



KALI LINUX

Seguridad Informática

Integrantes:

Christian Ordóñez
Alexander Peñaloza
Andrés Zhagüi
David Romero
Steven Muñoz



UNIVERSIDAD
DE CUENCA



CAPÍTULO 1

LA DISTRIBUCIÓN KALI



La Distribución Kali

Distribución de seguridad basada en Debian y diseñada para auditoría de seguridad, pruebas de intrusión e informática forense. Actualizada regularmente desde 2012.

Kali ofrece herramientas (+600) como NMAP, Wireshark, Aircrackng, Metasploit y John the Ripper para escaneo de puertos, análisis de redes, cracking, exploits y descifrado de contraseñas.

Mantenida por Offensive Security Ltd., Kali es adaptable a diversas arquitecturas (i386, AMD64, ARM). Incluye modos forenses para un análisis seguro desde dispositivos USB o CD sin utilizar el disco duro.

Instalación de Kali

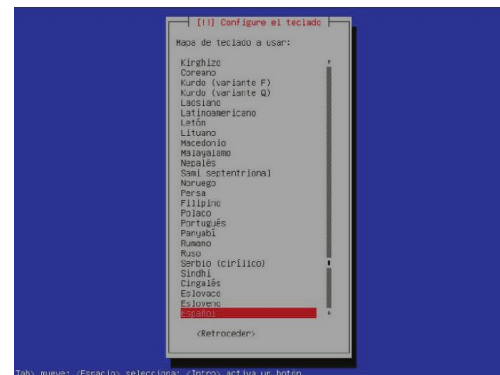
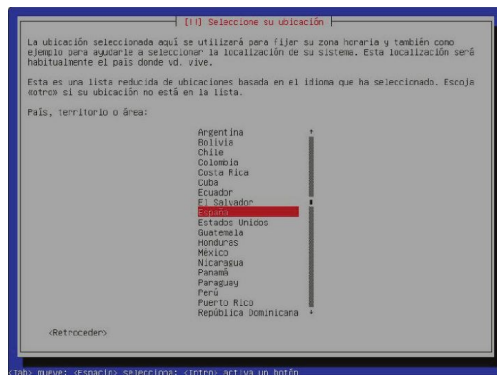
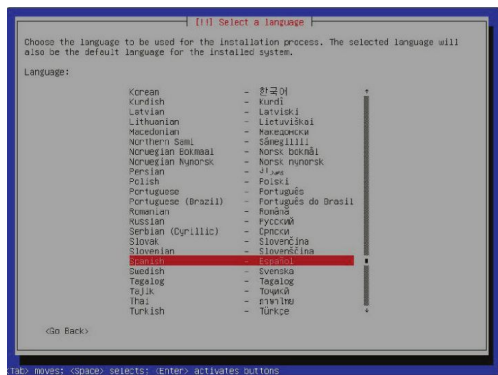
Se puede descargar la imagen de Kali desde la web <https://www.kali.org/downloads> y grabarlo en un dispositivo de arranque (USB, CD, HDD, SSD). La estabilidad del proceso de instalación dependerá del hardware que sea estable para soportar dicha instalación.

Luego se debe arrancar la PC desde el dispositivo con Kali y seleccionamos "Install"



Instalación de Kali

El proceso es un típico proceso de instalación de un sistema Linux, en donde se tienen que configurar ciertas cosas básicas como el idioma, la región, el teclado, nombre de la máquina, zona horaria, etc. Es un proceso guiado en donde es muy difícil perderse



```

[!!!] Configurar usuarios y contraseñas

Necesita definir una contraseña para el superusuario (root), la cuenta de
administración del sistema. Podría tener graves consecuencias que un usuario malicioso o
un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del
sistema, así que debe tener cuidado y elegir un la contraseña para el superusuario que no
sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o
una palabra que pueda asociarse fácilmente con usted.

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación,
y debe cambiarse regularmente.

La contraseña del usuario 'root' (administrador) no debería estar en blanco. Si deja esta
valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario
a la que se le darán permisos para convertirse en usuario administrador utilizando la
orden 'sudo'.

Tenga en cuenta que no podrá ver la contraseña mientras la introduce.

Clave del superusuario:

+-----+
[ ] Show Password in Clear
[Retornar]                                [Continuar]

```

[!] Configurar usuarios y contraseñas

Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.

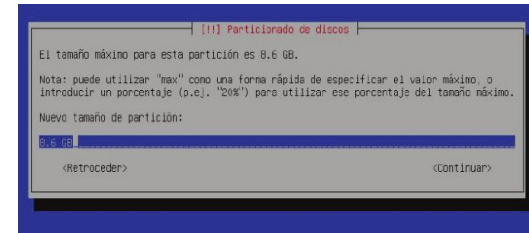
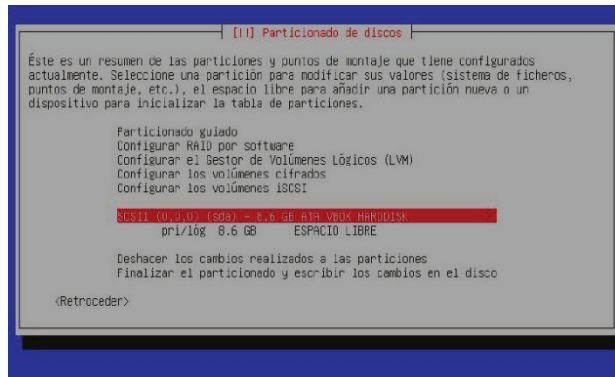
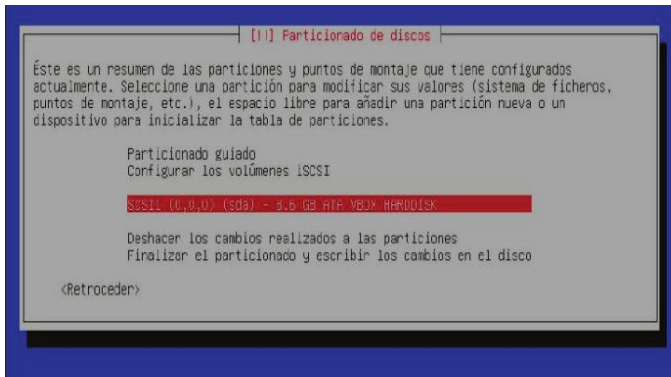
Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.

Nombre completo para el nuevo usuario:

<Retroceder> <Continuar>

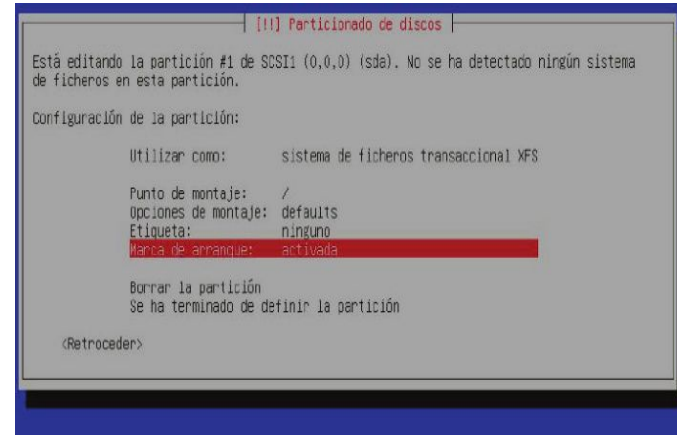
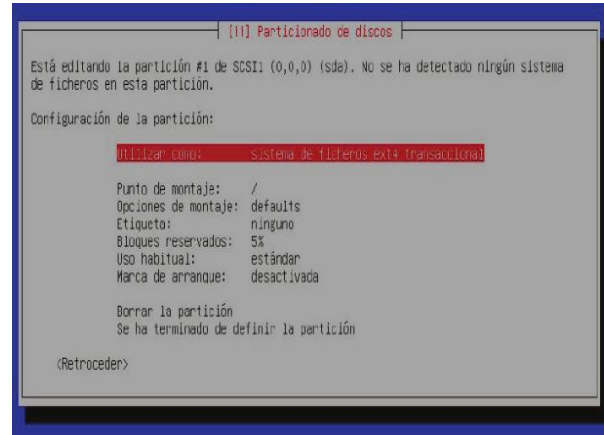
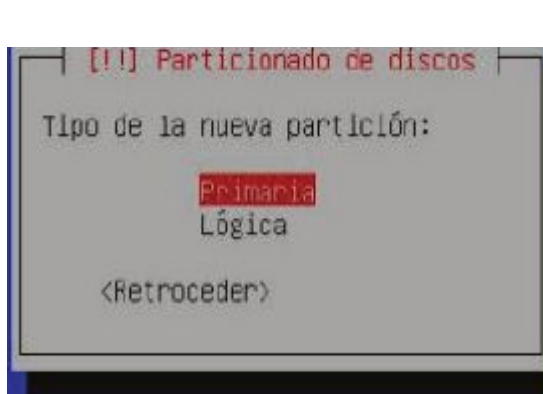
Instalación de Kali

Luego se debe particionar el disco, entonces seleccionamos un disco que deseamos particionar. Especificamos que punto de montaje queremos utilizar para una nueva partición y especificamos el tamaño (8GB mínimo y 16 GB mínimo recomendado)



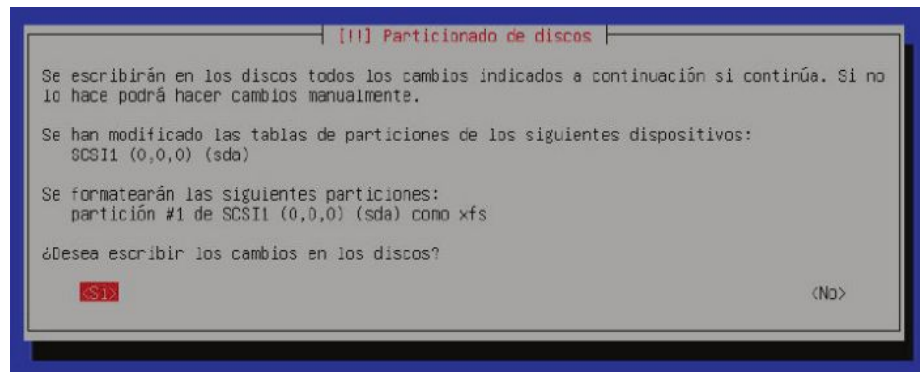
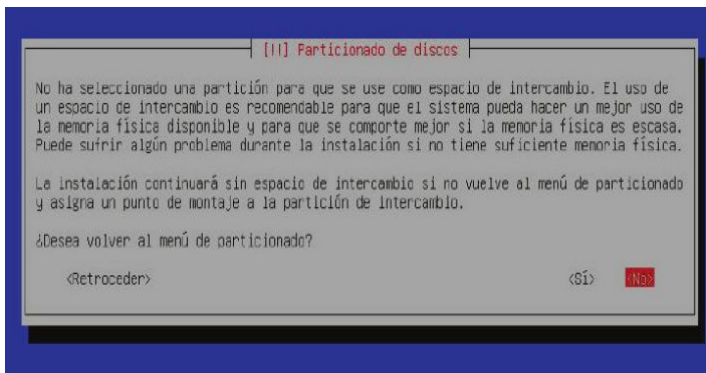
Instalación de Kali

Luego se debe elegir la partición como primaria, configurar la partición (ext4fs, XFS), activar la marca de arranque y finalizar la definición de la partición y escribir los cambios.



Instalación de Kali

Luego se puede decidir especificar una partición para swap (recomendable hacerlo cuando Kali esté instalado), se deben escribir todos los datos en disco y esperar que se instale el sistema.



Instalación de Kali

Una vez instalado el sistema, se procede a instalar el GRUB (cargador de arranque) en el registro principal de arranque, debemos seleccionar el dispositivo y finalmente presionar en continuar para una instalación completa de Kali.

[!] Instalar el cargador de arranque GRUB en un disco duro

Parece que esta instalación es el único sistema operativo en el ordenador. Si esto es así, puede instalar sin riesgos el cargador de arranque GRUB en el registro principal de arranque del primer disco duro.

Aviso: Si el instalador no pudo detectar otro sistema operativo instalado en el sistema, la modificación del registro principal de arranque hará que ese sistema operativo no pueda arrancarse. Sin embargo, podrá configurar GRUB manualmente más adelante para arrancarlo.

¿Desea instalar el cargador de arranque GRUB en el registro principal de arranque?

<Retroceder>

<Sí>

<No>

[!] Instalar el cargador de arranque GRUB en un disco duro

Ahora debe configurar el sistema recién instalado para que sea arrancable, instalando para ello el cargador GRUB en un dispositivo del que se pueda arrancar. La forma habitual de hacerlo es instalar GRUB en el registro principal de arranque («master boot record») del primer disco duro. Si lo prefiere, puede instalar GRUB en cualquier otro punto del disco duro, en otro disco duro, o incluso en un disquete.

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

<dev/sda> (ata-VBOX_HARDDISK_VB7a7087E0-94545da1)

<Retroceder>



Utilizar Kali sin Instalar: Modo persistencia

La modalidad de persistencia permite tener una Kali funcional y personalizada en un llavero USB, manteniendo la opción de arrancar en modo forense. Se puede instalar paquetes, almacenar paquetes y guardar datos.

Ideal para personalizar Kali y tenerla siempre disponible. Puede instalarse en el disco duro del ordenador, USB o DVD. La persistencia facilita el uso en modo forense, convirtiéndola en una herramienta potente.

Para configurar una Kali en persistencia, se lo debe hacer desde un Kali Linux ya preexistente.



Crear una partición de persistencia

Se pueden crear tres tipos de particiones de persistencia para Kali, en los cuales el espacio mínimo requerido es de 8GB y el recomendable es de 16GB para trabajar de forma continua:

- Ejecución virtualizada de Kali: recomendado para practicar y aprender a utilizar Kali
- Ejecución nativa en el propio USB de Kali: requerido 16Gb de espacio o recomendable más
- Ejecución nativa en disco físico: desde una herramienta de particionado preferida

Configurar la partición de persistencia

Para configurar la partición de persistencia, se debe reiniciar la máquina desde una imagen de Kali y arrancar en modo Live USB Persistence.

Luego se debe abrir una consola de texto y formatear la partición de persistencia con ext3.

```
mkfs.ext3 -L persistence /dev/sdh1
```

Si no le hemos puesto antes la etiqueta "persistence", se la ponemos:

```
e2label /dev/sdh1 persistence
```

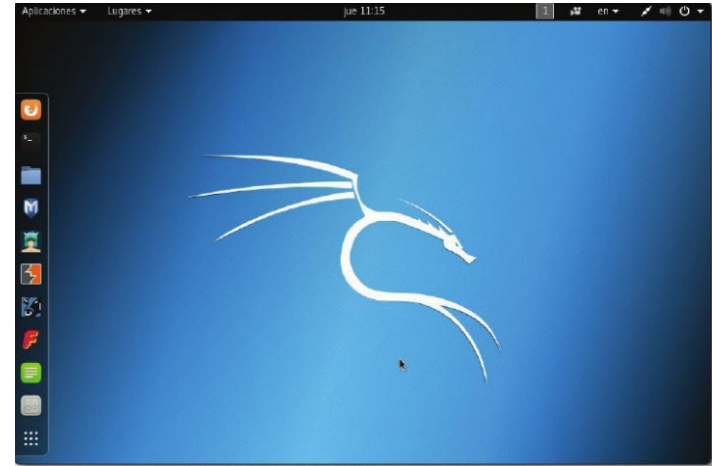
Finalmente, creamos el fichero de configuración del sistema de ficheros:

```
mount /dev/sdh1 /mnt  
echo "/" union" > /mnt/persistence.conf  
umount /mnt
```



Primero paseo por Kali

Al reiniciar la máquina nos aparecerá el GRUB de arranque para entrar en Kali y podremos visualizar la pantalla principal del sistema Kali. En la esquina superior izquierda tenemos un desplegable con las aplicaciones que Kali dispone. En la columna de la izquierda tenemos las aplicaciones que son de uso más común. La primera es el navegador iceweasel, un clon de Debian del navegador firefox. La siguiente, de arriba a abajo es la consola de texto. Después el gestor de archivos, Metasploit, Armitage, y así hasta completar una serie de aplicaciones y utilidades de uso común



Es muy recomendable después de haber instalado Kali, hacer una actualización de paquetes desde la terminal, ejecutando los siguientes comandos:

apt-get update (actualiza los repositorios)

apt-get upgrade (actualiza los paquetes)

Finalmente presionar “Enter” para ejecutar todas las actualizaciones del sistema

```

root@kali: ~
Archivo Editor Ver Buscar Terminal Ayuda

libmagickcore-6.q16-3 libmagickcore-6.q16-3-extra libmagickwand-6.q16-3
libmpx2 libnpt-common libnpt-runtime libnpt9 libnotiff4 libnss-myhostname
libobjc-6-dev libobjc4 libosmesa6 libpam-systemd libpango-1.0-0
libpangol-0-0 libpangoceiro-1.0-0 libpangoft2-1.0-0 libpangoft2-1.0-0
libplist3 libpocll libquadmath8 libradare2-1.1 libradare2-common
libradare2-dev librsane librsane-common libscbl libserf-1.1 libssodm18
libstdc++-6-dev libstdc++6 libsystemd libtiff5 libtss0 libudev1
libwayland-egl-mesa libwebkitgtk-4.0-37 libxatracker2 libxao5
linux-libc-dev llvm-3.8 llvm-3.8-dev llvm-3.8-runtime locales locales-all
mesa-common-dev mesa-va-drivers mesa-vgpu-drivers metasploit-framework
minikatz minicon multirarch-support nmap3 openjdk-8-jdk
openjdk-8-jdk-headless openjdk-8-jre openjdk-8-jre-headless openvpn
osinfo-db pocl-openssl icl postgresql postgresql-client-common
postgresql-common python-advanced-python python-apt-common python-cairo
python-flask python-formencode python-impact python-passlib python-tornado
python3-apt python3-reportbug radare2 rainbowcrack recon-ng reportbug
sane-utils set smmap sqlmap ssl-cert sslscan sysstat systemd systemd-sysv
udev unattended-upgrades vin vin-common vin-gtk vin-gui-common vin-runtime
vin-tiny x11-common xserver-xorg xserver-xorg-input-all
xserver-xorg-video-all xserver-xorg-video-nouveau xxd zsh

278 actualizados, 0 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
Se necesita descargar 0.8 MiB de archivos.
Se utilizarán 27,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]

```



CAPÍTULO 2

KALI PARA TESTS DE INTRUSIÓN

FASES DE UN TEST DE INTRUSIÓN



CONCEPTOS PREVIOS

1. Definición del Test de Intrusión:
 - Procedimiento de auditoría de seguridad activa.
 - Se realiza con autorización del propietario del sistema.
 - Analiza el sistema en busca de agujeros de seguridad.
2. Alcance del Test:
 - Enfoque en sistemas de información, incluyendo servidores, ordenadores y software.
 - Involucra al personal, procedimientos y gestión de información.
 - Puede utilizar técnicas no tecnológicas, como la ingeniería social.
3. Análisis Previo Requerido:
 - Diferencia de los escaneos automáticos indiscriminados.
 - Requiere un análisis previo detallado de los sistemas del cliente.
 - Es beneficioso después de una auditoría de seguridad ISO/IEC 27000.



CONCEPTOS PREVIOS

4. Legalidad y Delicadeza del Test:
 - Actos ilegales incluso con autorización expresa.
 - Es legalmente delicado y potencialmente ilegal, incluso con aprobación de la propiedad.
 - Consideraciones legales al leer correos electrónicos o intervenir comunicaciones.
5. Autorización y Propiedad:
 - La "propiedad" se refiere al dueño con el nivel ejecutivo máximo.
 - Cuidado al garantizar que el contratante tiene la autorización legal para la intrusión.
6. Fases No Lineales:
 - Posibilidad de regresar a fases anteriores en cualquier momento.
 - Ajustes en alcance, condiciones y permisos durante diferentes etapas.
 - Interpretar las fases en el contexto de interdependencia y posibles repeticiones.



FASE CERO: Emisión de presupuesto, acuerdo en los objetivos, y emisión de proformas iniciales

1. Presupuesto Detallado:
 - Documento con objetivos a cubrir, pruebas a realizar, máquinas involucradas y duración.
 - Iteraciones para ajustes y acuerdos por objetivos.
2. Contenidos del Presupuesto:
 - Hitos y entregables detallados.
 - Especificaciones claras sin exceso de tecnicismos.
3. Facturas Proforma:
 - Emitidas una vez aprobado el presupuesto.
 - Evitar emitir facturas por cantidades no recibidas.



FASE CERO: Emisión de presupuesto, acuerdo en los objetivos, y emisión de proformas iniciales

4. Cobro por Hitos:
 - Definición de logros en el presupuesto.
 - Emisión de factura proforma y cobro tras cumplir hito y entregar entregable.
5. Condiciones de Aceptación:
 - No iniciar siguiente etapa sin aceptación y pago del hito.
6. Porcentaje por Adelantado:
 - Evitar cancelaciones sin compensación.
 - Financiar proyecto hasta el primer hito en peor escenario.
7. Espaciar Hitos y Entregables:
 - Evitar disonancia cognitiva en el cliente.
 - Mantener fechas relativas para flexibilidad.



PRIMERA FASE: Alcance y condiciones del test de intrusión

1. Abono de Proforma y Emisión de Factura:
 - Inicia la fase de definición del alcance y condiciones del test de intrusión.
2. Enfoque de la Fase:
 - Detallar cómo se realizará el test más que qué pruebas se llevarán a cabo.
 - Explicar prueba a prueba, anticipando posibles resultados y restricciones.
3. Interacción con el Cliente:
 - Cliente puede poner restricciones basadas en inquietudes.
 - Propiedad y nosotros podemos agregar condiciones adicionales.
4. Precisiones Técnicas Necesarias:
 - Resultados precisos y detalle sobre la ejecución del test.
 - Especificar riesgos potenciales como paradas de servicios o saturación de red.



PRIMERA FASE: Alcance y condiciones del test de intrusión

5. Aprobación Explícita del Cliente:
 - Cliente debe aprobar explícitamente cualquier riesgo potencial.
 - Protección ante posibles demandas por responsabilidad civil.
6. Condiciones y Restricciones Adicionales:
 - Pueden implicar reducción o aumento en esfuerzo y tareas.
 - Evaluar la variación agregada del coste en función de estas condiciones.
7. Gestión de Variaciones de Coste:
 - Incrementos pueden compensar reducciones, manteniendo el costo final aproximado al presupuestado.
 - Comunicar al cliente cualquier desviación significativa y, si es necesario, volver a la fase de presupuesto.



SEGUNDA FASE: Recolección inicial de permisos y autorizaciones

1. Preparación Previa:
 - Con claridad sobre qué hacer y cómo, y propiedad aceptando efectos y consecuencias.
2. Permiso Escrito:
 - Obtener autorización escrita para llevar a cabo las operaciones especificadas.
3. Uso del Documento de Alcance:
 - El documento de alcance y condiciones puede servir como autorización en muchos casos.
4. Situaciones Específicas:
 - En casos complejos, se pueden requerir permisos adicionales.
 - Subcontratistas, autónomos, sistemas de otras empresas, etc.



SEGUNDA FASE: Recolección inicial de permisos y autorizaciones

5. Consentimiento Informado:

- Documento clave para individuos afectados, autorizando acciones y reconociendo posibles problemas y efectos secundarios.
- Categorizar efectos por probabilidad:
 - Seguro
 - Probable
 - Posible
 - Improbable pero técnica posible
 - Imposible

6. Negativa y Recurso:

- Si alguien se niega, discutir con su superior.
- Situaciones incómodas pueden surgir, pero no proceder sin autorizaciones apropiadas.



SEGUNDA FASE: Recolección inicial de permisos y autorizaciones

7. Comunicación de Impedimentos:
 - Notificar a la propiedad si alguna autorización es imposible.
 - Propiedad decide si sustituir a la persona, omitir la prueba o permitir que otra persona firme el consentimiento informado (si legalmente posible).
8. Continuación o Rediseño:
 - Proceder a la siguiente fase con todos los consentimientos informados.
 - Sin autorizaciones, puede requerir rediseño de tests e impactar el presupuesto.



TERCERA FASE: Validación legal y de permisos del alcance y condiciones del test de intrusión

1. Documentación Recopilada:
 - Revisar toda la documentación recopilada antes de iniciar cualquier acción.
2. Consideraciones Legales:
 - Evaluar la legalidad de las acciones planeadas.
 - Ataques a sistemas sin consentimiento, uso de cuentas no autorizadas, interceptación de comunicaciones, entre otros, son ilegales.
3. Límites Legales:
 - No se pueden realizar acciones ilegales, como robo, hurto, o registro no autorizado de pertenencias.
 - No se pueden acceder a correos electrónicos de terceros sin ser remitente o destinatario.



TERCERA FASE: Validación legal y de permisos del alcance y condiciones del test de intrusión

4. Consentimiento Informado:
 - Muchas acciones ilegales pueden legalizarse con el consentimiento informado del afectado.
 - Obtener consentimiento antes de llevar a cabo cualquier acción controvertida.
5. Alternativas Teóricas:
 - Si no es posible obtener consentimiento, analizar teóricamente la factibilidad de la acción.
 - Obtener pruebas de viabilidad y resultados sin ejecutarla.
6. Rediseño del Trabajo:
 - Si una acción es ilegal o impracticable, redefinir el alcance del trabajo.
 - Puede requerir ajustes en el presupuesto para reflejar cambios en el trabajo.



CUARTA FASE: Recolección de información

1. Introducción Técnica:
 - Primeras fases menos técnicas; esta marca el inicio de tres fases puramente técnicas.
2. Técnicas Utilizadas:
 - Empleo de técnicas como footprinting y fingerprinting para obtener información interna de sistemas y software bajo auditoría.
 - Uso de ingeniería social para obtener datos con poco esfuerzo.
3. Doble Objetivo de la Fase:
 - Evaluar la información accesible para un atacante externo.
 - Obtener datos prácticos no revelados en la información proporcionada, asegurándose de evitar filtraciones tácticas útiles para posibles ataques.
4. Prevenir el Filtrado de Información:
 - Propósito de mejorar la seguridad evitando la filtración de datos tácticos al exterior.



CUARTA FASE: Recolección de información

5. Segundo Objetivo: Información No Oficial:
 - Identificar aspectos no conocidos oficialmente, posiblemente ocultos por empleados de sistemas.
 - Descubrir información práctica que puede no estar en informes oficiales, como sistemas mantenidos extraoficialmente para resolver problemas desde casa o satisfacer demandas específicas de directivos.
6. Ejemplos de Información No Oficial:
 - Posibilidad de redes Wi-Fi no oficiales con bajas restricciones de seguridad.
 - Prácticas no reconocidas oficialmente, como soluciones informales a problemas o concesiones especiales a directivos.



QUINTA FASE: Análisis de las vulnerabilidades

1. Evaluación Detallada:
 - Partiendo de la información recolectada, analizar elemento por elemento en busca de vulnerabilidades conocidas y posibles brechas.
2. Definición de Estrategias de Ataque:
 - Plantear estrategias de ataque, especificando qué vulnerabilidades se documentarán, cuáles se probarán como prueba de concepto y cuáles se explotarán.
3. Consideración de Empresas Bien Preparadas:
 - En empresas con preparación integral, pasar a la siguiente fase sin problemas.
4. Aspectos Críticos Ocultos:
 - Encontrar aspectos críticos no revelados inicialmente podría requerir notificar a la propiedad para obtener autorización adicional.



QUINTA FASE: Análisis de las vulnerabilidades

5. Ejemplo de Notificación:
 - Descubrimiento de una red Wi-Fi no documentada con débil cifrado y autenticación.
 - No asumir autorización para "romperla"; notificar a la propiedad y obtener permisos antes de la explotación de vulnerabilidades.
6. Autorización para Explotar:
 - Propiedad debe otorgar permisos explícitos para la explotación de vulnerabilidades recién descubiertas.
7. Posibles Ampliaciones de Presupuesto:
 - Puede ser necesario extender el presupuesto si el cliente considera análisis adicionales necesarios debido a nuevas pruebas descubiertas durante la fase de ataque y evaluación.



SEXTA FASE: Explotación de las vulnerabilidades

1. **Aprehensión del Auditor:**
 - Fase que genera inquietud en aquellos sin experiencia o sin comprensión de las implicaciones legales.
2. **Preocupaciones del Auditor Experimentado:**
 - Preocupaciones serias sobre connotaciones legales, especialmente por posibles consecuencias negativas.
3. **Importancia de Documentar Vulnerabilidades:**
 - En muchos casos, documentar la existencia de una vulnerabilidad sin explotarla es suficiente.
 - Pruebas de concepto o demostraciones técnicas pueden ser adecuadas sin entrar en la fase de explotación.
4. **Pruebas de Concepto:**
 - Objetivo: demostrar la posibilidad técnica de explotar la vulnerabilidad, no causar daño.
 - Se utiliza cuando se enfrenta a personal técnico escéptico y la propiedad busca validación técnica.



SEXTA FASE: Explotación de las vulnerabilidades

5. Uso de Pruebas de Concepto:
 - Común en vulnerabilidades que afectan a bases de datos en producción, ERP, o que implican ataques de denegación de servicio.
 - No es necesario causar daño; la demostración de la posibilidad técnica es suficiente.
6. Explotación de Vulnerabilidades:
 - En algunos casos, se prefiere explotar las vulnerabilidades con la autorización del cliente.
 - Ejemplos: sistemas de seguridad perimetral, redes Wi-Fi, pinneo de NATs y firewalls, inyecciones SQL.
7. Razones para Explotar Vulnerabilidades:
 - Son técnicas necesarias para "saltar" a sistemas internos.
 - Permiten atacar máquinas aparentemente no en primera línea.
8. Importancia de Técnicas Inocuas:
 - Técnicas que no generan daño ni paradas de servicio son preferidas para evitar impactos negativos.



SÉPTIMA FASE: Redacción de informe de auditoría y presentación de resultados a la propiedad

1. Importancia Destacada:
 - Considerada como la fase más crucial de los tests de intrusión.
2. Transmisión Efectiva al Cliente:
 - La habilidad de comunicar los descubrimientos de manera comprensible al cliente es fundamental.
3. Redacción de Informes:
 - Requiere habilidades de redacción para ser técnico pero accesible, utilizando símiles del mundo físico para mayor comprensión.
4. Hablar en Público:
 - Habilidad para hablar en público, transmitir, conectar con la audiencia y presentar información desafiante de manera efectiva.



SÉPTIMA FASE: Redacción de informe de auditoría y presentación de resultados a la propiedad

5. **Aplomo y Cuajo:**
 - Necesidad de confianza y resiliencia para presentar hallazgos desagradables ante audiencias posiblemente hostiles.
6. **Asumir Críticas:**
 - Habilidad para aceptar críticas y tener rapidez mental para debatir argumentos en tiempo real.
7. **Autocontrol y Mesura:**
 - Mantener la calma y ser medido ante situaciones desafiantes, evitando reacciones impulsivas.



SÉPTIMA FASE: Redacción de informe de auditoría y presentación de resultados a la propiedad

8. Habilidades de Comunicación General:
 - Aspectos específicos de redacción y presentación son tratados en cursos de escritura y habla en público, aplicables a la auditoría informática.
9. Recomendaciones para Mejorar:
 - Participar en grupos como Toastmasters o teatro para mejorar habilidades de hablar en público, perder el miedo escénico y perfeccionar la vocalización.
10. Enfoque en Aspectos Profesionales:
 - Detalles específicos de la redacción de informes se encuentran en libros dedicados a la auditoría informática o informes periciales, ya que requieren un tratamiento más detallado.



OCTAVA FASE: Presentación de resultados al personal técnico y formación

1. Separación de Presentaciones:
 - Destacamos la separación de la presentación de resultados a la propiedad y al personal técnico.
 - La distinción se basa en la terminología específica del público y la dinámica de la reunión.
2. Razones para Separar las Presentaciones:
 - Razones de comunicación: adaptarse al lenguaje técnico del personal.
 - Mecánica de la reunión: evitar discusiones innecesarias con el personal técnico.
3. Enfoque Formativo:
 - Diferente enfoque en comparación con la presentación a la propiedad.
 - El objetivo es proporcionar formación más que simplemente presentar hallazgos.



OCTAVA FASE: Presentación de resultados al personal técnico y formación

4. Prevenir Discusiones Estériles:
 - Consideración de que el personal técnico puede sentirse atacado y tender a defenderse, generando discusiones improductivas.
5. Enseñar Soluciones y Buenas Prácticas:
 - Fomentar la comprensión del personal técnico sobre la naturaleza de los problemas y cómo abordarlos.
 - Enseñar buenas prácticas para evitar recurrencias.
6. Enfoque Similar al de la Presentación a la Propiedad:
 - Paralelismo en términos de presentación efectiva y enseñanza eficiente.



CAPÍTULO 3

RECOGIDA DE INFORMACIÓN INICIAL CON KALI



Recopilación de información inicial con Kali

- Fase esencial de un ataque de intrusión.
- Permite al atacante conocer la víctima
- Se divide en dos etapas:
 - Externa: sin acceso a los sistemas de la víctima
 - Interna: una vez que el atacante ha obtenido acceso a los sistemas
- Herramientas de Kali: Nmap, TheHarvester, Metasploit



Recogida de Información a través de OSI

- La recopilación de información externa se basa en técnicas OSINT, o inteligencia de fuentes abiertas.
- Las técnicas OSINT más utilizadas son la búsqueda por Internet de información de los sistemas de información de la empresa, especialmente a través de los perfiles de LinkedIn de trabajadores o de antiguos trabajadores.
- La recogida de información vía OSI siempre debe preceder al uso de herramientas, para evitar ser demasiado intrusivo.
- Existen herramientas en Kali que ayudan a organizar la información recopilada, como Maltego.
- La recopilación de información a través de técnicas manuales es importante para comprender cómo funcionan las técnicas OSINT y para evitar ser detectado por los sistemas de detección de intrusos.





Recogida de Información a través del DNS

- La recopilación de información a través del DNS es una técnica importante para la auditoría de seguridad.
- El análisis de DNS puede proporcionar información sobre los sistemas de la empresa, incluso si la empresa tiene un IDS bien configurado.
- Para obtener una transferencia de zona, se puede utilizar la herramienta dnsenum.
- Las entradas A de la zona DNS proporcionan información sobre las IP de las máquinas del dominio.
- Los servidores de nombre y los servidores de correo MX también son información importante que se puede recopilar a través del DNS.



Recogida de Información a través del DNS

- Los registros SPF pueden proporcionar información sobre las IP públicas activas del dominio.
- Los registros HINFO pueden proporcionar información sobre el sistema operativo de las máquinas del dominio.
- Los subdominios también pueden proporcionar información valiosa sobre los sistemas de la empresa.
- La herramienta dnsrecon puede utilizarse para buscar subdominios por fuerza bruta.



Identificación de nodos vivos y escaneo de puertos

- La identificación de nodos vivos se realiza mediante la opción -sP de nmap.
- El tipo de barrido para descubrir sistemas puede ser -PB, -PO, -PS, -PA, -PU, -PE, -PP, -PM o -PA.
- El tipo de sondeo sobre los nodos vivos puede ser -sP, -sT, -sS, -sU, -sO, -sN, -sF, -sX, -sA, -sW, -sM o -sl.
- Es importante tener en cuenta que los sondeos TCP SYN y TCP ACK solo indican que hay algo escuchando en el puerto, pero no que el puerto esté abierto.



Identificación de nodos vivos y escaneo de puertos

- Nmap es una herramienta fundamental para la auditoría de seguridad.
- Se puede utilizar para identificar nodos vivos y escanear puertos.
- Hay diferentes tipos de sondeos para identificar nodos vivos, cada uno con sus ventajas y desventajas.
- Hay diferentes tipos de escaneos de puertos, cada uno con sus ventajas y desventajas.



LYNIS

- Lynis es una utilidad para analizar la seguridad de un sistema. Se puede utilizar para realizar auditorías de seguridad desde una cuenta con privilegios de root o desde una cuenta no privilegiada.
- Para ejecutar Lynis desde una cuenta con privilegios de root, se utiliza el comando:

```
lynis audit system
```

- Para ejecutar Lynis desde una cuenta no privilegiada, se utiliza el comando:

```
lynis audit system --pentest
```



GOLISMERO

- Golismero es una herramienta de seguridad que permite escanear servidores web y encontrar vulnerabilidades.
- El uso básico de Golismero es el siguiente:

```
golismero scan servidor
```

- Golismero también permite automatizar los tests de penetración.
- Es importante tener en cuenta que Golismero puede realizar ataques contra los servidores web que escanea. Por lo tanto, es necesario obtener el consentimiento informado del cliente antes de utilizar la herramienta.




Otras utilidades

- Hay muchas otras utilidades y técnicas para obtener información que pueden ser utilizadas en pruebas de penetración.
- Algunas de las técnicas más importantes son:
 - nbtscan: Extracción de información de SMB
 - AccCheck: Verificación de accesos a los recursos virtuales IPC\$ y ADMIN\$
 - Nikto: Buscador de plugins de CMS
 - BlindElephant: Buscador de plugins de CMS
 - Plecost: Buscador de plugins de WordPress
 - Wpscan: Buscador de plugins de WordPress
 - JoomScan: Buscador de plugins de Joomla
- Es importante seleccionar la técnica adecuada para cada escenario.



CAPÍTULO 4

ANÁLISIS BÁSICO DE VULNERABILIDADES



Se introducen técnicas básicas para analizar vulnerabilidades.

La recolección de información nos permitirá:

- No notar como vulnerabilidades cosas que no lo son.
- Identificar procesos no conocidos por gerencia.
- Identificar cosas que faltan.
- Pistas e indicios sobre dónde están las vulnerabilidades reales.



YERSINIA

Su función básica es explotar vulnerabilidades conocidas de distintos protocolos de red; cubriendo un porcentaje muy importante de los protocolos de red comunes en entornos productivos.

Es capaz de validar un ataque, además puede ejecutarlo.

Tiene tres modos de uso:

- Línea de comandos.
- Utilizando comandos en ncurses.
- Interfaz GTK para Yersinia

Línea de comandos

yersinia protocolo -attack ataque opcionesataque

```
root@kali:~# yersinia dhcp -attack 1
Warning: interface eth0 selected as the default one
<*> Starting DOS attack sending DISCOVER packet...
<*> Press any key to stop the attack <*>
```

Dónde protocolo corresponde con el protocolo que vamos a atacar, ataque con un número que identifica al ataque, y que obtenemos en la página del manual -man- de yersinia, y opcionesataque son una serie de opciones del ataque que dependen del ataque, y son específicas para cada uno de estos

Ncurses

```
yersinia 0.7.3 by Slay & tomac - STP mode [03:23:56]
RootId      BridgeId      Port      Iface Last seen

Available commands
h      Help screen
x      eXecute attack
i      edit Interfaces
ENTER  information about selected item
v      View hex packet dump
d      load protocol Default values
e      Edit packet fields
f      list capture Files
s      Save packets from protocol
S      Save packets from all protocols
L      Learn packet from network
M      set Mac spoofing on/off
l      List running attacks
K      Kill all running attacks
c      Clear current protocol stats
C      Clear all protocols stats
g      Go to other protocol screen
Ctrl-L redraw screen
w      Write configuration file
a      About this proggie
q      Quit (bring da noize)

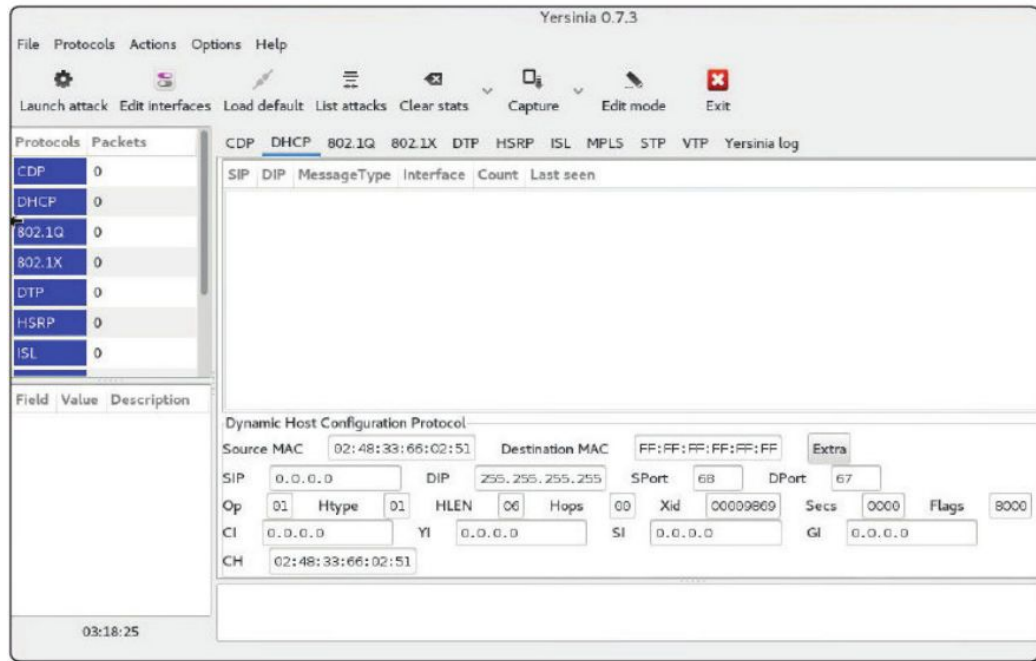
Total Packets: 0 AC Spoofing [X]
This is the help screen.

STP Fields
Source MAC 0A:23:16:02:FF:08 Destination MAC 01:80:C2:00:00:00
Id 0000 Ver 00 Type 00 Flags 00 RootId 5080.760F0E14AC58 Pathcost 00000000
BridgeId CB09.E7CD90117CAA Port 8062 Age 0000 Max 8014 Hello 0002 Pwd 000F
```

Es un modo muy práctico y fácil de utilizar, tanto en local como en remoto a través de consola ssh.

Una desventaja es que Ncurses hace difícil crear scripts.

GTK para Yersinia



Los ataques disponibles con Yersinia son:

- IEEE 802.1Q
- IEEE 802.1X
- Cisco Discovery Protocol (CDP)
- Dynamic Host Conguration Protocol (DHCP)
- Dynamic Trunking Protocol (DTP)
- Hot Standby Router Protocol (HSRP)
- Inter-Switch Link Protocol (ISL)
- Spanning Tree Protocol (STP)
- VLAN Trunking Protocol (VTP)



CAPÍTULO 5

ATAQUES A CONTRASEÑAS



Ataques a contraseñas

- Fuerza bruta: Versión Hollywoodense no es efectiva en el mundo real.
- Ingeniería social: Claves débiles basadas en datos personales; post-its con contraseñas.
- Ataque por diccionario: Uso de palabras clave dirigidas; efectivo en claves sencillas.
- Ataque por rainbow tables: Precomputa claves cifradas; limitado por el uso de "salts" aleatorios.
- Vulnerabilidades específicas: Explotación de debilidades en la aplicación o protocolo.



5.1 FINDMYHASH

FINDMYHASH es un script en Python para calcular hashes eficientemente.

Algoritmos Soportados: MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512, RMD160, MYSQL, LDAP_MD5, LDAP_SHA1, CISCO7, JUNIPER, GOST, WHIRLPOOL, LM, NTLM.

Uso Práctico: Útil para encontrar contraseñas de usuarios, especialmente en MySQL.

Si se encuentra una clave de un usuario, es probable que o esa clave o una parecida la utilice para su cuenta ssh.

EJEMPLO DE USO:

- `findmyhash algoritmo -h valordehash`
- `findmyhash MD5 -h 916f4c31aaa35d6b867dae9a7f54270d -g`

5.2 HYDRA

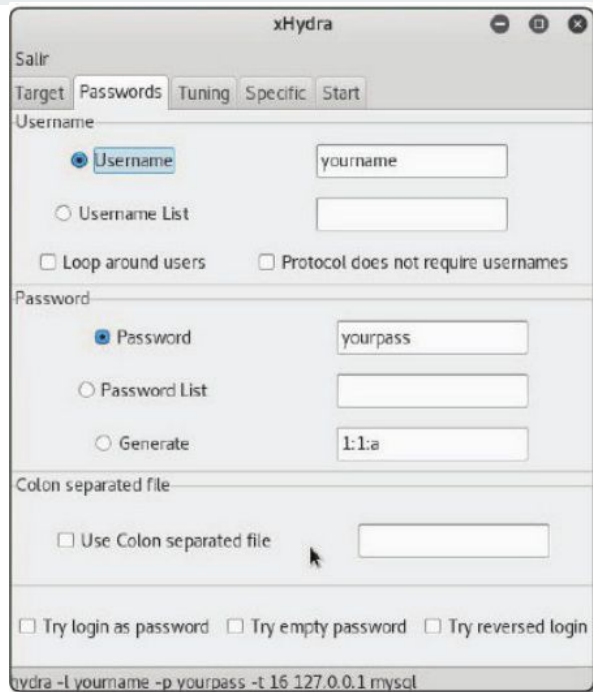
Útil para ataques de fuerza bruta, soporta varios protocolos. Una vez se lanza el programa se puede elegir que analizar. Se puede usar IPv4/IPv6, se elige puerto y protocolo a usar.

- Use SSL: Para pruebas a través de SSL.
- Show attemps: Muestra los intentos en la lengüeta de inicio.
- Be verbose: información adicional en la lengüeta de inicio.
- Debug: Información de depuración en la lengüeta de inicio.

afp	cisco	cisco-enable	cvs
firebird	ftp	http-get	http-head
http-proxy	https-get	https-head	https-form-get
https-form-post	icq	imap-ntlm	imap
ldap2	ldap3	mssql	mysql
ncp	nnntp	oracle-listener	pcanywhere

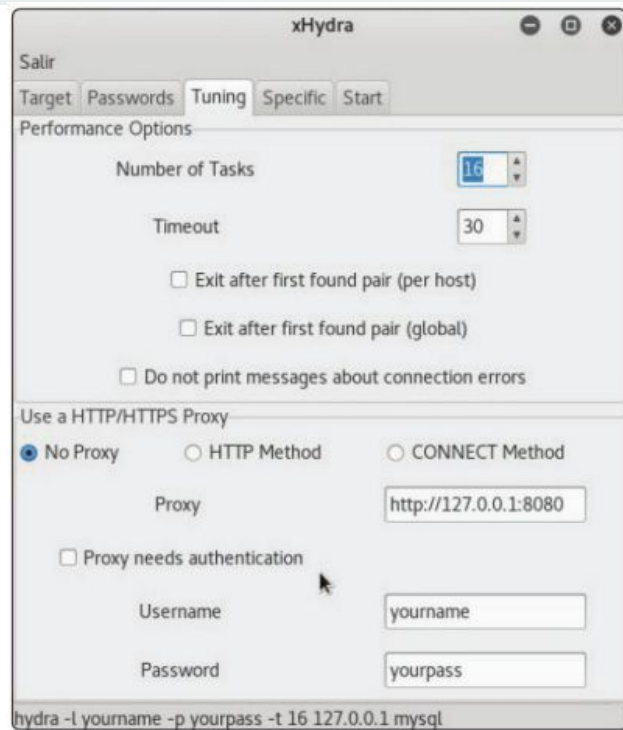
pcnfs	pop3	pop3-ntlm	postgres
rexec	rlogin	rsh	sapr3
sip	smb	smbnt	smtp-auth
smtp-auth-ntlm	snmp	socks5	ssh2
svn	teamspeak	telnet	vmauthd
vnc			

Protocolos que puede usar Hydra



Tuning: Opciones para mejorar el rendimiento

- Number of Tasks: Número de hilos a la vez, 36 por defecto.
- Timeout: Tiempo espera para la respuesta un objetivo. 30s defecto.
- Exit after first found pair: análisis termina cuando login/password funciona.
- No proxy / HTTP Method / CONNECT Method: si no se tiene proxy, o si se conecta por HTTP o por CONNECT.
- Proxy: Dirección del proxy, en formato http://IP:puerto

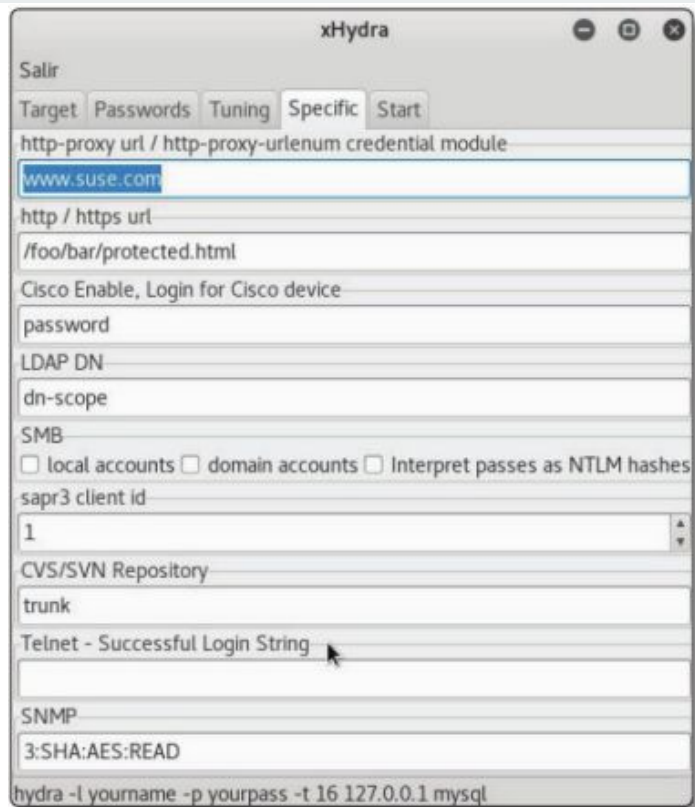


Passwords:

Colon separated file: Se puede indicar un fichero csv con usuarios y claves.

Try login as password: Prueba el nombre de login como posible combinación de contraseña

Try empty password: Prueba también con una clave vacía.



Specific: tenemos algunos parámetros específicos de algunos protocolos



Start: tenemos las opciones de arranque, parada, grabar la salida y limpiar la ventana de salida.

5.3 JOHN THE RIPPER

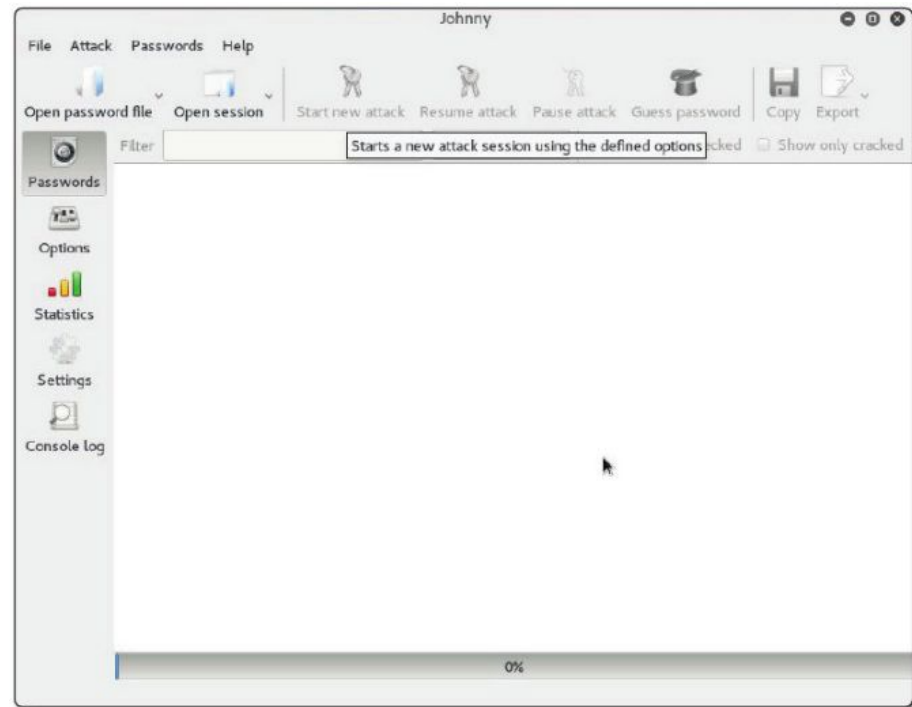
Funciona sin conexión. Usa CUDA o OpenCL para atacar claves con mayor eficiencia.

Soporta varios hashes: MD5, SHA1, LM y NTLM, y demás.

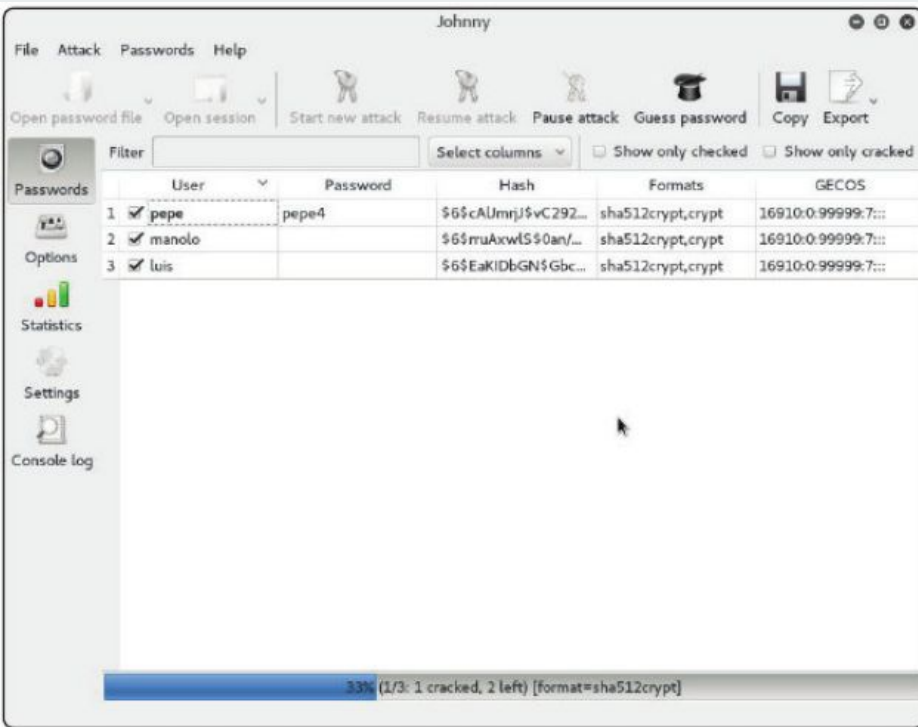
Para ello se necesita el fichero con los hashes; para probar claves, las codifica como hashes, y verifica si coincide con el hash almacenado.

Pulsando en “Options”, se puede elegir el modo de ataque.

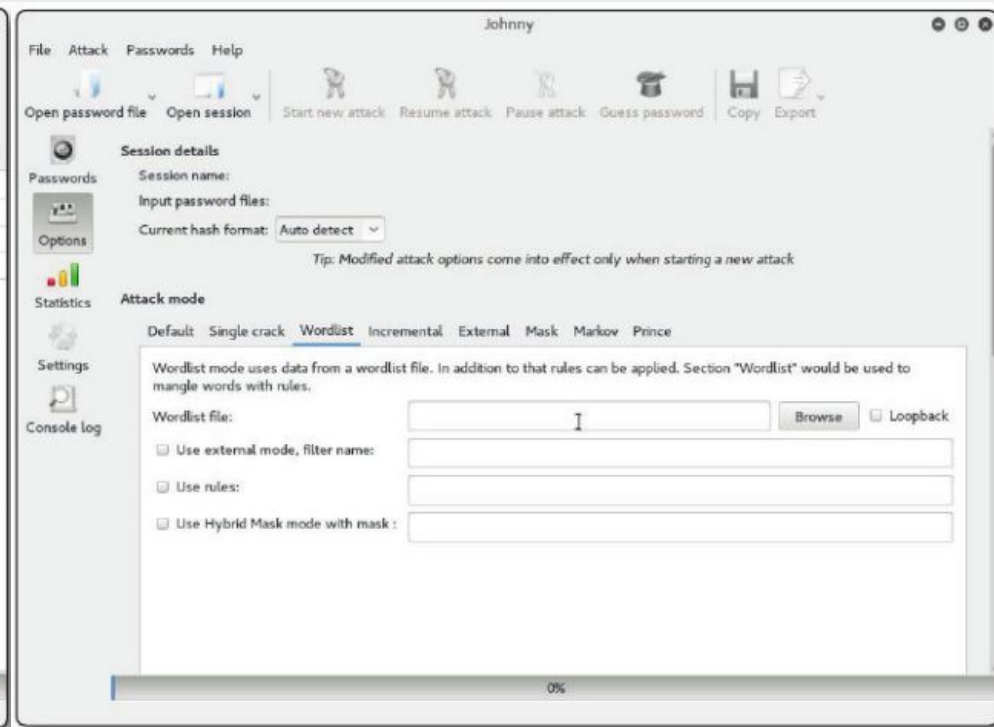
El modo por defecto hace primero el modo “Single Crack”, después el “Wordlist” y finalmente el “Incremental”. Se puede alterar el comportamiento de estos modos, y especificar modos adicionales. Si entramos en “Single Crack” vemos las opciones de este modo.



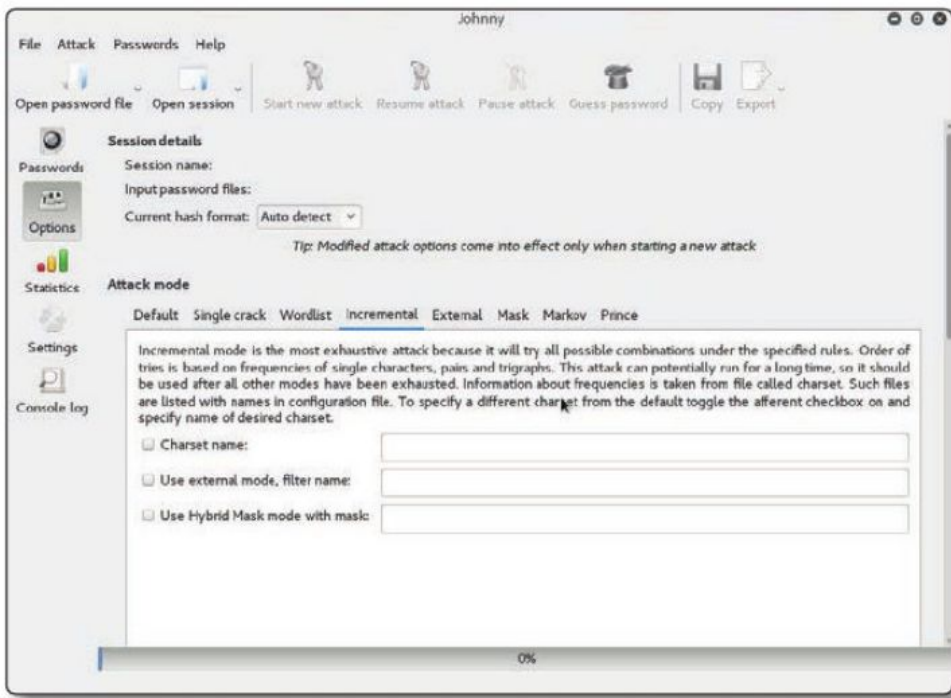
Ventana que aparece al ejecutar “johnny”



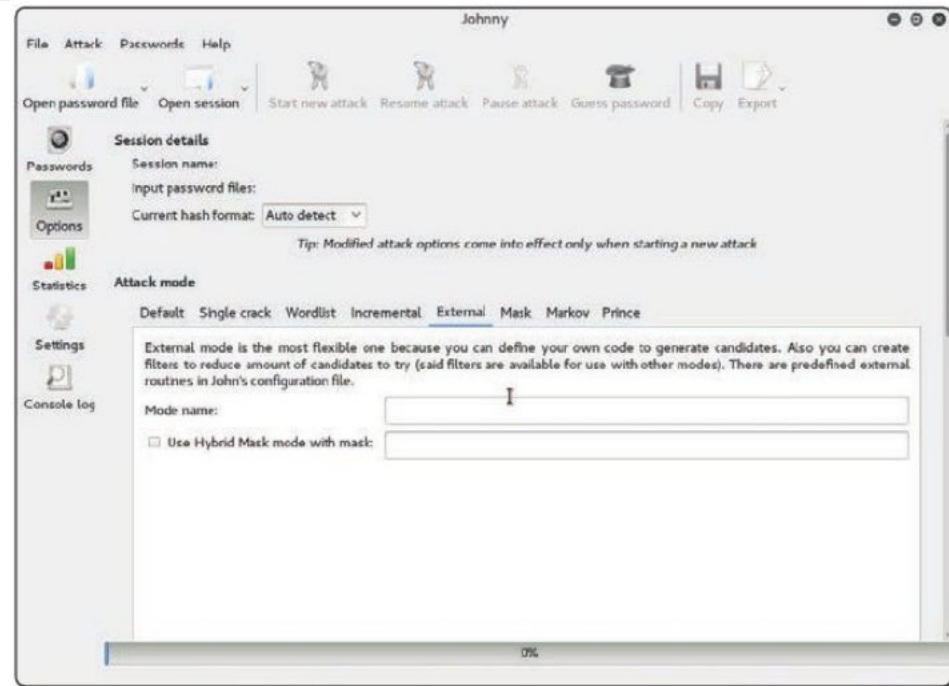
Permite que caigan las claves más fáciles de forma casi instantánea



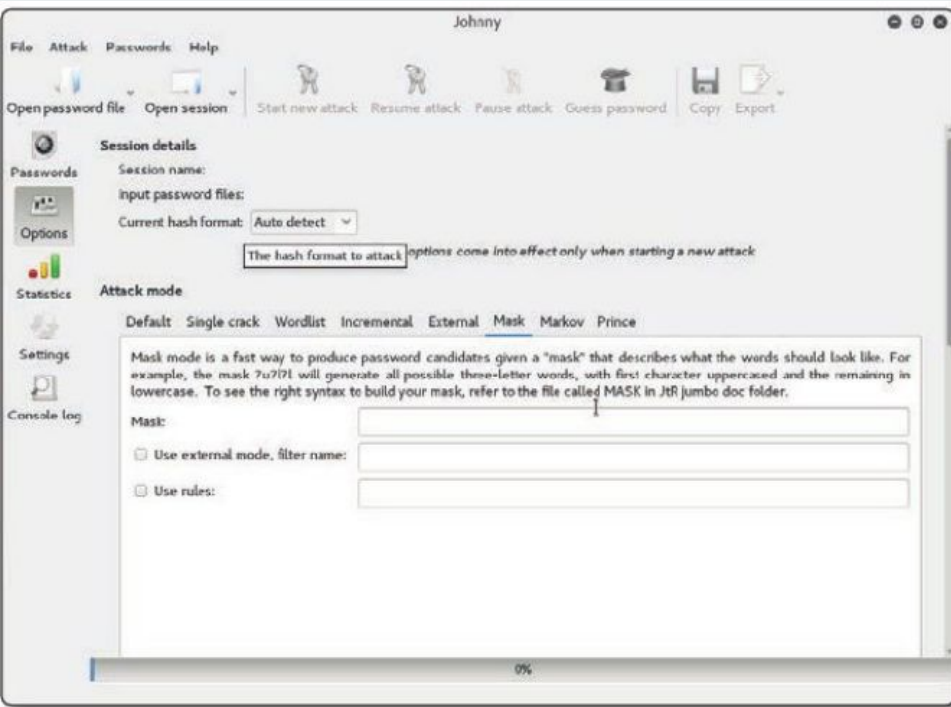
El modo Wordlist es un modo diccionario, pudiendo seleccionar diccionarios externos, y reglas sobre los diccionarios



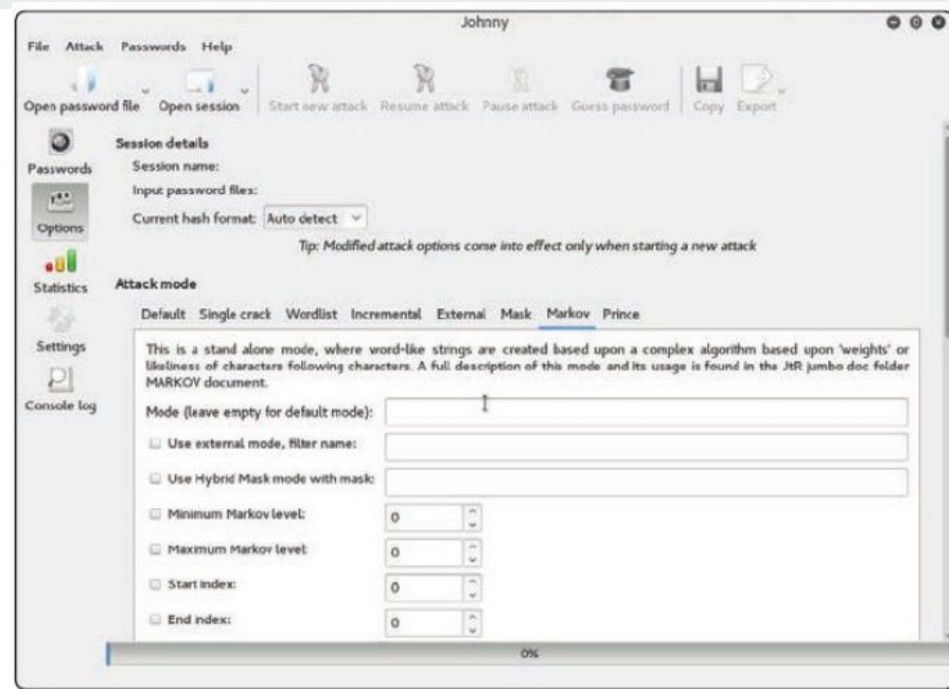
El modo Incremental corresponde con la fuerza bruta, pudiendo aplicar máscaras, filtros y qué juegos de caracteres vamos a utilizar.



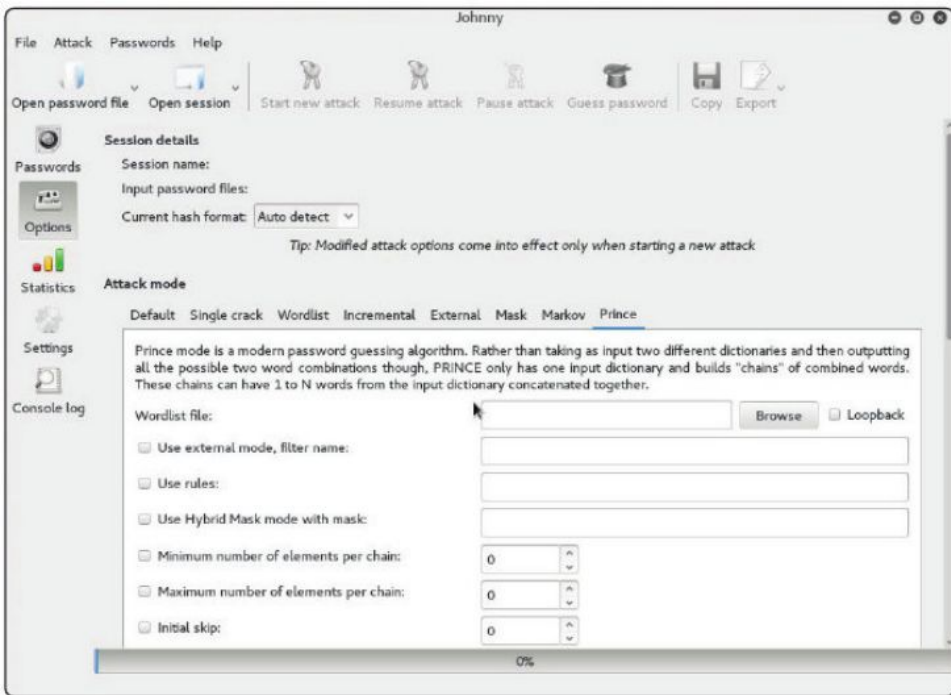
Podemos incluir nuestros propios generadores, programados por nosotros.



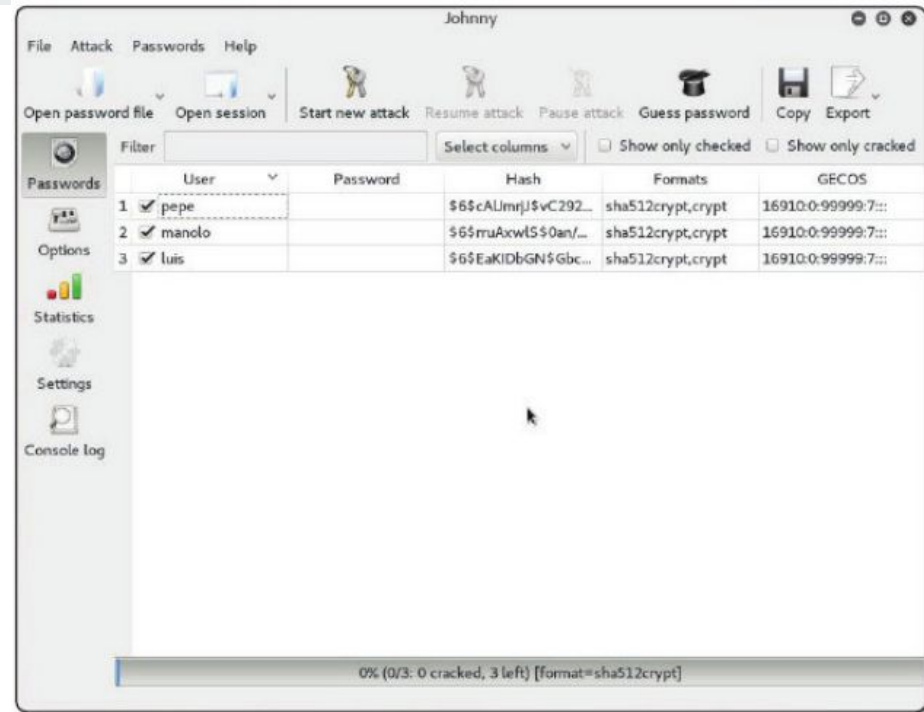
Tenemos un modo de máscara, útil cuando hemos “pescado” unos caracteres al ver teclear la clave, pero no los tenemos todos



Tenemos un modo predictivo, basado en cadenas de Markov, que funciona muy bien para claves “aparentemente” aleatorias pero tecleadas por un humano



Predicción de claves por PRINCE



Utilizar Johnny es tan simple como entrar en "File", seleccionar el chero con los hashes, y pulsar "Start new attack"



CAPÍTULO 6

AUDITORIAS A REDES WIFI



Auditorias a redes Wifi

- La auditoría de seguridad resalta la crítica importancia de examinar las redes Wi-Fi. Estas redes suelen albergar sistemas no reconocidos incluso por los administradores de sistemas, y una vez comprometidas, brindan acceso directo a la red interna sin atravesar firewalls.
- Aunque se aconseja diseñar las redes Wi-Fi como si estuvieran en la DMZ y emplear firewalls, en la práctica esto se realiza raramente.
- Las redes Wi-Fi presentan un alto potencial de vulnerabilidad, siendo susceptibles a ataques como envenenamiento o suplantación de puntos de acceso.
- Sin embargo, el enfoque central de esta auditoría se concentra en probar lo más esencial: obtener la clave de la red Wi-Fi.



WifiAuditor

- En domicilios particulares, es común que la configuración predeterminada del router y la contraseña no se modifiquen.
- Una estrategia inicial es buscar routers Wi-Fi con las claves "de fábrica". Aunque este método no suele ser efectivo, cuando lo es, la relación entre costo y resultado lo hace muy beneficioso.
- Dado que las WPA suelen tardar en caer aún con las claves por defecto, es una buena idea intentar este paso.
- Wi-Fi Auditor es un programa para ordenadores que realizan estas pruebas, además es fácil de instalar y ejecutar.



WifiAuditor

- La página de WiAuditor es:

`http://www.wiauditor.net/`

- WiAuditor está en Java, por lo que podremos ejecutarlo sin problemas nada más descargarlo si tenemos una máquina virtual Java. Lo podemos descargar desde:

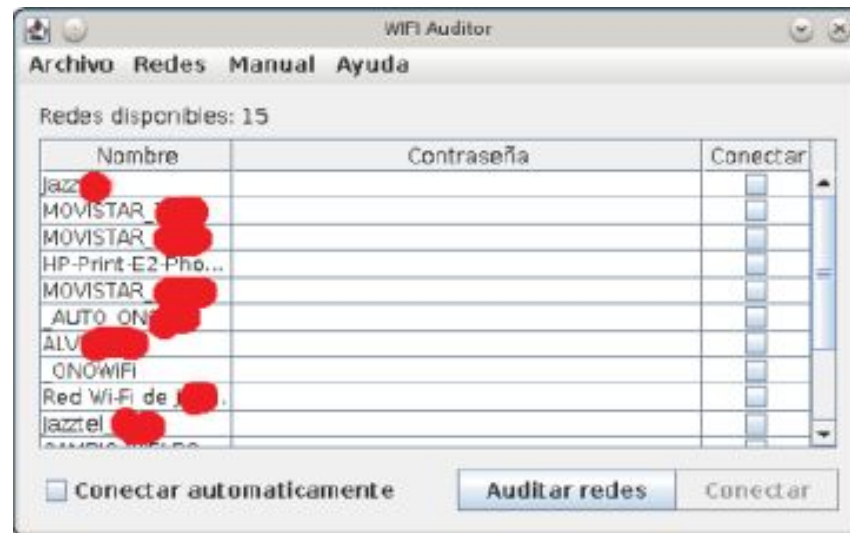
`http://wiauditor.net/WIFIAuditor.jar`

- Y lo lanzamos con:

`java -jar WIFIAuditor.jar`

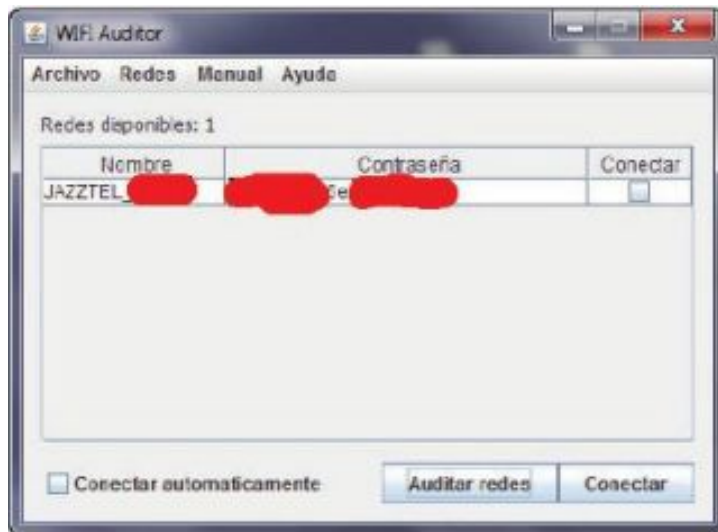
WifiAuditor

- Obteniendo una lista de redes:



WifiAuditor

- Seleccionamos una de las redes, y puede ocurrir que obtengamos la clave:



WifiAuditor

- O que no haya suerte, y la red en concreto ya no utilice la clave de fábrica:





WifiAuditor

- WifiAuditor está especializado en routers ADSL o de cable con Wifi.
- No hace fuerza bruta, ni tiene tabla rainbow. Ni siquiera técnicamente podemos deducir que se trate de ataque de diccionario de claves.
- Se limita a listar las redes que ha encontrado, a partir del nombre de la red deducir el proveedor, y a partir del proveedor, el nombre de la red y la MAC del router generar la clave por defecto que ha utilizado el proveedor de Internet en ese router concreto.
- En este análisis puede caer la red de una microPYME. Las empresas medianas, o las pequeñas que no tienen personal especializado, también pueden caer.
- Una empresa grande también puede caer, pero debido a que se puede colocar un router ADSL viejo para mayor cobertura en cascada vía Ethernet con la red principal.

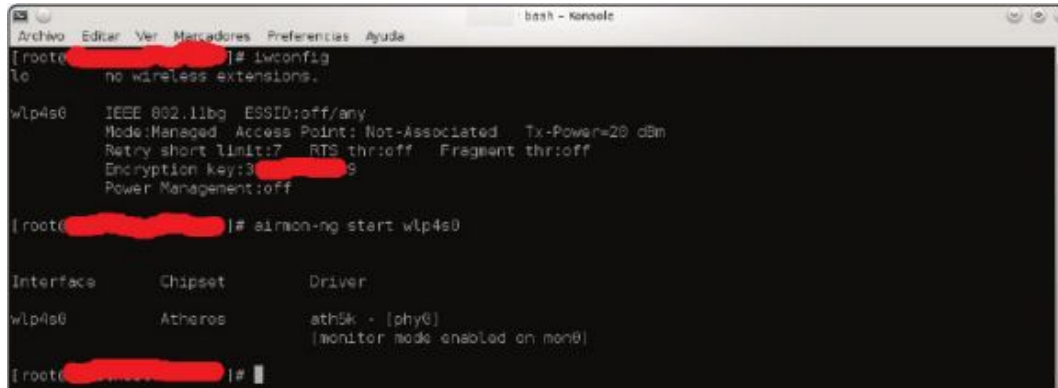


Cifrado WEP

- Es el sistema de cifrado que se ha utilizado tradicionalmente para hacer seguras las redes Wifi.
- Existen administradores de sistemas que no conocen la diferencia entre WEP y WPA.
- El cifrado WEP ya ha sido comprometido, por lo que no es seguro.
- Se ataca por simple observación –es decir, extrayendo los suficientes paquetes, el protocolo cae.

Cifrado WEP

- El primer paso es identificar las tarjetas Wi-Fi disponibles utilizando el comando `iwconfig`. Se selecciona la tarjeta deseada, y se inicia el modo monitor con `airmon-ng start dispositivo`.



```
Archivo Editor Ver Marcadores Preferencias Ayuda
[roote@redacted]# iwconfig
lo        no wireless extensions.

wlp4s0    IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:3[redacted]
          Power Management:off

[roote@redacted]# airmon-ng start wlp4s0

Interface  Chipset      Driver
wlp4s0     Atheros     ath5k - [phy0]
           |monitor mode enabled on mon0

[roote@redacted]#
```

- Se deben tener precauciones con los procesos en conflicto y, si es necesario, cambiar la dirección MAC del monitor.

Cifrado WEP

- Luego, se realiza un escaneo de redes disponibles con airodump-ng interfaz y se identifican BSSID y canales de interés.

```
CH 13 [| Elapsed: 20 s [| 2016-04-24 21:56

BSSID          PwR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
[redacted] 77 -85 205 18 0 3 54e WEP WEP [redacted]
[redacted] :B2 -89 2 1 0 1 54e WPA CCMP PSK [redacted]
[redacted] :48 -100 41 4 0 3 54e WPA2 COMP PSK [redacted]

BSSID          STATION          PwR  Rate  Lost  Frames  Probe
(not associated) [redacted] :B0 -04 0 - 1 0 4 [redacted]
(not associated) [redacted] :B0 -101 0 - 1 0 1 [redacted]
[redacted] :B2 [redacted] :B0 -83 0 - 1 458 7
[redacted] :B2 [redacted] :B0 -83 0 - 1 0 7

[root@ [redacted] ]#
```

- Se detiene cuando aparece la red objetivo.

Cifrado WEP

- A continuación, se inicia la captura de paquetes con airodump-ng -c canal -w archivo --bssid dirección interfaz.

```
CH 3 ][ Elapsed: 29 s ][ 2016-04-24 21:59 ][ fixed channel non0: -1
BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
[redacted] :77 -85 108    221    19   0   3  54e  WEP  WEP   Jac [redacted]
BSSID          STATION          PWR  Rate  Lost  Frames  Probe
```

- En un nuevo terminal, se asocia la tarjeta de red al BSSID con aireplay-ng -l 6000 -a BSSIDmac -h miMAC interfaz. Se acelera el proceso con aireplay-ng -2 -p 0841 -c FF:FF:FF:FF:FF:FF -b BSSIDmac -h miMAC interfaz.

```
[root@ [redacted]]# aireplay-ng -l 6000 -a [redacted] -h 00:11:22:33:44:55 non0
20:44:48 Waiting for beacon frame (BSSID: [redacted] on channel 1)
20:44:49 Sending Authentication Request (Open System)
20:44:49 Authentication successful
20:44:49 Sending Association Request
20:44:49 Association successful :-| (AID: 1)[]
```

Cifrado WEP

- Luego, se ataca la red con la opción `aireplay-ng -2` y se aprovechan los paquetes útiles. Se utiliza `aircrack-ng -z nombredelared*.cap` para intentar descifrar la clave utilizando los archivos generados. En caso de insuficientes IVs, se espera a obtener más con `airodump-ng`. El ataque se repetirá hasta obtener la clave.

```
[02:34:54] Tested 627489 keys (got 55118 IVs)

KB  depth  byte(vote)
0   0/ 1    (78080) (66304) (62976) (62720) (62464)
1   0/ 1    (72960) (64512) (63744) (62720) (62288)
2   0/ 2    (66560) (66560) (64768) (64256) (64256)
3   0/ 1    (79616) (66816) (64000) (64000) (63488)
4   0/ 2    (65280) (64256) (63232) (63232) (63232)
5   0/ 1    (76288) (66560) (60304) (65280) (65280)
6   0/ 1    (72192) (64256) (63744) (63488) (63232)
7   0/ 1    (72784) (60304) (64768) (64768) (64768)
8   0/ 2    (68352) (66816) (65536) (65824) (64512)
9   0/ 1    (68688) (64000) (63488) (63488) (62976)
10  0/ 1    (67328) (67328) (60304) (66948) (66948)
11  1/ 1    (66948) (65280) (64256) (64256) (63488)
12  1/ 2    (64444) (63700) (63220) (62420) (62368)

KEY FOUND! [XXXXXXXXXXXXXXXXXXXX]
Decrypted correctly: 100%
```



WPA/WPA2

- WPA y WPA2 son protocolos de seguridad recomendados para redes Wi-Fi, aunque no son invulnerables.
- A diferencia de WEP, suelen ofrecer mayor resistencia a ataques, especialmente en tipos de autenticación distintos al pre-shared key (PSK).
- No obstante, incluso redes seguras pueden ser vulnerables al ataque WPS (Wi-Fi Protected Setup), especialmente si algún punto de acceso tiene WPS activado.

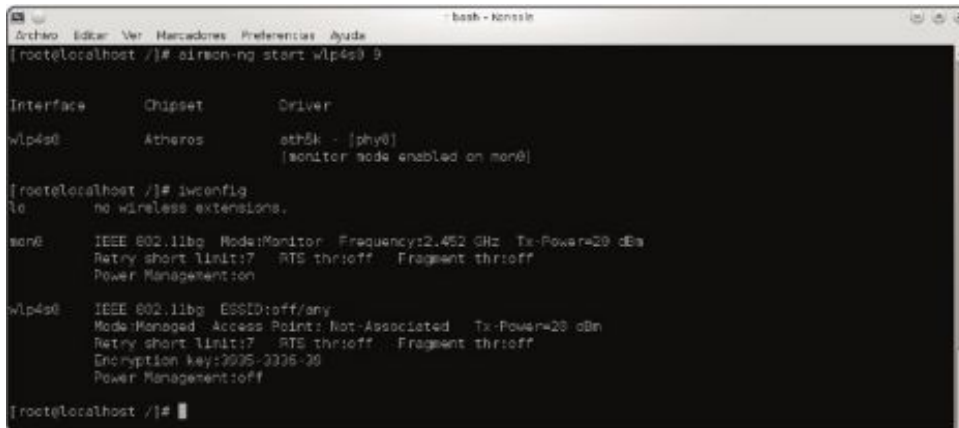


WPA/WPA2

- El ataque a WPS puede realizarse mediante herramientas como Reaver o Pixiewps, que aceleran el proceso de obtención de claves en ciertos casos.
- Si no hay soporte para WPS, se analiza el cifrado de la red.
- A diferencia de WEP, no se pueden aprovechar las debilidades de diseño de WPA o WPA2 para inyectar paquetes y acelerar el proceso de obtención de claves.
- En este caso, se recurre a ataques de fuerza bruta, diccionario de claves o tablas rainbow.

WPA/WPA2

- Se inicia el proceso deteniendo la interfaz actual con el comando `airmon-ng stop ath0`. Luego, se identifica el nombre del interfaz Wi-Fi mediante `iwconfig` y se arranca el modo monitor con `airmon-ng start interfaz 9`. Se verifica que se ha ingresado al modo monitor.



```
Archivo Editor Ver Marcadores Preferencias Ayuda
[root@localhost ~]# airmon-ng start wlan0 9

Interface      Chipset      Driver
wlan0          Atheros      ath9k - (phy0)
               (monitor mode enabled on wlan0)

[root@localhost ~]# iwconfig
lo                no wireless extensions.

wlan0 IEEE 802.11bg Mode:Monitor Frequency:2.452 GHz Tx-Power=20 dBm
      Retry short limit:7 RTS thr:off Fragment thr:off
      Power Management:on

wlan0 IEEE 802.11bg ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry short limit:7 RTS thr:off Fragment thr:off
      Encryption key:2036-3336-30
      Power Management:off

[root@localhost ~]#
```

WPA/WPA2

- El siguiente paso consiste en realizar un volcado de información utilizando airodump-ng interfazmonitor. Se espera un tiempo para observar las redes disponibles, prestando atención a aquellas con autenticación vía PSK y clientes conectados.

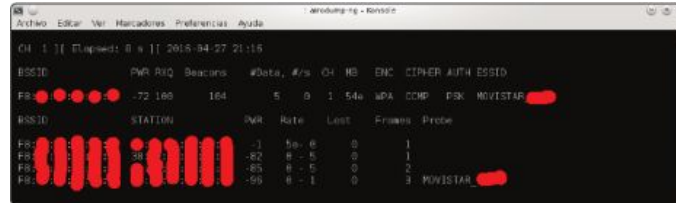
```
airodump-ng - Kismet
CH 2 || Elapsed: 16 s || 2016-04-27 21:39

BSSID          PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
-73 28 21 0 1 54w WPA COMP PSK MINISTAR
-80 27 1 0 1 54w WPA COMP PSK MINISTAR
-85 25 0 0 11 54w WPA COMP PSK TP-LINK_Extender
-87 23 0 0 11 54w WPA COMP PSK MINISTAR
-91 17 0 0 9 54w WPA2 COMP WEP
-92 22 0 0 9 54w WPA2 COMP PSK
-88 21 0 0 9 54w WPA
-90 19 1 0 11 54w WPA2 COMP PSK MINISTAR
-89 19 0 0 11 54w WPA COMP PSK MINISTAR
-93 18 0 0 6 54w WPA2 COMP PSK
-92 20 0 0 6 54w WPA2 COMP PSK
-93 26 4 0 3 54w WEP WEP
-99 19 0 0 1 54w WPA2 COMP PSK MINISTAR
-100 18 0 0 3 54w WPA
-100 2 0 0 4 54w WPA2 COMP WEP

BSSID          STATION          PWR Rate Lost Frames Probe
[not associated] -99 0 - 1 0 1
[not associated] -87 0 - 1 0 2
[not associated] -100 0 - 1 22 4
FR -82 0 - 5 0 4 MINISTAR
FR -82 0 - 5 0 4 MINISTAR
FR -92 5w-5w 0 21
-106 0 - 1 0 1
-1 1 - 0 0 1
-1 1 - 0 0 1
```

WPA/WPA2

- Se seleccionan las redes objetivo y se lanza el programa de volcado con `airodump-ng -c 1 --bssid macBSSID -w le interfazmonitor`.



```
airdump-ng - Kinsito
AirMin  Edit  Ver  Marcadores  Preferencias  Ayuda
CH: 1 | Elapsed: 0 s | 2018-04-27 21:18
BSSID      PWR  RX  Beacons  #Data  #rx  CH  HB  ENC  CIPHER  AUTH  SSID
F8:8E:8E:8E:8E:8E -72 160 164      5    0  1  54e WPA  COMP  PSK  MOVISTAR
BSSID      STATION  PWR  Rate  Lost  Frames  Probe
F8:8E:8E:8E:8E:8E 34  -82  8 - 5  0  1
F8:8E:8E:8E:8E:8E 34  -85  8 - 5  0  2
F8:8E:8E:8E:8E:8E 34  -96  8 - 1  0  3  MOVISTAR
```

- Después de identificar clientes conectados, se elige uno y se procede a desconectarlo de la red con `aireplay-ng -o 1 -a macBSSID -c macCliente interfazmonitor`.



```
bash - Kinsito
AirMin  Edit  Ver  Marcadores  Preferencias  Ayuda
[root@localhost ~]# aireplay-ng -o 1 -a F8:8E:8E:8E:8E:8E -c 30:8E:8E:8E:8E:8E -w le interfazmonitor
21:20:00 Waiting for beacon frame (BSSID: F8:8E:8E:8E:8E:8E) on channel 1
21:20:01 Sending 64 directed DeAuth. STXAC: [38:8E:8E:8E:8E:8E] [0[64 ACKs]
[root@localhost ~]#
```

WPA/WPA2

- Finalmente, se realiza el ataque con *aircrack-ng* utilizando un diccionario de claves. Se puede emplear diccionarios como *rockyou* o descargar otros desde fuentes externas. Se eliminan duplicados del diccionario para acelerar el proceso con `sort diccionario | uniq -u > diccionarioU`. Luego, se ejecuta el ataque con `aircrack-ng -w diccionario -b macBSSID file*.cap`.
- El resultado puede ser la obtención exitosa de la clave, evidenciada por la detección del handshake en la salida de *airodump-ng*.

```
[root@localhost ~]# aircrack-ng -w password.lst -b F8: [REDACTED] file*.cap
Opening file-61.cap
No valid WPA handshakes found..

Quitting aircrack-ng...
[root@localhost ~]#
```

```
Aircrack-ng 1.2 rc1

[00:00:00] 232 keys tested (1459.54 k/s)

Current passphrase: [REDACTED]

Master Key   : 36 [REDACTED] 00
              2F 70 [REDACTED] 05 01

Transient Key : 89 [REDACTED] 87 BE EB 83 1C 8F C7 A8 F1 5D
              16 F0 [REDACTED] EF CF F0 7D 51 93 F4 97
              E4 E0 01 0B 0E 0F [REDACTED] 06 93 0A 64
              04 2E 9F 34 0C DC 71 6C 0A

EAPOL HMAC   : CF [REDACTED] A8 [REDACTED] 12

Passphrase not in dictionary
```



CAPÍTULO 7

AUDITORÍAS A

APLICACIONES WEB



Auditorías a Aplicaciones Web

Las auditorías a aplicaciones web tienen dos enfoques:

- Identificar software instalado y si no está actualizado, aplicar las vulnerabilidades conocidas.
- Conocidas determinadas vulnerabilidades, intentar identificar si en algún momento el sitio web es vulnerable.

El primer enfoque es el más barato y el segundo es más exhaustivo, pero supone auditar mucho código. El primer enfoque es el más utilizado.



Inyección SQL

Consiste en concatenar variables sin verificar su contenido, aprovechando errores de programación. Por ejemplo: Concatenar una variable no validada en una sentencia SQL, permitiendo ataques como la eliminación de tablas.

Suelen ocurrir en plugins mal programados y código propio apresurado. El objetivo principal es explorar bases de datos internas, no necesariamente sabotear, buscando acceso a información estratégica.

En código en producción, se filtran caracteres sensibles, pero aún pueden existir vulnerabilidades. La auditoría implica rastrear variables desde el código fuente para identificar posibles inyecciones SQL, utilizando expresiones regulares y verificando la concatenación de cadenas.



XSS (Cross-Site Scripting)

Vulnerabilidad que permite la inserción de código, generalmente JavaScript, en sitios web remotos. Requiere sólidos conocimientos de programación web y JavaScript para su explotación efectiva.

Aprovecha la confianza predeterminada del servidor en su propio contenido. Permite ejecutar código no propio para extraer y manipular información, eludiendo restricciones de interfaz.

Útil para obtener listados de usuarios, volcados de tablas y enviar correos con información. Utiliza tags como script e iframe, atributos como behavior de STYLE de FK, y AJAX para introducir objetos XMLHttpRequest. La detección se puede realizar mediante el uso de proxys inversos, especialmente para código HTML o JavaScript empotrado.



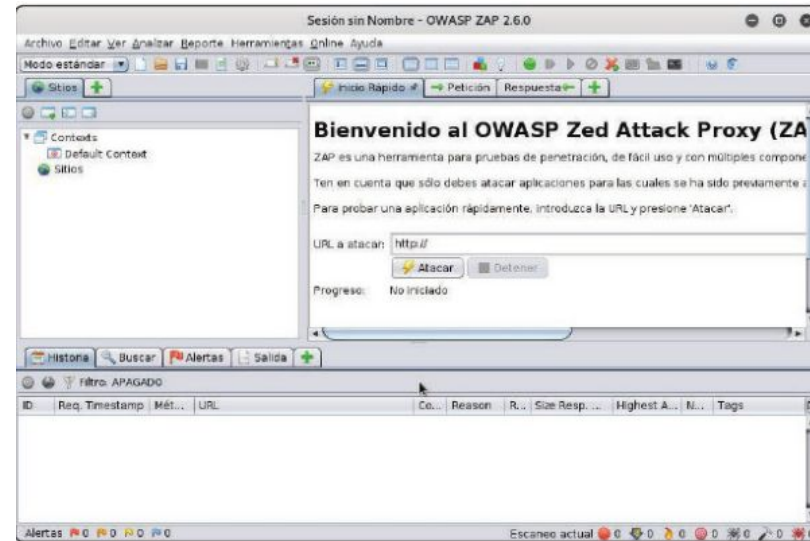
Inclusión de archivos locales

Similar a la inyección SQL, se aprovecha de parámetros sin filtrar en la manipulación de archivos. Permite acceder a archivos locales y obtener información sensible, como configuraciones de base de datos, al explotar parámetros en GET, POST o cookies.

Incluye técnicas como la Path Traversal, que utiliza trucos distintos para extraer archivos. También implica la inclusión de archivos remotos para acceder a recursos externos.

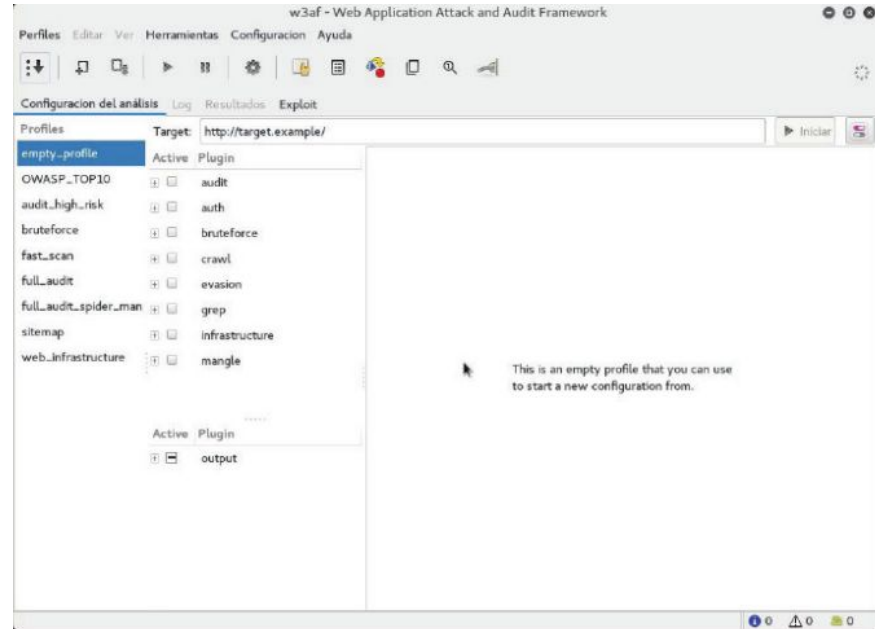
OWASP Zed Attack Proxy

Es una herramienta de auditoría de sitios web, que nos permite detectar vulnerabilidades comunes, posee escáneres pasivos y activos, entre otras funciones dispone de proxy inverso y fuzzing (alimentar la aplicación web con datos extraños y ver cómo se comporta).



W3AF

Es una herramienta enfocada a auditar y explotar las vulnerabilidades web. Es conceptualmente bastante parecida a ZAPProxy. Trae un conjunto de exploits que podemos validar contra una vulnerabilidad encontrada



NIKTO

Es una herramienta en consola para analizar las vulnerabilidades de un servidor

nikto -h servidor

```
root@kali:~# nikto -h www.peritoeninformatica.pro
- Nikto v2.1.6
-----
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: 80
+ Start Time: [REDACTED]
-----
+ Server: lighttpd/1.4.31
+ Retrieved x-powered-by header: PHP/5.4.45-0+deb7u2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, GET, HEAD, POST
+ OSVDB-12184: ??-PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: ??-PHPF9568F36-D428-11d2-A769-90AA601ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: ??-PHPF9568F34-D428-11d2-A769-90AA601ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: ??-PHPF9568F35-D428-11d2-A769-90AA601ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ 7668 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time: 2016-04-21 14:18:25 (GMT0) (625 seconds)
-----
+ 1 host(s) tested
```

Es una aplicación que realiza tests de penetración en sistemas web vía inyecciones SQL. Los parámetros de uso son:

- -u URL: página web objetivo.
- -p: parámetro vulnerable.
- -dbs: muestra el nombre de todas las bases de datos.
- -D: selecciona el nombre de la base de datos a la que queremos hacer las consultas.
- -tables: muestra el nombre de las tablas en la base de datos seleccionada.
- -T: muestra el nombre de la tabla en la que se realizarán las consultas.
- -columns: muestra el nombre de las columnas de la tabla seleccionada.
- -dump: extrae los datos de la tabla seleccionada a un fichero CSV.
- -dbms: permite seleccionar el sistema gestor de bases de datos, si es conocido.

```

root@kali:~# sqlmap -u http://10.10.10.10:8080/
[1] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
[1] user's responsibility to take all applicable local, state and federal laws. Developers assume no liability and
[1] are not responsible for any misuse or damage caused by this program.
[*] starting at 19:29:51

[19:29:51] [INFO] testing connection to the target IP
sqlmap got a 301 redirect to 'http://10.10.10.10:8080/'. Do you want to follow? [Y/n] y
[19:29:56] [INFO] checking if the target is protected by some kind of waf/IPS/IDS
[19:29:57] [WARNING] reflective values found and filtering out
[19:29:57] [INFO] testing if the target URL is stable
[19:29:57] [INFO] [WARNING] GET parameter 'id' does not appear dynamic
[19:29:58] [INFO] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[19:29:58] [INFO] testing for SQL injection on GET parameter 'id'
[19:29:58] [INFO] testing AND boolean-based blind - WHERE or HAVING clause
[19:30:22] [INFO] testing MySQL >= 5.6 boolean-based blind - Parameter replace
[19:30:24] [INFO] testing MySQL >= 5.6 AND error-based - WHERE or HAVING clause
[19:30:26] [INFO] testing MySQL AND error-based - WHERE or HAVING clause
[19:30:39] [INFO] testing Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause
[19:30:51] [INFO] testing Oracle AND error-based - WHERE or HAVING clause
[19:31:02] [INFO] testing MySQL >= 5.6 error-based - Parameter replace
[19:31:03] [INFO] testing MySQL inline queries
[19:31:04] [INFO] testing PostgreSQL inline queries
[19:31:05] [INFO] testing Microsoft SQL Server/Sybase inline queries
[19:31:06] [INFO] testing MySQL > 5.0.11 stacked queries (SELECT 'comment')
[19:31:09] [CRITICAL] could not login but logging has been disabled (connection refused). Please use --log-value
[19:31:10] [INFO] testing PostgreSQL >= 8.3 stacked queries (comment')
[19:31:11] [INFO] testing PostgreSQL >= 8.3 stacked queries (comment')
[19:31:12] [INFO] testing Microsoft SQL Server/Sybase stacked queries (comment')
[19:31:38] [INFO] testing Oracle stacked queries (DENSE_RANK RECEIVED MESSAGE 'comment')
[19:31:52] [INFO] testing MySQL >= 5.0.12 AND time-based blind (SELECT)
[19:31:49] [INFO] testing PostgreSQL >= 8.1 AND time-based blind
[19:31:47] [INFO] testing Microsoft SQL Server/Sybase time-based blind
[19:32:00] [INFO] testing Oracle AND time-based blind
[19:32:08] [INFO] testing Generic UNION query (NULL - 1 to 10 columns)
[19:32:08] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can
[19:32:09] [INFO] try to explicitly set it using opt --dbms=MySQL or --dbms=MSSQL or --dbms=Oracle
[19:32:09] [INFO] testing MySQL UNION query (NULL - 1 to 10 columns)

```

WAPITI

Es un potente escáner de vulnerabilidades que identifica los siguientes errores:

- XSS
- Inyecciones de base de datos(Inyeccion SQL, XPATH y PHP, JSP yASP)
- Inyección LDAP
- Errores en la gestión de ficheros –fopen, readle, include–
- Detección de ejecución de comandos –eval, system, passtru–
- Inyección CRLF –jación de sesión, HTTP RS–

Wapiti puede ser sensiblemente lento en webs muy grandes, como instalaciones funcionales de Woocommerce. Pero aún así, es bastante interesante su uso

```
root@kali:~# wapiti www.owasp.org
Wapiti-2.3.0 (wapiti.sourceforge.net)

Note
=====
Este escaneo se ha guardado en el archivo /root/.wapiti/scans/www.owasp.org.xml
Puedes usarlo para realizar ataques sin escanear de nuevo el website mediante el parámetro "-k"
(*) Cargando módulos:
    mod_crlf, mod_exec, mod_file, mod_sql, mod_xss, mod_backup, mod_htaccess, mod_blindsql, mod_permanentx
s, mod_nikto

[+] Lanzando módulo exec
[+] Lanzando módulo file
[+] Lanzando módulo sql
[+] Lanzando módulo xss
[+] Lanzando módulo blindsql
[+] Lanzando módulo permanentxss

Informe
=====
Se ha generado un informe en el fichero /root/.wapiti/generated_report
Abrir /root/.wapiti/generated_report/index.html con el navegador para ver el informe
```

WPSCAN

Es un escaner de plugins, temas y vulnerabilidades de ambos para Wordpress, que es bastante potente y sencillo de usar. Su sintaxis básica es:

wpscan --url dominio

Donde dominio es el dominio que queremos analizar.

```
root@kali:~# wpscan --url [redacted]

WPSCAN

WordPress Security Scanner by the WPScan Team
Version 2.9
Sponsored by Sucuri - https://sucuri.net
@_WPScan_, @ethicalhack3r, @enwan_lr, pvd1, @_FireFart_

[!] It seems like you have not updated the database for some time.
y
[+] Updating the Database ...
[+] Update completed.
[+] URL: http://[redacted]
[+] Started: Tue Apr 19 19:30:00 2016

[+] The WordPress 'http://[redacted]/readme.html' file exists exposing a version number
[+] Full Path Disclosure (FPD) in 'http://[redacted]/wp-includes/rss-functions.php':
[+] Interesting header: LINK: <http://[redacted]/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: SERVER: lighttpd/1.4.31
[+] Interesting header: X-POWERED-BY: PHP/5.4.45-8+deb7.2
[+] XML-RPC Interface available under: http://[redacted]/xmlrpc.php

[+] WordPress version 4.4.2 identified from meta generator
[+] WordPress theme in use: zerif-lite - v1.8.4.0

[+] Name: zerif-lite - v1.8.4.0
| Latest version: 1.8.4.0 (up to date)
| Location: http://[redacted]/wp-content/themes/zerif-lite/
| Readme: http://[redacted]/wp-content/themes/zerif-lite/readme.txt
```



Otras Aplicaciones

Hay muchas más aplicaciones para auditorías de aplicaciones web. Estas son:

De base de datos:

- bbsql
- sqlinja
- sqlsus

De identificación de CMS:

- blindElephant
- plecost

De identificación de IDS:

- ua-tester

Indexadores web:

- dirb
- dirbuster
- webscarab

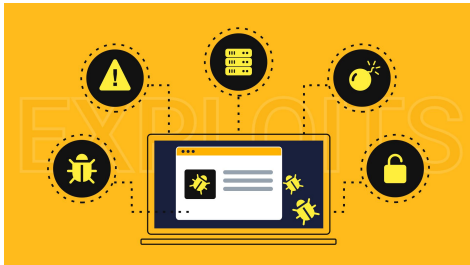


CAPÍTULO 8

METASPLOIT

Conceptos Previos

- Un exploit es un código que aprovecha un agujero de seguridad preexistente para ejecutar código no autorizado.
- El payload es el código que se quiere ejecutar con el exploit.
- Un exploit puede ser local o remoto.
- Hay muchos exploits conocidos y documentados, pero también existen exploits 0-day que aún no son conocidos por la comunidad de seguridad informática.





Qué es Metasploit

- Metasploit es un framework para pentesting que incluye herramientas para cubrir todo el proceso de auditoría proactiva de seguridad del sistema.
- Metasploit tiene fama de ser complejo de usar, ya que no tiene un bonito menú desplegable ni muchos botoncitos para hacer cosas.
- Metasploit está pensado para que alguien que sabe, pueda utilizar la herramienta sin problemas y pueda hacer todas las tareas de auditoría desde el propio programa.



Partes de Metasploit

- Metasploit es una suite completa que incluye una base de datos de exploits y de payloads, así como una serie de utilidades para aplicarlos.
- Las utilidades más importantes de Metasploit son: msfconsole, msfgui, msfd, msfcli, msfupdate, msfbinscan, msfpayload, msfencode, msfvenom y msfpescan.
- Metasploit también se puede utilizar desde msfgui, o con aplicaciones como Armitage que se integran con Metasploit.

Utilidad	Descripción
msfconsole	Consola de línea de comandos para ejecutar módulos y mandar órdenes a Metasploit.
msfgui	Interfaz gráfica de usuario con funcionalidad equivalente a la consola msfconsole.
msfd	Daemon de Metasploit que permite lanzar las órdenes a Metasploit desde una máquina remota.
msfcli	Utilidad para lanzar módulos.
msfupdate	Actualiza la base de datos de exploits, los módulos y la funcionalidad de Metasploit.
msfbinscan	Auditoría dentro de ejecutables. Búsqueda de instrucciones de salto y sobre la pila.
msfpayload	Generación de shellcodes en varios lenguajes de programación. Generación de shellcodes empotradas en ejecutables de varios sabores de Unix y versiones de Windows.
msfencode	Ofusca el código de la shellcode contra antivirus y sistemas IDS.
msfvenom	Implementa la funcionalidad de las utilidades ya comentadas msfpayload y msfencode.
msfpescan	Análisis de las DLL, y generación de direcciones de retorno para las shellcode.




Meterpreter

- Meterpreter es un troyano completo que permite tomar el control remoto de una máquina.
- Desde Meterpreter, se puede acceder a información sensible, escalar privilegios y realizar ataques.
- En un sistema Unix bien configurado, Meterpreter puede obtener privilegios de usuario efectivo.
- En sistemas Windows, Meterpreter puede obtener privilegios completos de administración.
- Meterpreter es una herramienta muy potente que puede utilizarse para causar daños significativos.



CAPÍTULO 9

ADVERTENCIA LEGAL

- 
- Kali Linux es una herramienta al borde de lo legal, por lo que tiene que ser usada con responsabilidad.
 - El uso de Kali linux en situaciones en las que no se pueda justificar su uso tiene sanciones legales como :
 - Años en prisión.
 - Multas económicas.
 - Su uso en ambiente profesional tiene que contar con la respectiva documentación y autorización para realizar las auditorías.
 - Las sanciones varían su severidad de acuerdo a la normativa de cada país.



CAPÍTULO 10

ANÁLISIS FORENSE CON

KALI

ANÁLISIS FORENSE CON KALI

Al arrancar, Kali ofrece un modo forense “Live”
–Live (forensic mode)–

En modo forense, Kali no monta automáticamente ningún medio de almacenamiento distinto que el propio disco de arranque.

Esto incluye discos duros internos, y particiones swap –que, por defecto, todas las distribuciones montan habitualmente–.

No se activa la red por defecto, debiendo activarse a mano.

La clave de root de la distribución en Live es toor.





10.1 USO DE KALI EN ANÁLISIS FORENSE. CLONADO DE DISCOS

Introducción al Clonado de Discos en Análisis Forense:

- Tarea frecuente en trabajo forense.
- Evitar arrancar desde el disco duro analizado.

Comando DD para Clonado de Discos:

- Sintaxis: `dd conv=sync,noerror if=dispositivodisco of=cherosalida bs=tambloque`
- `conv=sync,noerror`: no parar al leer bloques erróneos, en cambio llenar de ceros.
- Acelerar el proceso con `tambloque`: `tambloque` es tamaño del bloque, leer de `tambloque` en `tambloque`.

Generación de la RMA MD5 y SHA512:

- MD5: `md5sum nombreimagen > nombreimagen.md5`.
 - `nombreimagen` nombre del fichero donde se grabará la imagen. MD5 es vulnerable a ataques de colisión de hash
- SHA512: `sha512sum nombreimagen > nombreimagen.sha512`.
 - Firmas SHA512 son largas, se suele firmar este fichero con MD5.



10.1 USO DE KALI EN ANÁLISIS FORENSE. CLONADO DE DISCOS

Problemas Comunes y Soluciones:

- El disco que se ha llevado para clonar es más pequeño que el disco a clonar, para ello se comprime la imagen
 - a. Comprimir imagen: `dd conv=sync,noerror if=dispositivodisco bs=tambloque | gzip -c > ficherosalida.gz.`
- Clonado a través de la red: cuando no se tiene acceso físicamente al disco
 - a. `nc -l -p puerto | dd conv=sync,noerror of=cherosalida.bz bs=tambloque`

10.2 USO DE KALI EN ANÁLISIS FORENSE. VISIÓN Y EDICIÓN DE IMÁGENES DE DISCO

Trabajo con Volcados de Discos Enteros:

Importancia de Volcados Completos:

- Se recomienda trabajar con volcados de discos enteros en lugar de volcados de particiones.
- Información forense crucial puede estar fuera de las particiones.

Desafíos del Montaje Directo:

- No es posible montar la imagen directamente debido a la necesidad de un paso intermedio. Para ello se usa kpartx

Uso de kpartx:

- `kpartx -a imagen.img` crea dispositivos loop en `/dev/mapper` para cada partición de la imagen.
- Facilita el montaje posterior de las particiones con `mount`.

```
loop1p1 : 0 7775397 /dev/loop1 63
loop1p3 : 0 16065 /dev/loop1 7775460
loop1p4 : 0 16065 /dev/loop1 7791525
```

Ver particiones con:
`kpartx -l imagenAnalisis.img`

```
control
loop0p1
loop0p3
loop0p4
```

Ver contenido del directorio `/dev/mapper`:
`ls -l /dev/mapper/`



10.3 USO DE KALI EN ANÁLISIS FORENSE. DATA CARVING

Una tarea frecuente es recuperar archivos de una imagen.

- Data carving o file carving busca archivos utilizando expresiones regulares que modele un tipo concreto de fichero, o su firma de cabecera, recorre toda la imagen del disco buscando esa expresión regular o esa firma de cabecera.
- Se suele usar scalpel pero suele fallar, entonces se usa foremost
- Foremost se ejecuta con la sintaxis “foremost -t tipo -i imagen -o salida”, donde tipo es el tipo de archivo a extraer.

Es importante que recordemos que el tipo lo debemos indicar sin el punto; es decir, si queremos extraer los archivos JPG, haremos:

- `foremost -t jpg -i imagen -o salida`

En lugar de:

- `foremost -t .jpg -i imagen -o salida`

Que no funcionará.



10.4 USO DE KALI EN ANÁLISIS FORENSE. OTRAS UTILIDADES

Otras utilidades que pueden ser interesantes para hacer un análisis forense y que son difíciles de encuadrar son:

- vol: análisis forense de memoria RAM y particiones de swap.
- xxd: permite generar volcados hexadecimales de ficheros binarios.
- pdfresurrect: permite hacer análisis forense sobre ficheros PDF.
- p0f: fingerprinting pasivo, para identificar ataques Man in the Middle.