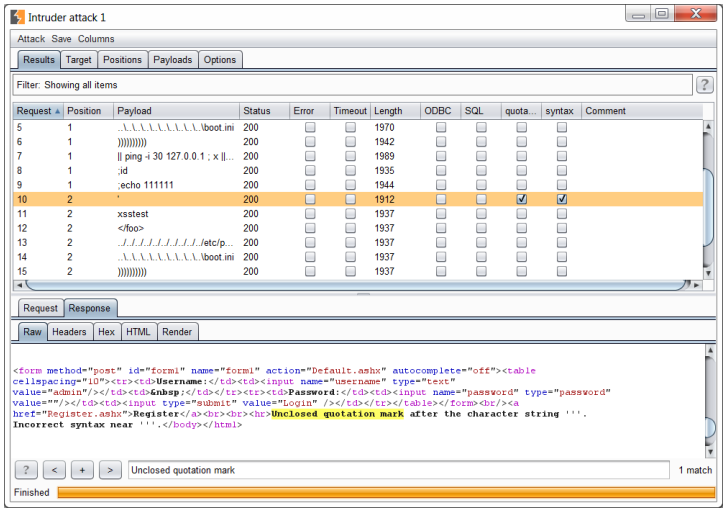

Figura 7. Burp suite

- **Dextojar:** Dex2jar es una herramienta que a partir de un archivo APK o el classes.dex, devuelve un archivo .jar que puede ser decompilado con herramientas como JD-GUI y acceder al código de la aplicación en Java.
  - **Temáticas en las que se emplea**:
    - Análisis de Malware en Android.
  - **URL de descarga**: https://github.com/pxb1988/dex2jar
- **Dumpzilla.py:** La aplicación dumpzilla está desarrollada en Python 3.x y tiene como finalidad extraer toda la información de interés forense de los navegadores Firefox, Iceweasel y Seamonkey para su posterior análisis. Dumpzilla mostrará el hash SHA256 de cada fichero utilizado para extraer la información y al final de la extracción, un resumen con los totales.
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
  - **URL de descarga**: http://www.dumpzilla.org/
- **DVWA:** Es una aplicación web PHP y MySQL para el entrenamiento de explotación de vulnerabilidades web en un entorno controlado y de manera legal. Dispone distintos niveles de dificultad y varios tipos de vulnerabilidades web a explotar. No viene instalada de forma predeterminada en el sistema operativo Kali Linux.
  - **Temáticas en las que se emplea**:
    - Programación segura de sitios Web.
    - Fundamentos del análisis de sitios Web

- **URL de descarga**: http://www.dvwa.co.uk/

Figura 8. Aplicación DVWA

- **Foca:** Es una herramienta para encontrar Metadatos e información oculta en documentos de Microsoft Office, Open Office y documentos PDF/PS/EPS. Permite extraer todos los datos de ellos exprimiendo los ficheros al máximo y una vez extraídos cruzar toda esta información para obtener datos relevantes de una organización.
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
    - Espionaje y Cibervigilancia
  - **URL de descarga**: https://www.elevenpaths.com/es/labstools/foca-2/index.html

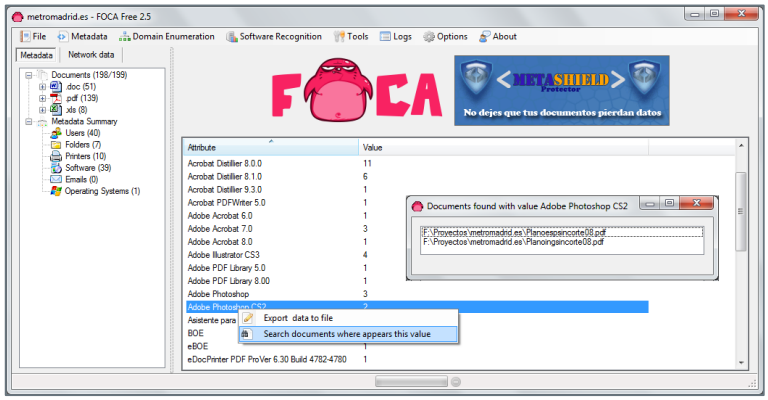

Figura 9. Herramienta FOCA

- **Flu:** El software Flu, desarrollado por Flu Project, es una herramienta abierta de tipo troyano que permite controlar máquinas de manera remota.
  - **Temáticas en las que se emplea**:
    - Mi ordenador es un Zombi.

- **URL de descarga**: http://code.google.com/p/flu-project/

Figura 10. Malware educativo Flu

- **GeoSetter:** GeoSetter es una herramienta de escritorio diseñada para geolocalizar fotos a través de los metadatos incrustados.
  - **Temáticas en las que se emplea**:
    - Espionaje y Cibervigilancia.
  - **URL de descarga**: http://www.geosetter.de/en/

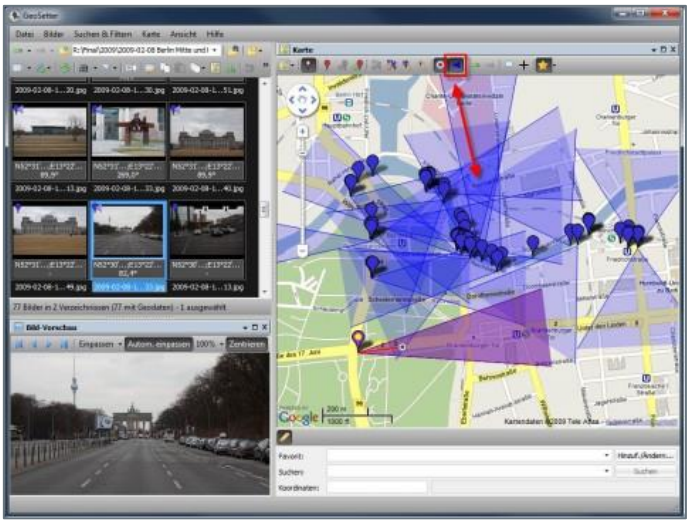

Figura 11. Herramienta GeoSetter

- **Java decompiler:** Decompilador y desensamblador para Java que reconstruye el código fuente original de los archivos CLASS binarios compilados.
  - **Temáticas en las que se emplea**:
    - Análisis de Malware en Android.

- **URL de descarga**: https://github.com/java-decompiler/jd-gui

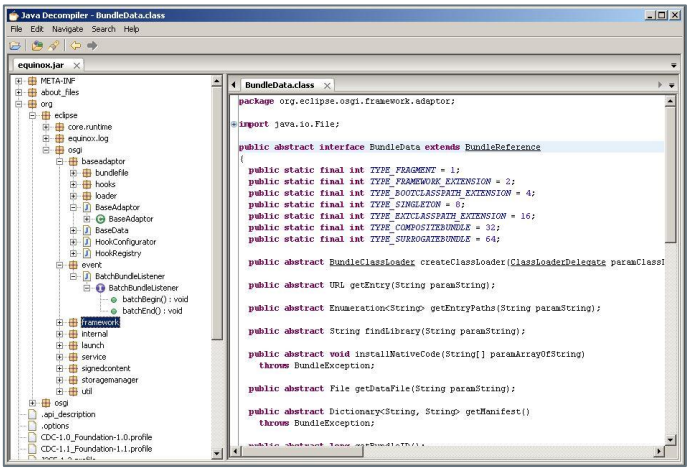

Figura 12. Java decompiler

- **MDD:** MDD también conocido como DD ManTech o DD Memoria, se encarga de generar una imagen forense de la memoria física del sistema y almacenarla como un fichero binario (raw).
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
  - **URL de descarga**: http://sourceforge.net/projects/mdd/

- **NMap:** Se trata de un escáner de puertos que permite analizar la exposición de un sistema, los servicios que posee abiertos y las versiones de los mismos. Posee diferentes tipos de escaneos avanzados para evasión de elementos de seguridad perimetral.
  - **Temáticas en las que se emplea**:
    - Fundamentos del análisis de sistemas
  - **URL de descarga**: *Herramienta instalada por defecto en Kali Linux*

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)
```

Figura 13. Escáner NMap

- **OpenVAS:** Es un escáner de vulnerabilidades que se emplea para detectar e identificar fallos de seguridad.

- **Temáticas en las que se emplea**:
  - Fundamentos del análisis de sistemas
  - Fundamentos del análisis de sitios Web
- **URL de descarga**: *Herramienta instalada por defecto en Kali Linux* (es necesario configurarla antes de utilizarla por primer vez)

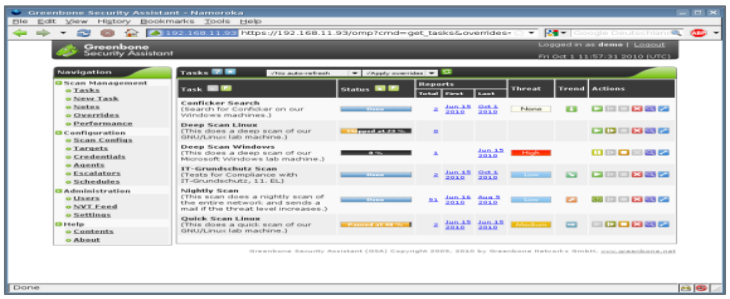

Figura 14. Escáner OpenVas

- **Process Explorer:** La herramienta Process Explorer de Sysinternals sirve para verificar cada proceso del sistema y aplicaciones que se ejecutan en el equipo. Es posible finalizar procesos, analizar dónde se almacenan los ejecutables de cada aplicación, que ruta del registro de Windows se genera, etc.
  - **Temáticas en las que se emplea**:
    - Mi ordenador es un Zombi.
  - **URL de descarga**: https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

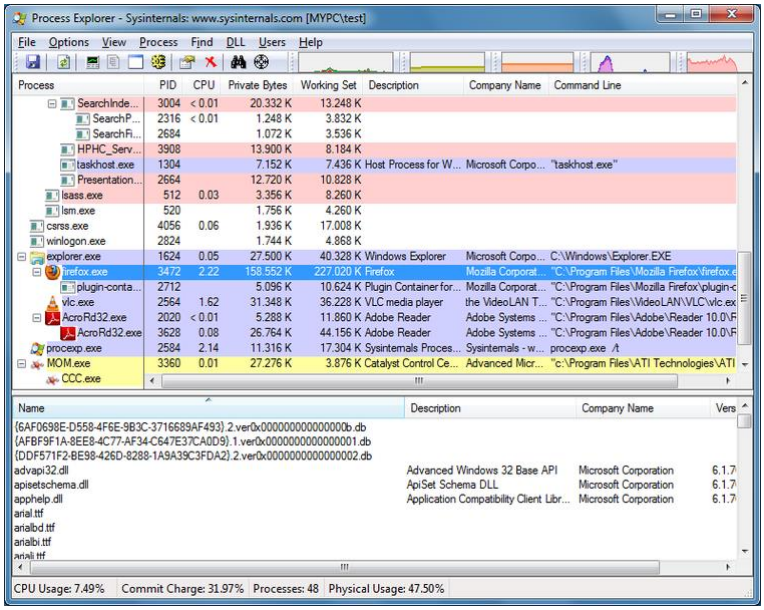

Figura 15. Process Explorer

- **Process Monitor:** Permite ver las acciones realizadas por un proceso. Este programa permite monitorizar cualquier tipo de actividad en el sistema: creación de ficheros temporales, operaciones de escritura o lectura en disco, etc.

- **Temáticas en las que se emplea**:
  - Mi ordenador es un Zombi.
- **URL de descarga**: https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

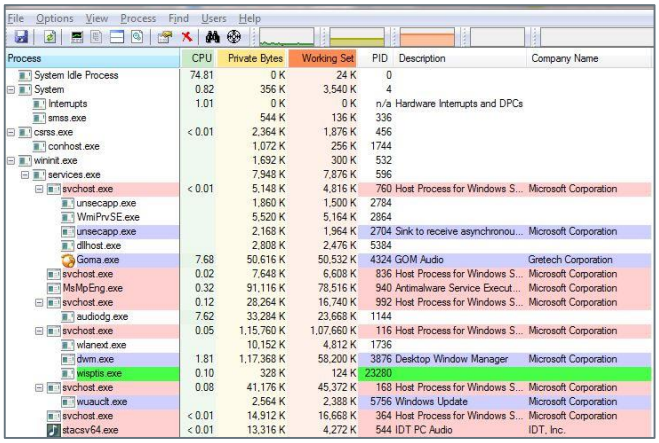

Figura 16. Process Monitor

- **Recuva:** Es un programa de recuperación de datos desarrollado por Piriform, para Microsoft Windows.
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
  - **URL de descarga**: https://www.piriform.com/recuva

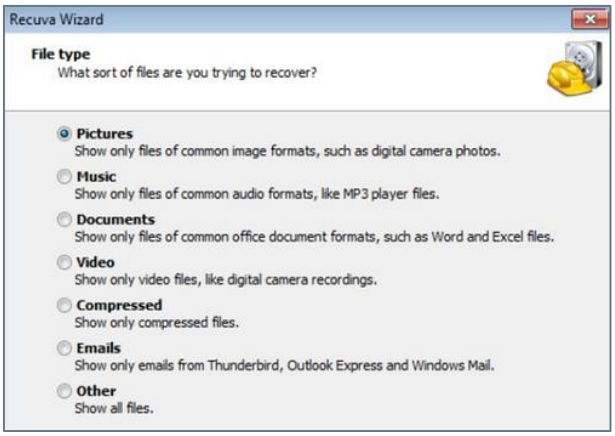

Figura 17. Herramienta Recuva

- **SilentEye:** Esta aplicación permite ocultar mensajes de texto y hasta archivos de cualquier formato dentro de imágenes BMP y JPEG.
  - **Temáticas en las que se emplea**:
    - Espionaje y Cibervigilancia

- **URL de descarga**: http://www.silenteye.org/

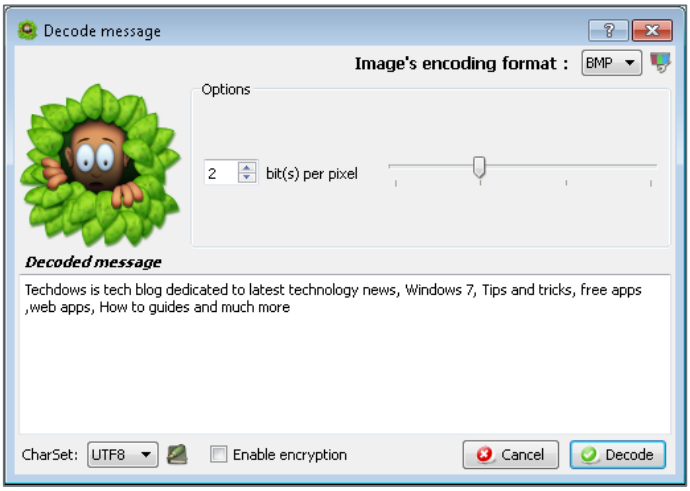

Figura 18. Herramienta SilentEye

- **Sysinternals:** Es una suite de herramientas que ofrece recursos técnicos y utilidades para gestionar, diagnosticar, solucionar problemas y supervisar un entorno de Microsoft Windows. Se utiliza en la temática de Análisis Forense en Windows.
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
  - **URL de descarga**: https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

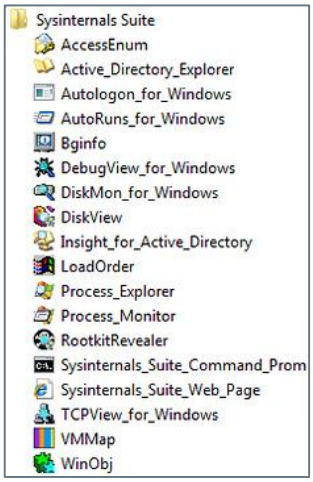

Figura 19. Suite Sysinternals

- **Tor:** El uso más habitual de Tor es aprovechar sus características para lograr cierto grado de privacidad en la navegación web en internet, además, mantiene la integridad y el secreto de la información que viaja por ella.
  - **Temáticas en las que se emplea**:
    - Espionaje y Cibervigilancia.

- **URL de descarga**: https://www.torproject.org/projects/torbrowser.html.en

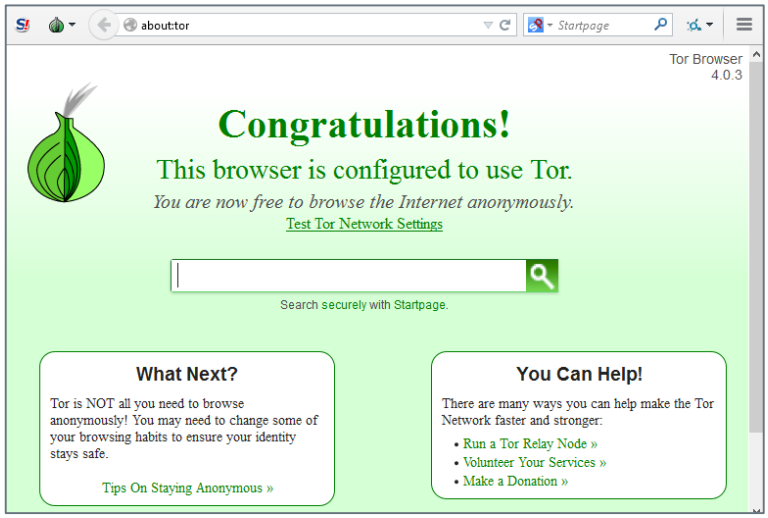

Figura 20. Navegador Tor Browser

- **Volatility:** Se usa para analizar la memoria RAM de Windows. Se puede extraer la tabla de conexiones, entradas ARP, ficheros abiertos, módulos cargados, procesos existentes, etc.
  - **Temáticas en las que se emplea**:
    - Forense en Windows.
  - **URL de descarga**: http://www.volatilityfoundation.org
- **Wamp:** Es una herramienta que permite levantar un servidor web local en la máquina del usuario.
  - **Temáticas en las que se emplea**:
    - Mi ordenador es un Zombi.
  - **URL de descarga**: http://www.wampserver.com/en/
- **Wireshark:** Herramienta que captura el tráfico enviado por una red y permite analizar el tráfico capturado empleando gran cantidad de analizadores de protocolo.
  - **Temáticas en las que se emplea:**
    - Fundamentos del análisis de sistemas

- **URL de descarga:** Herramienta instalada por defecto en Kali Linux

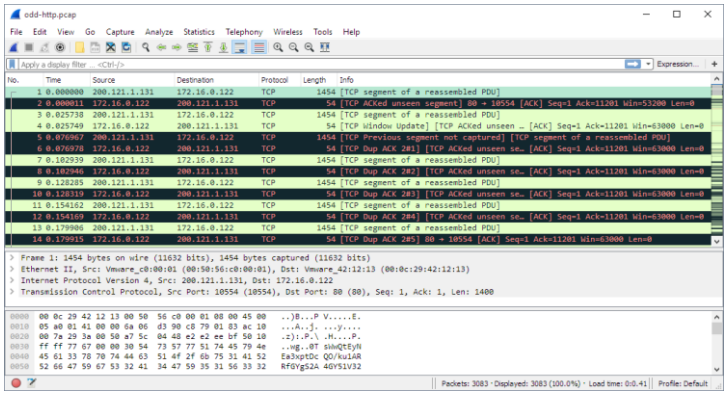

Figura 21. Capturador de tráfico Wireshark

3. MÁQUINAS VIRTUALES

3.1. Utilización de máquinas virtuales

La ejecución de los ejercicios prácticos se realizará en un entorno controlado; para ello se emplearán máquinas virtuales que deberá generar el profesor de forma previa a la impartición de la Jornada.

A continuación se detallan las máquinas virtuales necesarias junto con las temáticas en las que se emplea cada una de ellas:

3.1.1. Máquinas virtuales de los alumnos

Los alumnos deberán tener instaladas y debidamente configuradas las siguientes máquinas virtuales para el correcto desarrollo de las prácticas:

- **VM Kali:** Distribución basada en Debian y especialmente diseñada para la realización de auditorías de seguridad.
  - Temáticas en las que se utilizará:
    - Programación segura de sitios Web
    - Fundamentos del análisis de sitios Web
    - Fundamentos del análisis de sistemas
    - Seguridad Wifi
    - Forense en Windows
- **VM Windows 7:** Distribución de Windows 7 para propósito general y donde se deberán instalar las herramientas específicas para cada una de las temáticas.
  - Temáticas en las que se utilizará:
    - Forense en Windows
    - Espionaje y Cibervigilancia
    - Mi ordenador es un zombi
    - Análisis de Malware en Android

3.1.2. Máquinas virtuales del formador

Con el objetivo de que los alumnos dispongan de un entorno seguro donde realizar pruebas, en ciertas temáticas el formador pondrá a disposición de los alumnos plataformas para la realización de prácticas y ataques reales en un entorno controlado:

Las máquinas virtuales que el formador necesitará para la impartición de los talleres son:

- **VM Metasploitable2:** Distribución de un sistema basado en Linux con gran cantidad de servicios instalados, diseñado específicamente para pruebas de hacking y seguridad ya que contiene multitud de vulnerabilidades conocidas.
  - Temáticas en las que se utilizará:
    - Fundamentos del análisis de sistemas

- **VM Windows 7 – Botnet (botmaster):** Distribución de Windows 7 donde se deberá instalar el software para controlar una botnet.
  - Temáticas en las que se utilizará:
    - Mi ordenador es un zombi
- **VM Kali Linux**: Distribución basada en Debian y especialmente diseñada para la realización de auditorías de seguridad.
  - Temáticas en las que se utilizará:
    - Mi ordenador es un zombi
    - Programación segura de sitios Web
    - Fundamentos del análisis de sitios Web
    - Fundamentos del análisis de Sistemas
    - Seguridad Wifi
    - Forense en Windows

3.2. Instalación de software de virtualización

Durante el taller, se empleará el software de virtualización VirtualBox. Para su instalación, el primer paso es descargar el software (página oficial de descarga: www.virtualbox.org). Para ello pulsar el botón Download VirtualBox, remarcado en rojo en la siguiente imagen.

Figura 22. Página principal de VirtualBox

Descargar la versión necesaria para el equipo.

Figura 23. Descarga de VirtualBox

Una vez descargada instalarla como cualquier programa convencional (ejecutando el fichero .exe), teniendo en cuenta que durante el proceso de instalación pedirá permiso para instalar unos controladores de red para conectar las máquinas virtuales a Internet.

3.3. Creación de una máquina virtual

Cuando ya se ha completado la instalación del software de virtualización se debe proceder a crear la máquina virtual.

Para el taller, vamos a necesitar las máquinas virtuales de Kali Linux y de Windows 7.

Para crear una máquina virtual, hay que abrir el VirtualBox y hacer “click” en Nueva.

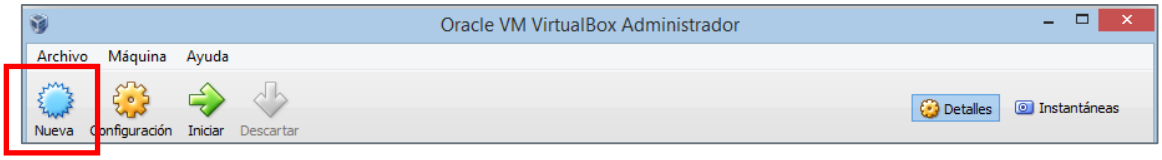

Figura 24. Creación de nueva máquina virtual

Al pulsar Nueva, aparece la siguiente pantalla, donde se puede elegir el Sistema Operativo

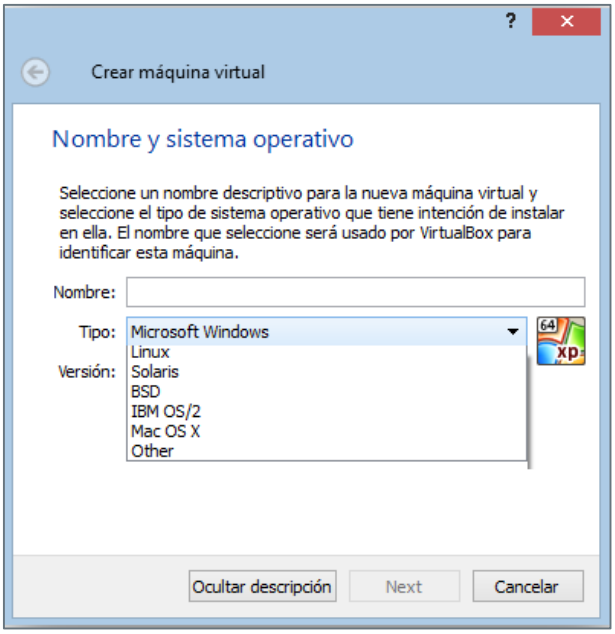

Figura 25. Configuración de sistema operativo

El siguiente paso es elegir el tamaño de memoria RAM que se asignará al sistema Operativo. Se recomienda asignar como **mínimo 1GB de memoria RAM a la máquina virtual** para que el sistema funcione sin problemas. Ese tamaño puede variar según la disponibilidad de recursos del sistema operativo base.

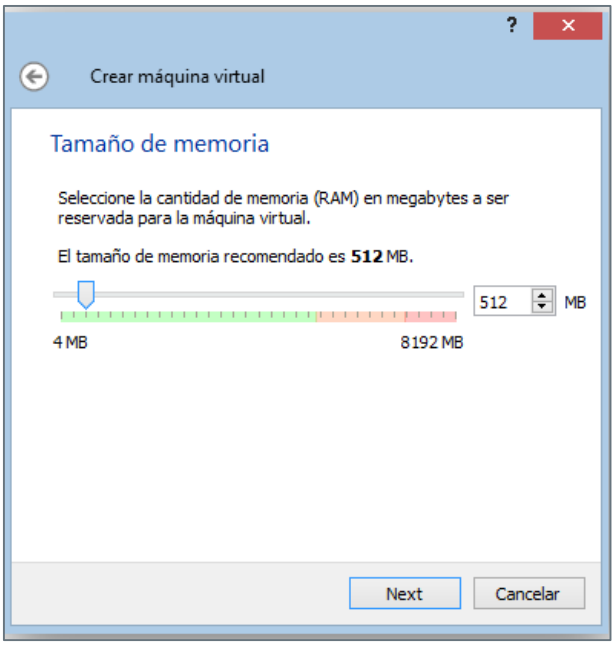

Figura 26. Asignación de memoria RAM

Posteriormente, seleccionar la opción “Crear un disco duro virtual ahora”.

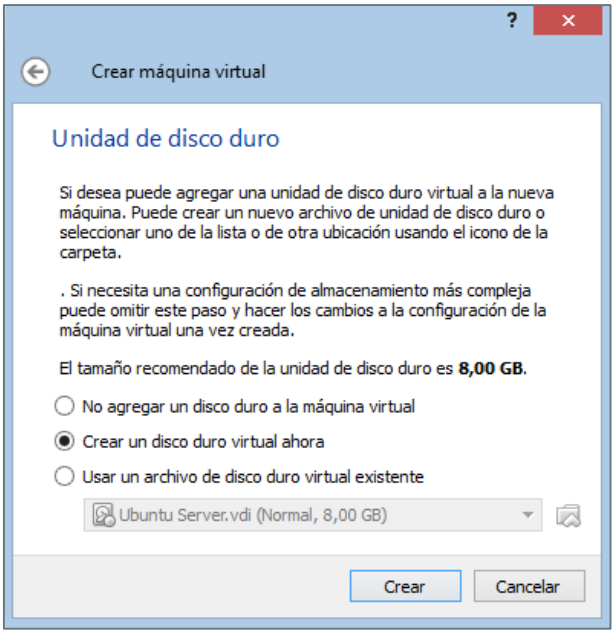

Figura 27. Configuración de disco duro virtual

En la ventana que aparece se deberán configurar los siguientes apartados:

- **Nombre:** establecemos el nombre que daremos al disco duro de cara a guardarse en nuestro disco físico (no tiene que ser uno en concreto, es solo para identificarlo posteriormente).
- **Tamaño:** el tamaño que tendrá nuestro disco duro.

- **Tipo de disco duro virtual:** el tipo de disco duro, que permitirá abrirlo en otros programas de virtualización. Por defecto viene tipo VirtualBox Disk Image (Para la instalación de Kali Linux hay que seleccionar VMDK).
- **Almacenamiento en el disco físico:** Permite elegir cómo se guardará el disco duro en nuestro disco duro físico.

Finalmente, pulsar en el botón "Crear" y el proceso de creación de la máquina virtual habrá terminado y estará lista para su uso.

3.4. Importación de máquinas virtuales

Una vez se tiene el software para las máquinas virtuales instalado como hemos visto en el apartado anterior, se debe proceder a importar las máquinas virtuales.

Para ello, hay que hacer click en "Archivo" → "Importar servicio virtualizado"

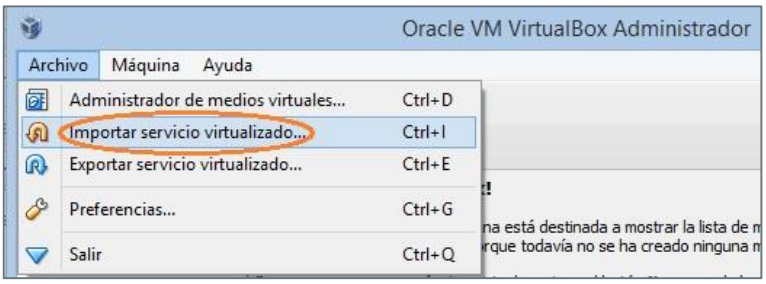

Figura 28. Importar máquina virtual

Elegir la ruta donde se encuentra la máquina virtual que se ha exportado anteriormente.

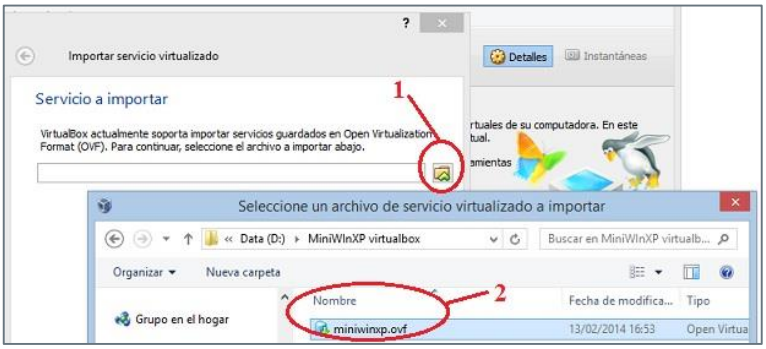

Figura 29. Selección de máquina virtual a importar

Por último, cambiar la configuración en caso de que sea necesario y hacer click en "Importar".

Figura 30. Confirmación de la importación

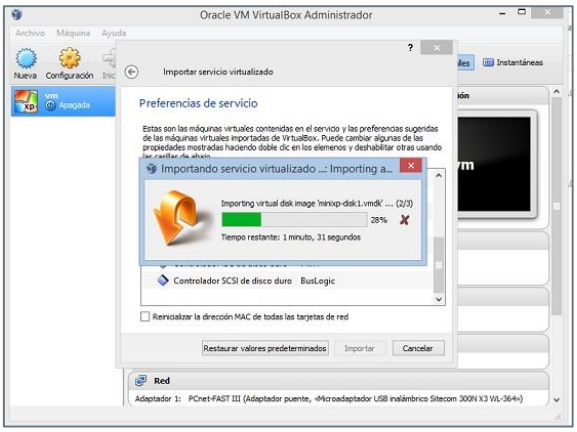

Figura 31. Pantalla durante la importación

3.4.1. Importación de máquinas virtuales vulnerables

- **Metasploitable2:** La máquina virtual Metasploitable es una versión de Ubuntu Linux intencionalmente vulnerable diseñada para probar herramientas de seguridad y demostrar vulnerabilidades comunes. Se utiliza en la temática de Fundamentos del análisis de sistemas.

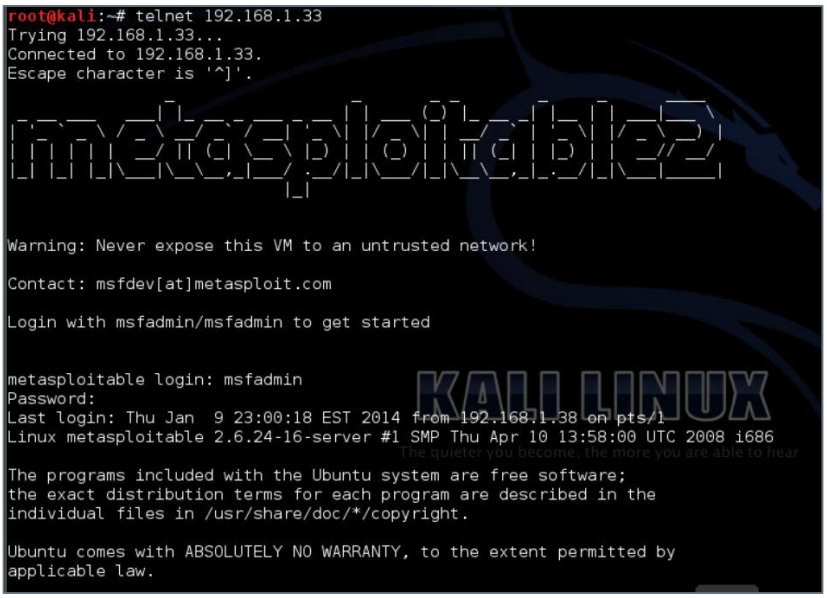

Figura 32. Máquina virtual Metasploitable2

La imagen de metasploitable2 puede ser descargada desde el siguiente enlace oficial: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

El proceso de importación es similar al detallado en el apartado 3.4. Una vez importada la máquina y en funcionamiento, es posible administrarla de forma interna con las siguientes credenciales:

- Usuario: msfadmin
- Contraseña: msfadmin

- Temáticas en las que se emplea:
  - Fundamentos del análisis de sistemas

3.5. Configuración de red de las máquinas virtuales

Para asegurar la visibilidad entre las diferentes máquinas virtuales desplegadas en la red, es necesario que estas se integren directamente con una IP de la propia red local, y no haciendo una redirección de tipo NAT.

Es necesario configurar en VirtualBox que el adaptador de red de la máquina virtual funcione en modo puente (bridge mode), de manera que obtenga una IP de la red de área local sobre la cual se van a realizar las pruebas.

Para ello, seleccionamos la máquina virtual a configurar y pulsamos sobre el botón "Configuración":

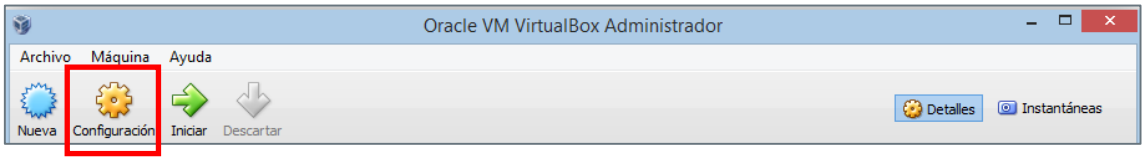

Figura 33. Acceso a configuración de la máquina virtual

En la ventana de configuración, seleccionamos la opción “Red”:

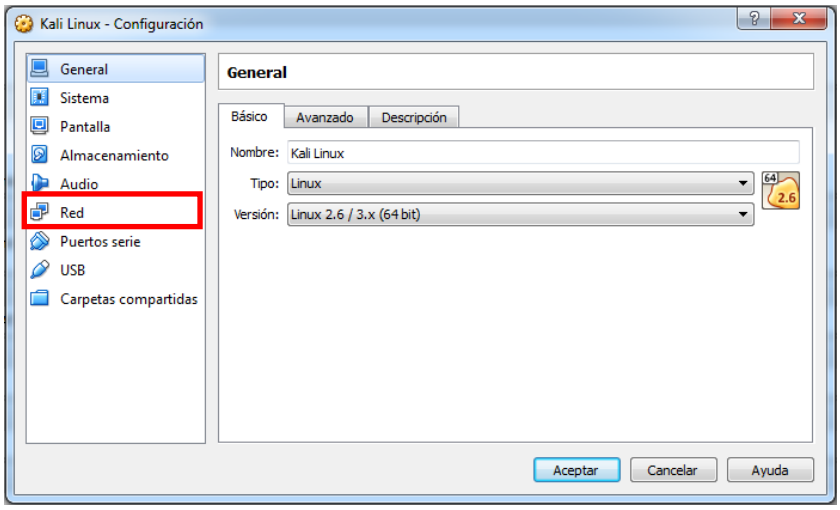

Figura 34. Acceso a la configuración de red

Posteriormente hay que seleccionar “Adaptador puente” en el desplegable:

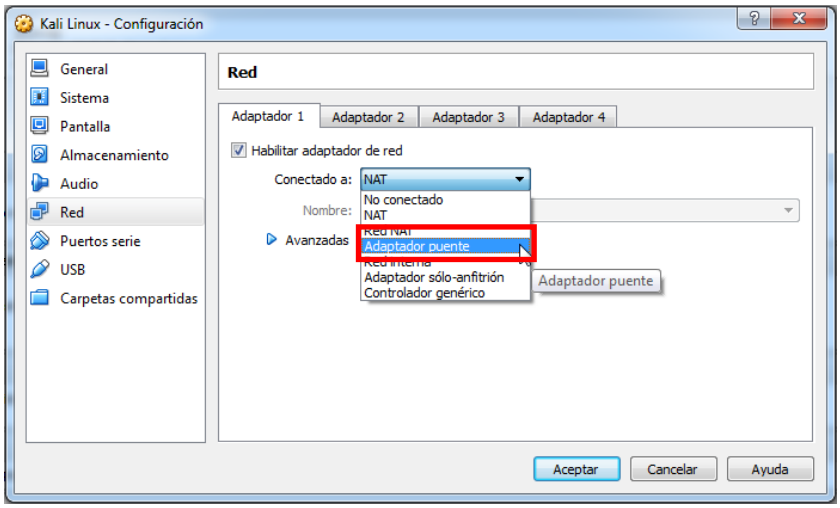

Figura 35. Configuración de la red en modo puente

Una vez seleccionado el modo “Adaptador puente”, hay que aceptar los cambios en la configuración.

4. CONFIGURACIÓN DEL ENTORNO

4.1. Requisitos de la red

La realización de gran parte de las prácticas requiere la configuración de un diseño de red específico en el cual se desplegarán las distintas máquinas virtuales citadas anteriormente.

Para ello, la red ha de cumplir una serie de requisitos que permitan una comunicación directa entre las diferentes máquinas virtuales desplegadas en la red:

- Disponibilidad de una red de área local con una máscara que permita conectar tantos dispositivos como máquinas virtuales se vayan a desplegar (el número de equipos de alumnos más las necesarias del formador).
- No debe existir ningún tipo de restricción de acceso a la red por parte de equipos no registrados, por ejemplo en caso de que exista un dominio Windows que restrinja la conexión de equipos no registrados.
- Deshabilitar cualquier otro mecanismo de seguridad que evite la conexión de equipos no contemplados, como por ejemplo mecanismos de filtrado MAC.
- Todos los alumnos y el formador deben tener sus respectivas máquinas virtuales en una misma vlan, de manera que sean visibles entre sí.
- El servidor DHCP debe estar configurado para proporcionar IPs automáticamente a sistemas nuevos.
- En gran parte de los ejercicios prácticos, es necesario que los equipos dispongan de acceso a Internet.
- En caso de que la red de área local a utilizar sea una red WiFi, los equipos deben tener una tarjeta de red inalámbrica.

5. CONFIGURACIÓN DE LOS ENTORNOS DE PRUEBAS

En los siguientes apartados, se detallan los esquemas de configuración de cada uno de los entornos de pruebas. De igual manera, se detallan las diferentes máquinas virtuales que es necesario desplegar en cada escenario.

Los diferentes diagramas de arquitectura deben ser tomados como una referencia conceptual y a alto nivel para mejorar el entendimiento del entorno, y no como un diagrama de red real.

5.1. Mi ordenador es un zombi

5.1.1. Configuración de red

Nos encontramos con el "Hacker" (profesor) que ataca a las víctimas a través de internet (alumnos). N representaría el número de equipos de los que se dispone para realizar el taller.

Tanto las máquinas virtuales del profesor como las máquinas virtuales de los alumnos deben estar en la misma red local y tener conectividad entre ellas.

El profesor debe tener instalado en la máquina virtual de Windows 7 las herramientas Flu, Process Monitor, Process Explorer y Wamp. Para realizar la fase de propagación del Malware es necesario conectar la máquina virtual de Kali Linux con la Máquina virtual de Windows 7 del profesor y utilizar la herramienta Beef.

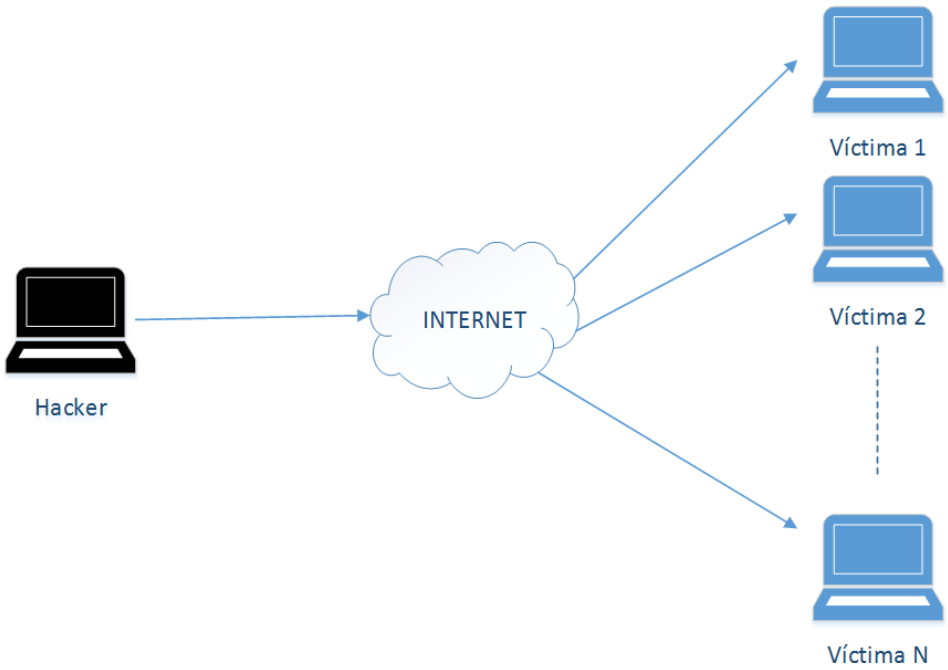

Figura 36. Entorno del taller Mi ordenador es un zombi

5.1.2. Máquinas virtuales necesarias

- **Profesor**
  - Sistema Operativo: Windows 7 – Botnet (botmaster)
    - Herramientas
      - Flu
      - Process Monitor
      - Process Explorer
      - Wamp
  - Sistema Operativo: Kali Linux
    - Herramientas:
      - Beef
- **Alumnos**
  - Sistema Operativo: Windows 7
    - Herramientas:
      - Process Monitor
      - Process Explorer

5.2. Programación segura de sitios Web

5.2.1. Configuración de red

El papel de los asistentes son los alumnos que entrarán en la página web vulnerable que se encuentra en su correspondiente servidor.

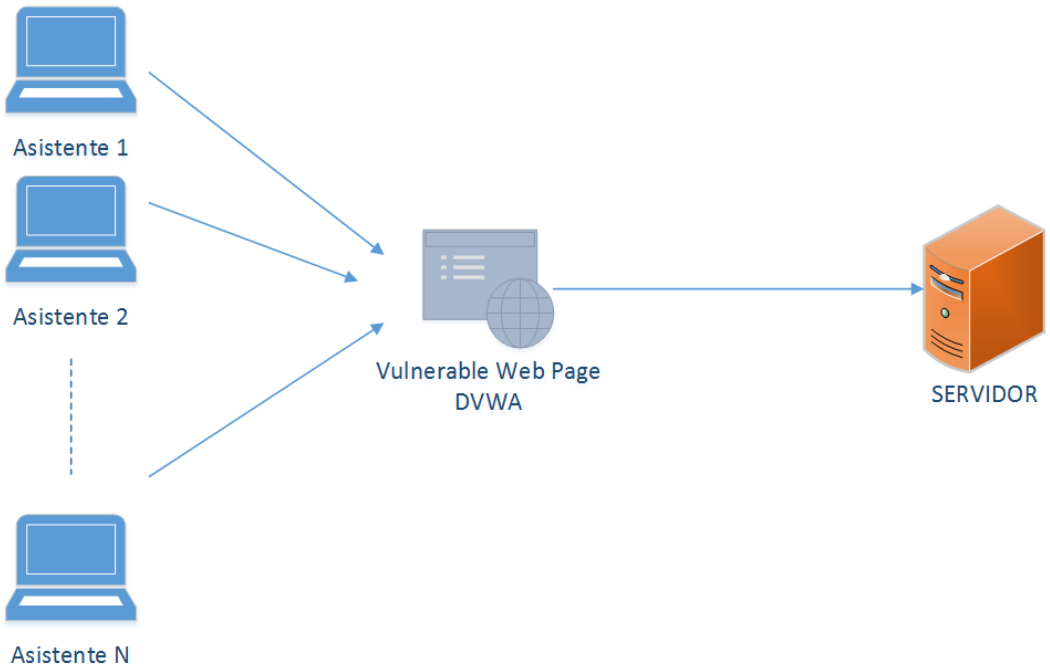

Figura 37. Entorno del taller Programación segura de sitios Web

5.2.2. Máquinas virtuales necesarias

- **Alumnos**
  - Sistema Operativo: Kali Linux.
    - Herramientas
      - Burp Suite
      - DVWA

Para arrancar DVWA es necesario introducir los siguientes comandos en cada uno de los equipos de los alumnos:

- service apache2 start
- service mysql start

Una vez arrancado el servidor, los alumnos accederán a la aplicación introduciendo la siguiente URL en el navegador:

- http://localhost/DVWA

Por último, las credenciales para autenticarse en la aplicación son:

- Usuario: admin
- Contraseña: password

5.3. Fundamentos del análisis de sitios Web

5.3.1. Configuración de red

El papel de los asistentes son los alumnos que entrarán en la página web vulnerable que se encuentra en su correspondiente servidor.

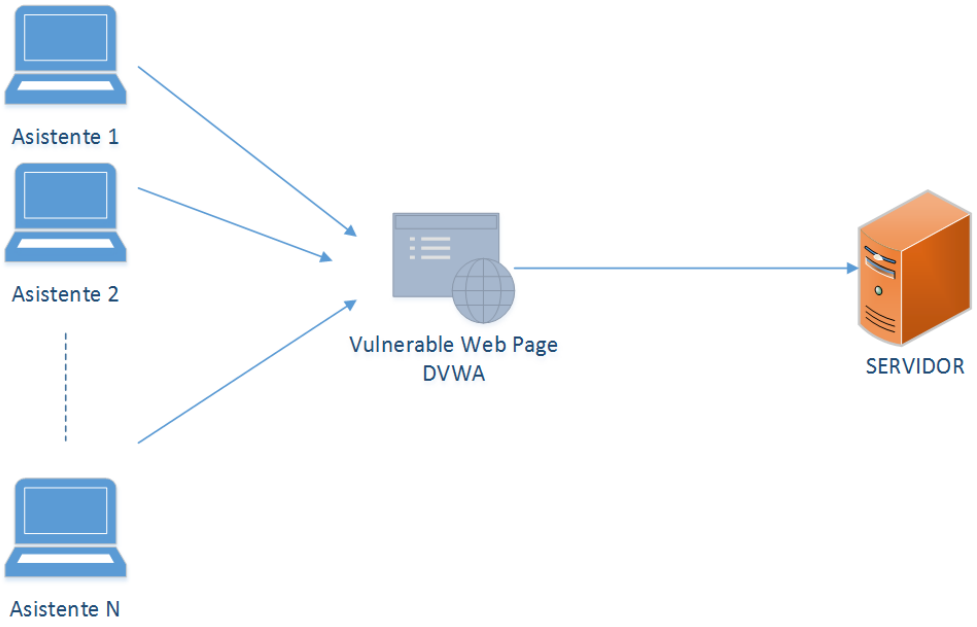

Figura 38. Entorno del taller Fundamentos del análisis de sitios Web

5.3.2. Máquinas virtuales necesarias

- **Alumnos**
  - Sistema Operativo: Kali Linux.
    - Herramientas
      - DVWA
      - OpenVas

  Para arrancar DVWA es necesario introducir los siguientes comandos en cada uno de los equipos de los alumnos:

  - service apache2 start
  - service mysql start

  Una vez arrancado el servidor, los alumnos accederán a la aplicación introduciendo la siguiente URL en el navegador:

  - http://localhost/DVWA

  Por último, las credenciales para autenticarse en la aplicación son:

  - Usuario: admin
  - Contraseña: password

5.4. Fundamentos del análisis de sistemas

5.4.1. Configuración de red

En este caso, los atacantes (alumnos) interactuarán con un sistema objetivo que simula un servidor web convencional. Dicho sistema será representado con la máquina virtual vulnerable *metasploitable2,* que estará controlada por el profesor.

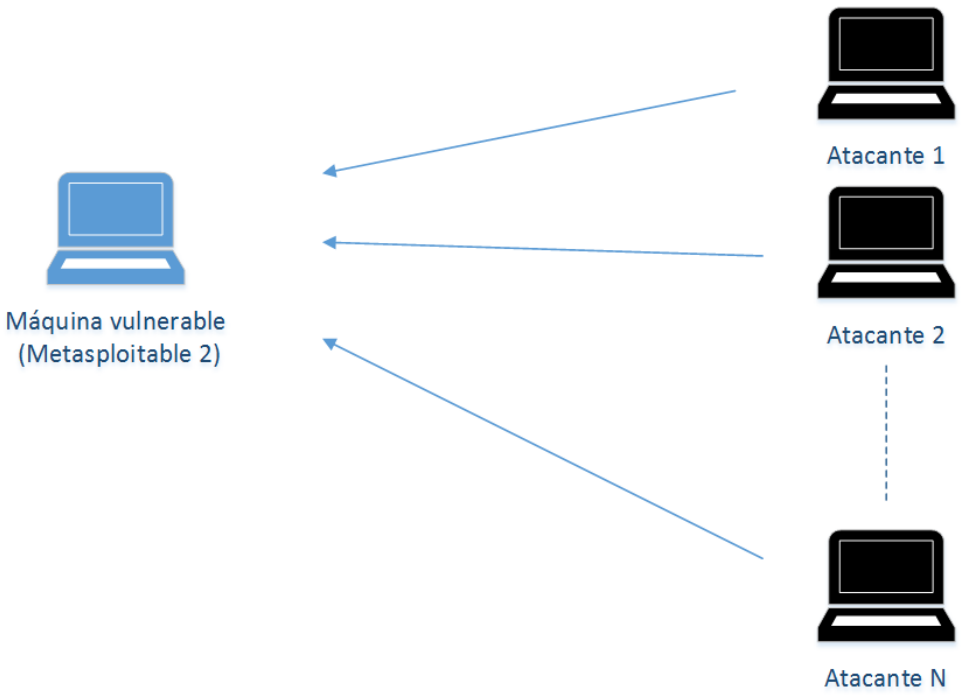

Figura 39. Entorno del taller Fundamentos del análisis de sistemas

5.4.2. Máquinas virtuales necesarias

- **Profesor**
  - Sistema Operativo: Metasploitable 2
    - Herramientas: sin necesidad de herramientas externas
- **Alumnos**
  - Sistema Operativo: Kali Linux
    - Herramientas: sin necesidad de herramientas externas

5.5. Análisis de malware en Android

5.5.1. Configuración de red

La práctica se realizará analizando una APP de Android.

Desde INCIBE recomendamos utlizar la APP Conan Mobile, aplicación segura que realiza gran cantidad de acciones y emplea varios permisos para poder llevar a cabo su cometido.

Se recomienda tener descargada la APP en los equipos antes de comenzar la formación, de cara a agilizar la clase y no invertir tiempo en la descarga durante el taller.

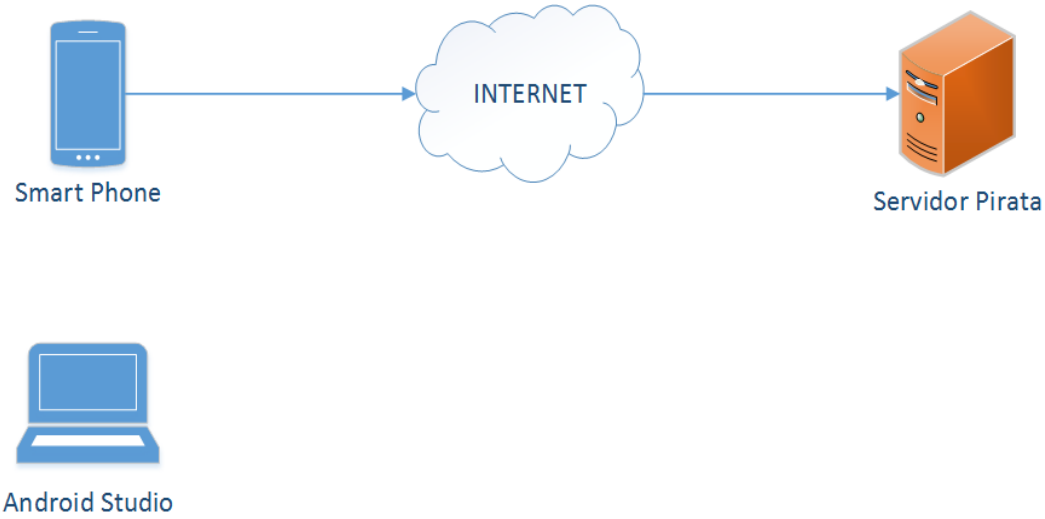

Figura 40. Entorno del taller Análisis de malware en Android

5.5.2. Máquinas virtuales necesarias

- **Profesor y alumnos**
  - Sistema Operativo: Windows 7
    - Herramientas:
      - Android Studio
      - Dextojar
      - Java Decompiler
      - Apktools
      - APP: Conan Mobile

5.6. Seguridad Wifi

5.6.1. Configuración de red

El entorno estará formado por un punto de acceso Wifi al cual se conectarán los asistentes, tanto alumnos como profesor. Posteriormente, dicho punto de acceso será el que se explotará durante la parte práctica.

El punto de acceso ha de ser configurado con **cifrado WEP** para realizar la práctica del taller. Esta configuración se realiza desde el panel de administración de cada router a través de la puerta de enlace.

Para que los asistentes puedan interactuar con el punto de acceso Wifi es necesario **disponer de tarjetas de red Wifi en cada uno de los ordenadores**.

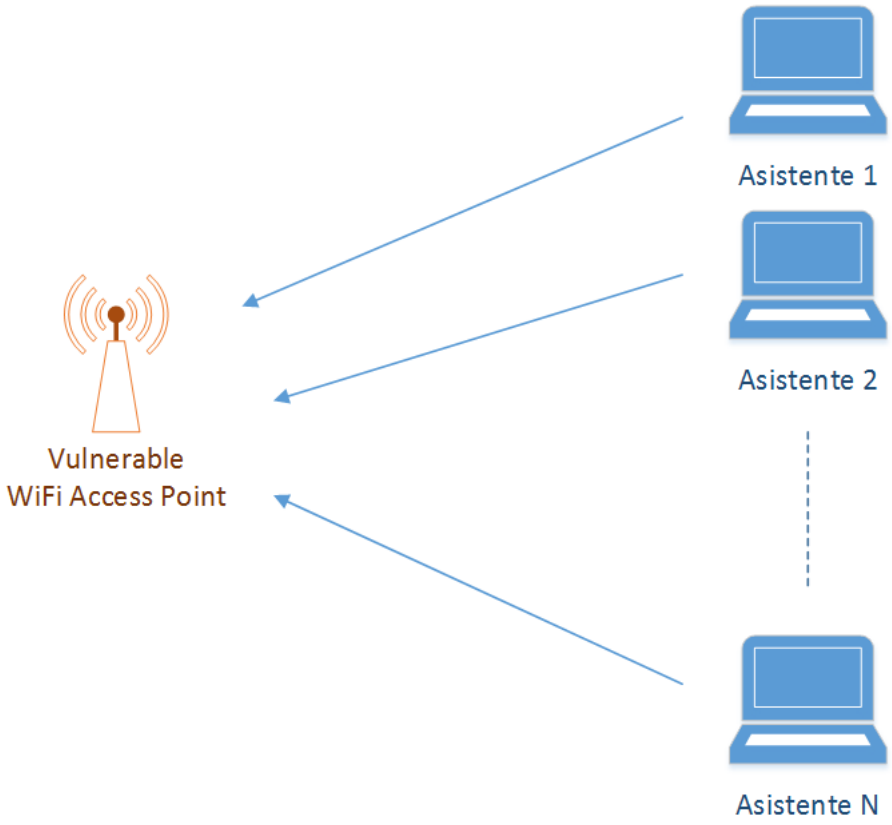

Figura 41. Entorno del taller Seguridad Wifi

5.6.2. Máquinas virtuales necesarias

- **Profesor y alumnos**
  - Sistema Operativo: Kali Linux
    - Herramientas: sin necesidad de herramientas externas

5.7. Espionaje y Cibervigilancia

5.7.1. Configuración de red

Nos encontramos con el asistente (alumnos) que se conectan de manera individual a Internet para realizar las búsquedas y prácticas contempladas durante la parte práctica.

Figura 42. Entorno del taller Espionaje y cibervigilancia

5.7.2. Máquinas virtuales necesarias

- **Profesor y alumnos**
  - Sistema Operativo: Windows 7
    - Herramientas:
      - Foca
      - GeoSetter
      - SilentEye
      - Tor

5.8. Forense en Windows

5.8.1. Configuración de red

En este último caso, toda la parte práctica es llevada a cabo de forma local, por lo que únicamente es necesario que los alumnos desplieguen las máquinas virtuales.

5.8.2. Máquinas virtuales necesarias

- **Profesor y alumnos**
  - Sistema Operativo: Windows 7
    - Herramientas:
      - Foca
      - MDD
      - Volatility
      - Dumpzilla
      - Suite Sysinternals
      - Recuva
  - Sistema Operativo: Kali Linux
    - Herramientas: sin necesidad de herramientas externas

6. PRINCIPALES PROBLEMAS

6.1. Resolución de problemas de virtualización

En ocasiones, es posible que se produzcan problemas al importar la máquina virtual por ciertos aspectos de compatibilidad o configuración. En este apartado se enumeran los problemas más comunes:

- **Error durante la importación:** Debido a que las máquinas virtuales exportadas son ficheros de tamaño considerable, puede ser común que al copiar el mismo en el equipo que va a virtualizar el sistema se corrompa el fichero. En caso de que se produzca un error durante la importación, se recomienda copiar de nuevo la máquina virtual exportada al disco duro local para solucionar una potencial corrupción del fichero.

- **Error de compatibilidad con USB 2.0:** Si el software VirtualBox no posee el Extension Pack instalado, puede producirse un error con el controlador de USB durante el inicio de la máquina. Para solucionarlo hay que dirigirse a *Opciones* > *USB* y deshabilitar el checkbox *Habilitar controlador USB 2.0*

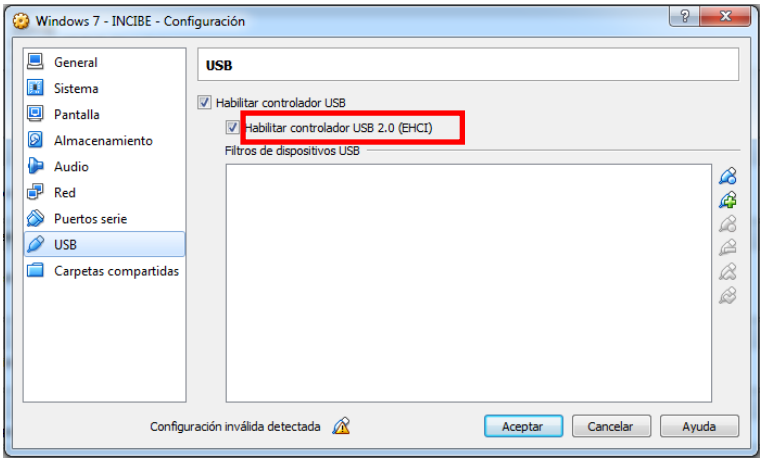

Figura 43. Error con compatibilidad USB

- **Fallo con el driver vboxdrv:** En caso de utilizar VirtualBox sobre un sistema Linux, es posible obtener un error con el driver vboxdrv al arrancar la máquina virtual. Para solucionarlo, hay que cerrar VirtualBox y ejecutar en la consola el comando *sudo /etc/init.d/vboxdrv setup.* Una vez finalice la acción, volver a lanzar VirtualBox.

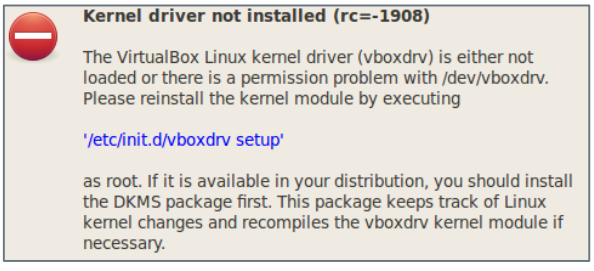

Figura 44. Error con drivers vboxdrv

- **Otros errores:** En caso de obtener otro tipo de error, se recomienda leer cuidadosamente el mensaje y los detalles del mismo, ya que es común que se detalle la causa del fallo y en ocasiones como solucionarlo.

6.2. Resolución de problemas de la red

En función de la configuración o tipología de la red, es posible que existan problemas derivados con la misma, siendo los más comunes los siguientes:

- **No existe visibilidad entre máquinas virtuales:** Verificar que la máquina virtual está configurada en modo puente, de manera que se asigne una IP de la red local. Adicionalmente, comprobar mediante el comando ifconfig (Linux) o ipconfig (Windows) que la IP asignada pertenece al rango configurado en la red local.

- **Las máquinas virtuales no obtienen IP:** Puede que el servicio DHCP no esté asignando IP a las máquinas virtuales de forma automática. Una posible solución es especificar la IP de forma estática en cada una de las máquinas virtuales.

6.3. Potenciales problemas con los entornos

La realización simultanea de las pruebas prácticas conceptuales y de los diferentes ataques, puede ocasionar ciertos problemas en los entornos:

- **Caída de sistemas:** Durante las prácticas sobre servidores vulnerables, es posible que el ataque simultáneo de todos los alumnos ralentice o deje no disponible el sistema. En ese caso, es necesario reiniciar la máquina virtual para reestablecer el servicio.

- **Ralentización en el acceso a Internet:** En prácticas que requieran de búsquedas o consultas en la red, es posible que se produzcan retardos en la respuesta en función del ancho de banda de la salida a Internet. En ese caso, se recomienda dividir la clase en dos o más grupos, de manera que intercalen las peticiones y no saturen la red.

- **Dispositivos WiFi:** Para la realización de los ejercicios prácticos de WiFi, es necesario disponer de un punto de acceso compatible con los ejercicios prácticos de la misma. Antes de llevar a cabo este taller se recomienda revisar la presentación del mismo y analizar la capacidad de configuración del dispositivo en función de las prácticas llevadas a cabo.

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INSTITUTO NACIONAL DE CIBERSEGURIDAD