Universidad Luterana Salvadoreña
Facultad de Ciencias del Hombre y la Naturaleza
Licenciatura en Ciencias de la Computación

Proyecto Kali PI

Integrantes:
Dennys Ernesto García Rivas
Jimmy Alexander García Rivas
Ronald Geovani Jorge Ortiz
Alex Jonathan Gutiérrez Girón
Jorge Alberto Barahona Portillo

Catedratico:
Jonathan Mejía

Introducción al Software Libre Ciclo 2-2017

Contenido

Objetivos

Objetivo General:

Introducirnos al software Libre a través de su uso, un uso más amplio, en este caso con Kali Linux, instalarlo en una Raspberry Pi 3 y utilizarlo guiándonos con los conocimientos adquiridos en clases.

Objetivos Específicos:

- Instalar kali Linux en Raspberry Pi.
- Conocer las herramientas de este sistema operativo.
- Utilizar la herramienta Zap para aprender a poder hacer auditorias web.

Introducción

El proyecto **Kali Pi**, consiste en instalar una una distro de Kali Linux en una Raspberry Pi 3, Raspberry Pi es un computador de placa reducida, computador de placa única o computador de placa simple de bajo costo desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas. El el proyecto ira dirigido a Kali Linux para explorar y probar sus funcionalidades, herramientas y diferentes usos que se le puede dar a este Software Libre. Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Kali Linux trae preinstalados más de 600 programas, pero para dispositivos como la Raspberry Pi 3 estas herramientas vienen un poco limitadas asi que en este proyecto se harán pruebas de auditoria usando el programa Zap de Owasp, que es El proyecto abierto de seguridad en aplicaciones Web OWASP por sus siglas en inglés es una comunidad abierta dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables. Todas las herramientas, documentos, foros y capítulos de OWASP son gratuitos y abiertos a cualquiera interesado en mejorar la seguridad de aplicaciones. En el trayecto del proyecto se aprende a utilizar esta herramienta muy útil para la seguridad web que además es es libre y usada en un sistema operativo libre como lo es Kali Linux.

Marco teórico

Kali Pi es un proyecto en el cual expandiremos nuestros conocimientos sobre software Libre, Hardware Libre y herramientas de las cual podemos hacer uso en este proyecto vamos a instalar el sistemas operativo Kali Linux en una minicomputadora que es la rraspberry Pi 3 y atravez de la herramienta libre Zap de Owasap vasmo hacer pruebas de vulnerabilidades, auditorias y pentesting cabe mencionar que todas estas pruebas son con fines educativos.

Raspberry Pi es un computador de placa reducida, computador de placa única o computador de placa simple (SBC) de bajo costo desarrollado en Reino Unido por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas.4567

Aunque no se indica expresamente si es hardware libre o con derechos de marca, en su web oficial explican que disponen de contratos de distribución y venta con dos empresas, pero al mismo tiempo cualquiera puede convertirse en revendedor o redistribuidor de las tarjetas RaspBerry Pi,8 por lo que da a entender que es un producto con propiedad registrada, manteniendo el control de la plataforma, pero permitiendo su uso libre tanto a nivel educativo como particular.

En cambio el software sí es open source, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian, aunque permite usar otros sistemas operativos, incluido una versión de Windows 10. En todas sus versiones incluye un procesador Broadcom, una memoria RAM, una GPU, puertos USB, HDMI, Ethernet (El primer modelo no lo tenía), 40 pines GPIO y un conector para cámara. Ninguna de sus ediciones incluye memoria, siendo esta en su primera versión una tarjeta SD y en ediciones posteriores una tarjeta MicroSD1910

La fundación da soporte para las descargas de las distribuciones para arquitectura ARM, Raspbian (derivada de Debian), RISC OS 5, Arch Linux ARM (derivado de Arch Linux) y Pidora (derivado de Fedora);2 y promueve principalmente el aprendizaje del lenguaje de programación Python.4 Otros lenguajes también soportados son Tiny.

En esta Minicomputadora instalamos Kali Linux, la primera vez nos vimos obligados a desinstalar y volver a instalar el sistema operativo por motivos de errores con los que no contábamos cabe resaltar que fueron fallas propias y no del sistema, ni del dispositivo.

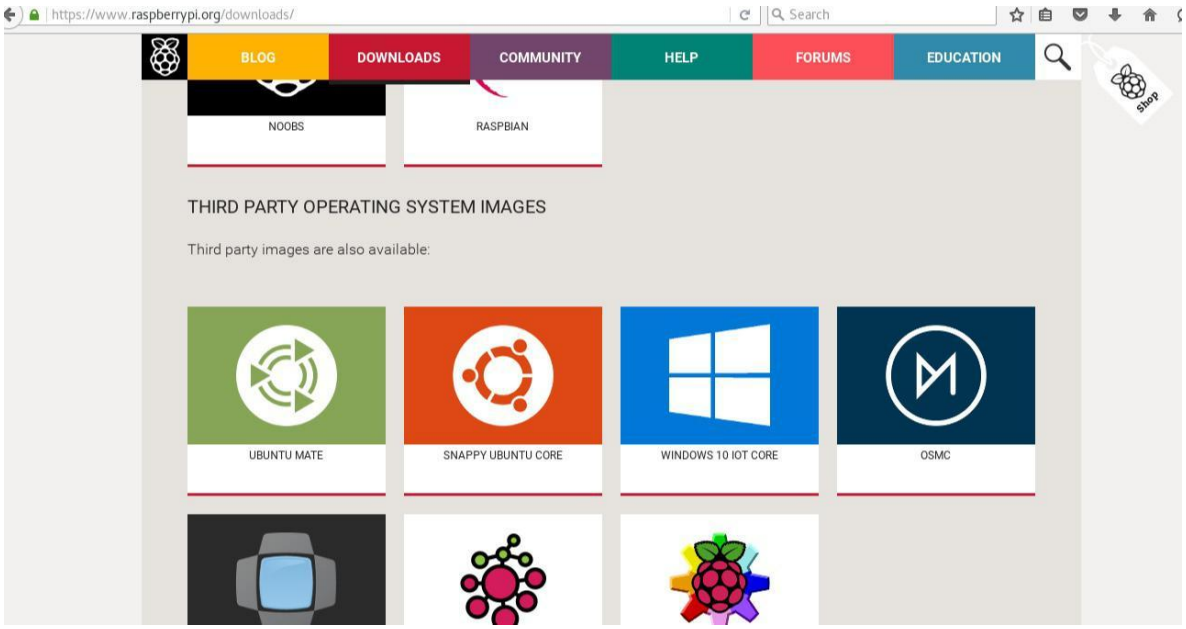
Pasos de Instalación de Kali Linux en Raspberry Pi 3

¿Cómo se instala?

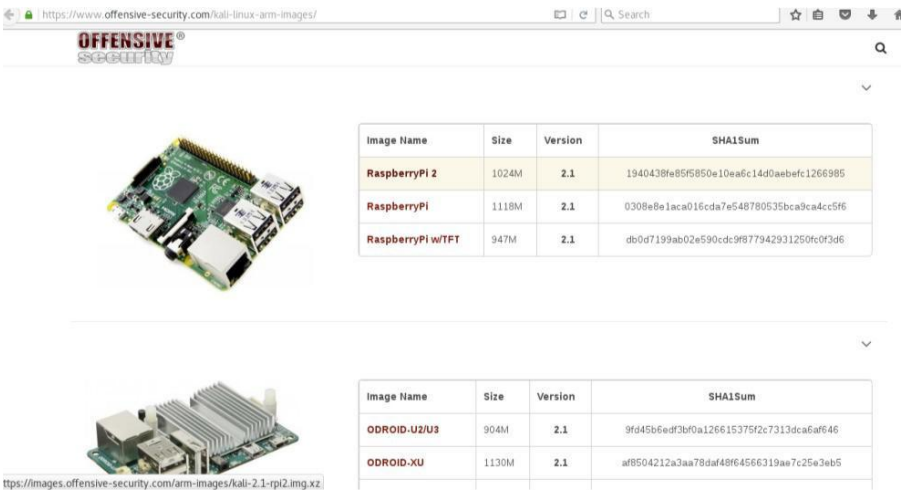
Podemos hacerlo por medio de linux, windows y Mac en mi caso mostrare en LINUX y WINDOWS.

1. Paso: Vamos a instalar Kali Linux pero también te ofrece muchos otros sistemas.

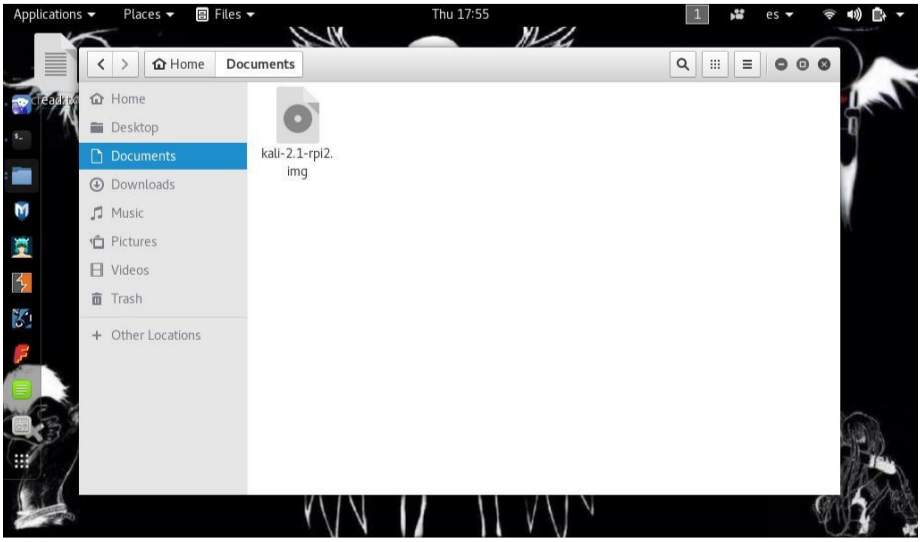
Link para página de rspberry pi https://www.raspberrypi.org/downloads/



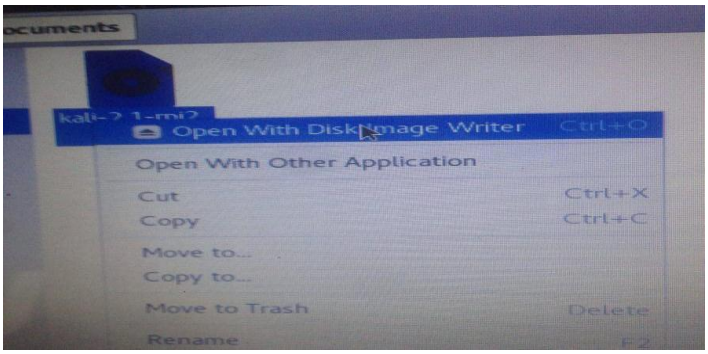
2. Paso: Vamos a descargar nuestro archivo .img.xz para subirlo a nuestro SD vamos a ir a Offensive Security
   Link de Offensive Security https://www.offensive-security.com/kali-linux-arm-images/
   Vemos muchas placas en cual vamos a seleccionar la de raspberry pi 3



Al tenerlo descomprimido vamos a la iso que ha creado.



Le damos click derecho y los ofrece estas opciones. El cual vamos a seleccionar Escribir la imagen



Kali Linux

Quien creo kalinux
Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.
Kali es desarrollado en un entorno seguro; el equipo de Kali está compuesto por un grupo pequeño de personas de confianza quienes son los que tienen permitido modificar paquetes e interactuar con los repositorios oficiales. Todos los paquetes de Kali están firmados por cada desarrollador que lo compiló y publicó. A su vez, los encargados de mantener los repositorios también firman posteriormente los paquetes utilizando GNU Privacy Guard.

Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM).

El Shell es un intérprete de comandos. Más que únicamente una capa aislada entre el Kernel del sistema operativo y el usuario, es también un poderoso lenguaje de programación. Un programa shell, llamado un script, es un herramienta fácil de utilizar para construir aplicaciones “pegando” llamadas al sistema, herramientas, utilidades y archivos binarios. El Shell Bash permite automatizar una acción o realizar tareas repetitivas que consumen una gran cantidad de tiempo.

Para la siguiente práctica se utilizará un sitio web que publica listados de proxys. Utilizando

comandos del shell bash se extraerán las direcciones IP y Puertos de los Proxys hacia un archivo
Durante los últimos años Backtrack Linux ha sabido ganarse el lugar como una de las mejores distribuciones para profesionales de la seguridad informática, pero con cada nueva versión este se volvía mas lento, pesado e incluía cosas que realmente muy pocas personas usaban, esto dio pié a que distribuciones como

Bugtraq crecieran en la popularidad y tomaran fuerza.

Offensive Security estaba consciente de esta realidad y hace un tiempo anunció que la versión 5 R3 seria la ultima versión de Backtrack como tal, la que seria la versión 6 de Backtrack pasaría a llamarse Kali.

Un aspecto en el que se diferencia de Backtrack es que Kali Linux inicia en modo gráfico directamente, distinto de Backtrack donde había que iniciarla mediante el comando startx. Además Kali posee un gestor de paquetes gráfico llamado gpk-application que permite la instalación de paquetes de forma sencilla, donde por ejemplo es posible instalar LibreOffice para utilizarlo.

- Más de 300 herramientas de pruebas de penetración: Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.
- Gratis y siempre lo será: Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.

- Git – árbol de código abierto: Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.

    - Obediente a FHS: Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente

  archivos binarios, archivos de soporte, bibliotecas, etc.
- Amplio apoyo a dispositivos inalámbricos: Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.
- Kernel personalizado con parches de inyección: Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.

- Entorno de desarrollo seguro: El equipo de Kali Linux está compuesto por un

pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.

1. Paquetes firmado con PGP y repos: Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.

- Multi-lenguaje: Aunque las herramientas de penetración tienden a ser escritas en Inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.
- Totalmente personalizable: Estamos completamente consiente de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan personalizar Kali Linux a su gusto, todo el camino hasta el núcleo.

- Soporte ARMEL y ARMHF: Dado a que los sistemas basados en ARM son cada vez más frecuentes y de bajo costo, sabíamos que el soporte de ARM de Kali tendrían que ser tan robusta como podríamos administrar, resultando en instalaciones que trabajan en sistemas de ARMEL y ARMHF. Kali Linux tiene repositorios ARM integrado con la línea principal de distribución de modo que las herramientas para ARM serán actualizada en relación con el resto de la distribución. Kali está disponible para los dispositivos ARM siguientes:

- rk3306 mk/ss808
- Raspberry Pi
- ODROID U2/X2
- MK802/MK802 II
- Samsung Chromebook

Descargar en formas de Kali Linux

- 32 bits (torrent) (descarga directa) (Mini ISO)
- 64 bits (torrent) (descarga directa) (Mini ISO)
- ARMEL (torrent) (descarga directa)
- ARMHF (torrent) (descarga directa)

Kali también está disponible como una máquina pre-hecha virtual de VMware con VMware Tools instalado. Las imágenes de VMware están disponibles en formatos de 32-bit y 64-bit.

Verificar que la USB haya sido reconocida por el equipo, muy común en equipos virtualizados.
Usar dmesg para verificar la etiqueta del disco, o usar gparted o alguna otra
herramienta para admnistrar discos Opcional (?): Usar gparted o algún otra herramienta para remover cualquier partición existente en la USB. En mi caso esto fue esencial, pues sin esto la memoria no era reconocida como un dispositivo de arranque. Copiar kali.iso a la USB. Aquí entra el comando que se menciona en la documentación oficial. sudo dd if=~/carpeta_personal/kali-linux-1.0.5-amd64/kali-

linux-1.0.5-amd64.iso of=/dev/sdb1 De preferencia usar sudo o el comando en su distribución para escalar los
Durante la instalación, Kali Linux permite configurar una contraseña para el usuario root. Sin embargo, si decides iniciar con la imagen live en vez de las imagenes, i386, amd64, VMWare o ARM, estas iran configuradas con el password predeterminado para root, que es – “toor“, sin comillas. Nueva Funcionalidad de autrodestrucción en Kali Linux v1.0.6

Privilegios como root.
Instalar Kali Linux en una memoria USB desde Windows:

Nuevo parche llamado **“nuke”** en cryptsetup (es la herramienta que maneja el cifrado de disco en kali), que destruye todo los datos cifrados en nuestro disco de
forma permanente.

Existe la posibilidad de poder eliminar el acceso a una partición cifrada simplemente ingresando una contraseña específica al momento de iniciar el sistema.

Esta nueva funcionalidad aplica a aquellos usuarios que encriptaron, o deseen cifrar, alguna de sus particiones dentro de Kali Linux. Si bien la posibilidad de poder cifrar particiones por medio de la combinación de LUKS (Linux Unified Key Setup) y LVM (Logical Volume Management) no es una novedad, si lo es la

capacidad de poder eliminar las llaves de acceso a las mismas con una simple contraseña. Para poder explicar mejor esto, es necesario antes aclarar en qué consiste el cifrado de las particiones.

¿Cómo se protege una partición cifrada en Kali Linux?

Este proceso se realiza desde el instalador de la distribución, y puede aplicarse sobre un disco duro o incluso sobre un dispositivo USB. Al seleccionar la opción de proteger la partición completa con un LVM encriptado se le solicitará al usuario que ingrese una frase secreta que utilizará como contraseña. Dicha frase le será solicitada al usuario al momento de iniciar (bootear) el sistema de manera de poder descifrar el disco para su uso.

Si bien el único dato que el usuario conoce para descifrar el disco es la frase que él mismo eligió, no es ese valor el que se utilizó para cifrar el disco. El disco, al momento de ser encriptado, utiliza una llave (key) generada aleatoriamente por el sistema para protegerlo. La frase del usuario solo le permite al sistema acceder a dicha llave (key) para que esta, posteriormente, descifre el contenido en cuestión.

Es decir que si se cifraran dos particiones idénticas con la misma contraseña las llaves maestras no podrían ser intercambiadas ya que permanecen únicas para cada instancia. Además, indistintamente de cuál es la contraseña utilizada, si la llave maestra se pierde, recuperar la información sería imposible.

¿Cómo funciona la “Nuke Password“?

Este nueva característica consiste en la creación de una frase de seguridad (contraseña) secundaria la cual, al ser ingresada borra de forma segura todas las llaves maestras, dejando inaccesible la información encriptada.

No obstante, los desarrolladores de la ampliamente difundida plataforma de seguridad, Offensive Security, realizaron previo al lanzamiento de la versión 1.0.6, una encuesta para conocer la preferencia o rechazo de sus usuarios ante esta nueva funcionalidad, obteniendo un 95% de respuesta afirmativa

OWASP

Open Web Application Security Project
OWASP (acrónimo de Open Web Application Security Project, en inglés 'Proyecto abierto de seguridad de aplicaciones web') es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP. La comunidad OWASP está formada por empresas, organizaciones educativas y particulares de todo mundo. Juntos constituyen una comunidad de seguridad informática que trabaja para crear artículos, metodologías, documentación, herramientas y tecnologías que se liberan y pueden ser usadas gratuitamente por cualquiera.

OWASP es un nuevo tipo de entidad en el mercado de seguridad informática. Estar libre de presiones corporativas facilita que OWASP proporcione información imparcial, práctica y redituable sobre seguridad de aplicaciones informáticas. OWASP no está afiliado a ninguna compañía tecnológica, si bien apoya el uso informado de tecnologías de seguridad. OWASP recomienda enfocar la seguridad de aplicaciones informáticas considerando todas sus dimensiones: personas, procesos y tecnologías.

Los documentos con más éxito de OWASP incluyen la Guía OWASP y el ampliamente adoptado documento de autoevaluación OWASP Top 10. Las herramientas OWASP más usadas incluyen el entorno de formación WebGoat, la herramienta de pruebas de penetración WebScarab y las utilidades de seguridad para entornos .NET OWASP DotNet. OWASP cuenta con unos 50 capítulos locales por todo el mundo y miles de participantes en las listas de correo del proyecto. OWASP ha organizado la serie de conferencias AppSec para mejorar la construcción de la comunidad de seguridad de aplicaciones web.

ZAP

Una de las herramientas más potentes del programa OWASP es ZAP (Zed Attack Proxy) . Esta plataforma está diseñada especialmente para monitorizar la seguridad de las aplicaciones web de las compañías, siendo una de las aplicaciones del proyecto más activas en cuanto a auditorías de seguridad.

Las principales características de OWASP ZAP son:

- Herramienta totalmente gratuita y de código abierto.
- Herramienta multi-plataforma, compatible incluso con Raspberry Pi.
- Fácil de instalar, dependiendo únicamente de Java 1.7 o superior.
- Posibilidad de asignar un sistema de prioridades.
- Traducida a más de 12 idiomas, entre ellos, el español.
- Excelente manual de ayuda y gran comunidad en la red.

Los usuarios de esta herramienta forense de seguridad podrán auditar diferentes aplicaciones web con una serie de funciones y análisis específicos:

- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Posibilidad de localizar recursos en un servidor.
- Análisis automáticos.
- Análisis pasivos.
- Posibilidad de lanzar varios ataques a la vez.
- Capacidad para utilizar certificados SSL dinámicos.
- Soporte para utilizar tarjetas inteligentes (DNI-e, por ejemplo) y certificados personales.
- Análisis de sistemas de autenticación.
- Posibilidad de actualizar la herramienta automáticamente.
- Dispone de una tienda de extensiones (plugins) con las que añadir más funcionalidades a la herramienta.

Recientemente se ha publicado la versión 2.4 de ZAP. Esta nueva versión supone un importante cambio en la herramienta ya que implemente una serie de funciones y herramientas

- Han añadido un nuevo “modo de ataque” para buscar vulnerabilidades.
- Mejoras en el sistema de inyección que permite atacar varios puntos a la vez.
- Nuevo sistema de políticas que nos permite elegir las reglas que formarán parte del análisis.
- Nuevos diálogos de escaneo con opciones avanzadas.
- Por defecto sólo se muestran las pestañas básicas del programa, quedando el resto ocultas hasta que el usuario las necesita.
- Nuevos plugins: “control de acceso” y “secuencia de escaneo”.
- Se han añadido nuevas reglas de análisis y se han cambiado algunos parámetros de otras reglas existentes.
- Cambios en la interfaz del programa, por ejemplo, una ventana de carga, mejoras en la barra de progreso y un nuevo sistema de alertas.

CRONOGRAMA DE ACTIVIDADES

Actividades	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	
Reunión de grupo								
Instalación de Kali Linux								
Instalación de Owasp zap								
filmación de Videos								
Reinstalación de kali Linux y Owas Zap								
Reunión de grupo								
Pruebas de auditoria de seguridad 1								
Pruebas de auditoria de Seguridad 2								

Factibilidad Kali Linux

excelente para utilizar las herramientas más populares incluidas en Kali Linux, las cuales abarcan las bases de las Pruebas de Penetración. Así mismo como proteccion a la auditorias de de informacion de las bases de datos utilizando el OWASP en conjunto para obtener mejores resultados sin dañar la informacion y se ejecuta una forma mas facil para losprofesionales inmersos en el tema.

Viabilidad Kali Linux

Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar auditorías de seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas, es muy viable para nuestra carrera de ciencias de la computacion.

Conclusión

Kali Linux es un sistema operativo muy amplio con muchas herramientas y absolutamente sin ningún costo , sus herramientas son muy efectivas para los trabajos de seguridad y auditorias sumándole a esto el trabajo con la organización Owasp que es una organización sin fines de lucros más que para ayudar en la seguridad de aplicaciones web lo cual es muy bueno para la comunidad informática, empresas y otras instituciones que hacen usos de los servicios, como experiencia propia en el uso de ZAP vemos que es una herramienta muy buena para detectar vulnerabilidades webs, pero creemos que su uso debe ser ético y educativo y con fines de trabajo u oficio para quien trabajo en seguridad web de empresas, instituciones etc. El uso de todo esto es muy accesible ya que es de código abierto y eso es muy bueno para la comunidad informática más herramientas y sistemas libres para todas las personas que hacen uso de estas herramientas ya que entre todos nos hacemos fuertes y logramos que esto se mantenga en buen camino, de nosotros depende que todo este movimiento siga adelante.

Bibliografía

Pagina de Owasp https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/

Pagina Oficial de Raspberry https://www.raspberrypi.org/downloads/
Descarga de Zap https://github.com/zaproxy/zaproxy/wiki/Downloads
Rasspberry Pi Organización https://www.raspberrypi.org
Caracteristicas Raspberry pi 3 https://es.wikipedia.org/wiki/Raspberry_Pi
http://www.ReYDeS.com.
Correo electrónico:
caballero.alonso@gmail.com

Anexos

Listado completo de Herramientas

Aplicaciones de sistema cali Linux	Herramientas DNS	Herramientas cali Linux	Herramientas de cali Linux
• Tcpflow (monitorizar tráfico red) • Intrace • Zenmap (Escáner de puertos) • Sqlninja (SQL Server) • Acccheck (SMB Samba) • Forensics mode • Offline password cracking como John the Ripper • Guymager (creación imágenes) • Chkrootkit (anti rootkit) • Metasploit	*Análisis DNS* • dnsdict6 • dnsenum • dnsmap • dnsrecon • dnsrevenum6 • dnstracer • dnswalk • fierce • maltego • nmap • urlcrazy *Identificación Host* • fragroute • fragrouter • wafw00f • alive6 • arping • cdpsnarf • detect-new-ip-6 • detect-sniffer6	Scáners de Red • dmitry • dnmap-client • dnmap-server • netdiscover • nmap Detección Sistema Operativo (OS Fingerprinting) • dnmap-client • dnmap-server • miranda • nmap Herramientas OSINT (Essential OSINT Tools for Social Engineering) • casefile	Análisis Base de Datos (SQL) • bbqsql • dbpwaudit • hexorbase • mdb-export • mdb-parsecsv • mdb-sql • mdb-tables • oscanner • sidguesser • sqldict • sqlmap • sqlninja • sqlsus • tnscmd10g Herramientas Fuzzing (Fuerza Bruta) • bed • fuzz_ip6 • ohrwurm • powerfuzzer

- apktool

- dnmap-server
- fping
- hping3
- inverse_lookup6
- miranda
- ncat
- netdiscover
- nmap
- passive_discovery6
- thcping6
- wol-e
- xprobe2

Herramientas Off-line

- cachedump
- chntpw
- cmospwd
- crunch
- dictstat
- hashcat
- hash-identifier
- john the ripper

- maltego
- metagoofil
- theharvester
- twofi
- urlcrazy

Análisis Samba

- accheck
- nbtscan
- nmap

Análisis SNMP

- braa
- cisco-auditing-tool
- cisco-torch
- copy-router-config
- merge-router-config
- nmap
- onesixtyone

Análisis SSL

- spike-generic_chunked
- spike-generic_listen_tcp
- spike-generic_send_tcp
- spike-generic_listen_upd
- burpsuite
- powerfuzzer
- webscarab
- webslayer
- websploit
- wfuzz
- xsser
- zaproxy

Identificación de CMS

- blindelephant
- plecost
- wpscan

Proxys

	plus • ophcrack • ophcrack-cli • policygen • pwdump • pyrit • rainbowcrack • rcracki_mt • rsmangler • samdump2 • sipcrack • sucrack • truecrack Herramientas Online • accheck • burpsuite • cewl • cisco-auditing-tool • dbpwaudit • findmyhash • hydra • hydra-gtk • medusa	• sslstrip • sslyze • stunnel4 • tlssled Análisis de Tráfico • cdpsnarf • intrace • irpas-ass • irpass-cdp • p0f • tcpflow • wireshark Análisis de VOIP • ace • enumiax Análisis VPN • ike-scan Análisis Vulnerabilidades • cisco-auditing-tool • cisco-	• zaproxy Herramientas Web • apache-users • burpsuite • cutycapt • cutycapt • dirbuster • vega • webscarab • webslayer • zaproxy Herramientas GPU • oclhashcat-lite • oclhashcat-plus • pyrit Sniffers de Red • darkstat • dnschef • dnsspoof • dsniff • ettercap-graphical

- patator
- phrasendrescher
- thc-pptp-bruter
- webscarab
- zaproxy

Ataques Bluetooth

- bluelog
- bluemaho
- blueranger
- btscanner
- fang
- spooftooph

Herramientas Wireless - Wifi

- aircrack-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- asleap
- cowpatty
- eapmd5pass
- fern-wifi-cracker
- yersinia

Herramientas de Tunneling

- cryptcat
- dbd
- dns2tcpc
- dns2tcpd
- iodine
- miredo
- ncat
- proxychains
- proxytunnel
- ptunnel
- pwnat
- sbd socat
- sslh
- stunnel4
- updtunnel

Debuggers (Decompiladores) y Reversing

- edb-debugger
- ollydbg
- jad
- rabin2
- covery6
- sslsniff
- tcpflow
- urlsnarf
- webmitm
- webspy
- wireshark
- ettercap-graphical
- evilgrade
- fake_advertise6
- fake_dns6d
- fake_dnsupdate6
- fake_mipv6
- fake_mld26
- fake_mld6
- fake_mldrouter6
- fake_router6
- fake_solicitate6
- fiked
- macchanger
- parasite6
- randicmp6
- rebind
- redir6

		• mdk3 • wifiarp • wifidns • wifi-honey • wifiping • wifitap • wifite • zbassocflood • zbconvert • zbdsniff • zbdump • zbfind • zbgoodfind • zbid • zbreplay • zbstumbler Herramientas Android • android-sdk • apktool • baksmali • dex2jar • smali Herramientas Análisis Forense (Creación imágenes,	cli • apktool • clang • clang++ • dex2jar • flasm • javasnoop • radare2 • rafind2 • ragg2 • ragg2-cc • rahash2 • rarun2 • rax2 Herramientas Stress de Red (Web, Wlan) • denial6 • dhcpig • dos-new-ip6 • flodd_advertise6 • flood_dhcpc6 • flood_mld26 • flood_mld6 • flood_mldr	• yersinia Herramientas VoIP • iaxflood • inviteflood • ohrwurm • protos-sip • rtpbreak • rtpflood • rtpinsertsound • rtpmixsound • sctpscan • siparmyknife • sipp • sipsak • svcrack • svcrash • svmap • svreport • svwar • voiphopper Sniffers Web • burpsuite • dnsspoof	

- bulk_extractor
- chrootkit
- dc3dd
- dcfldd
- extundelete
- foremost
- fsstat
- galleta
- tsk_comparedir
- tsk_loaddb
- affcompare
- affcopy
- affcrypto
- affdiskprint
- affinfo
- affsignaffstats
- affuse
- affverify
- affxml
- blkcalc
- blkcat
- blkstat
- bulk_extractor
- ffind

- fragmentation6
- inundator
- kill_router6
- macof
- rsmurf6
- siege
- smurf6
- iaxflood
- invite flood
- thc-ssl-dos
- mdk3
- reaver

- webmitm
- webscarab
- webspy
- zaproxy

Backdoors

- cymothoa
- dbd
- intersect
- powersploit
- sbd
- u3-pwn

```
if( (keyslot > 0) && ((keyslot & CRYPT_ACTIVATE_NUKE) != 0) ) {
        nuke = 1;
        keyslot ^= CRYPT_ACTIVATE_NUKE;
}
if( (keyslot < 0) && ((keyslot & CRYPT_ACTIVATE_NUKE) == 0) ) {
        nuke = 1;
        keyslot ^= CRYPT_ACTIVATE_NUKE;
}
r = keyslot_verify_or_find_empty(cd, &keyslot);
if (r)
```

Nuevo parche llamado "nuke" en cryptsetup (es la herramienta que maneja el cifrado de disco en kali), que destruye todo los datos cifrados en nuestro disco de forma permanente.