UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

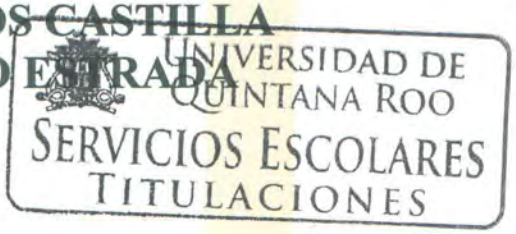
PENTEST: AUDITORÍA DE SEGURIDAD INFORMÁTICA UTILIZANDO UN SMARTPHONE

TESIS
PARA OBTENER EL GRADO DE
INGENIERO EN REDES

PRESENTA
EDGAR ROBERTO ZETINA IROLA

DIRECTOR DE TESIS
MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORES
MSI. LAURA YÉSICA DÁVALOS CASTILLA
MTI. MELISSA BLANQUETO ESTRADA



CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2014

UNIVERSIDAD DE QUINTANA ROO
DIVISIÓN DE CIENCIAS E INGENIERÍA

TRABAJO DE TESIS ELABORADO BAJO SUPERVISIÓN DEL COMITÉ DE ASESORÍA

Y APROBADO COMO REQUISITO PARCIAL PARA OBTENER EL GRADO DE:

INGENIERO EN REDES

COMITÉ DE TRABAJO DE TESIS

DIRECTOR: _____

MTI. VLADIMIR VENIAMIN CABAÑAS VICTORIA

ASESORA: _____

MSI. LAURA YÉSICA DÁVALOS CASTILLA

ASESORA: _____

MTI. MELISSA BLANQUETO ESTRADA

UNIVERSIDAD DE QUINTANA ROO
SERVICIOS ESCOLARES
TITULACIONES

CHETUMAL QUINTANA ROO, MÉXICO, NOVIEMBRE DE 2014

UNIVERSIDAD DE QUINTANA ROO
DCI DIVISIÓN DE CIENCIAS E INGENIERÍA

AGRADECIMIENTOS

Agradezco a Dios por darme la vida y las fuerzas de seguir adelante durante toda mi vida.

Un agradecimiento especial, quien fue de muy grande apoyo durante esta tesis y gran maestro durante la carrera, al MTI. Vladimir Veniamin Cabañas Victoria por su tiempo, dedicatoria, por brindarme su apoyo y herramientas necesarias para esta Tesis.

Al igual agradezco por su tiempo y paciencia por revisar esta tesis a MTI. Melissa Blanqueto Estrada y a la MSI. Laura Yésica Dávalos Castilla quien igual le agradezco por ser mi tutora durante la carrera.

Gracias a todos los profesores, que dedicaron su tiempo y la convivencia que se vivió a lo largo de la carrera, grandes profesores y amigos los cuales me dieron las herramientas necesarias para aprender y salir adelante. Muchas gracias a todos ellos.

Un agradecimiento importante a mis padres los cuales me dieron la vida y me apoyaron siempre para seguir mis metas y aspiraciones. Gracias a mi Madre por dedicar su tiempo a cuidarme, y estar conmigo en los buenos y malos momentos de mi vida, gracias por ayudar a levantarme y seguir adelante. Gracias Mamá por llevarme en la vida en el camino de lo correcto y animarme en todo momento doy gracias a Dios por haberme dado una Mamá como tú. Una madre única e inigualable

Mamá este éxito es para ti que te debo agradecer la vida y todo lo hermoso que me has dado muchas gracias.

Papá gracias por tu apoyo y por tus ayudas durante mis estudios por enseñarme varias cosas para mi futuro gracias de ti he aprendido muchas cosas gracias por dedicarte tu tiempo a enseñármelas y por tu amor que me has dado.

Y un agradecimiento con amor a mi novia quien estuvo conmigo durante la tesis y me ha apoyado en todo y ha estado conmigo dándome fuerzas para seguir adelante. Gracias amor por tu apoyo y el amor que me demuestras.

DEDICATORIA

A mis Padres Con todo mi amor y dedicación

A mi novia con todo mi cariño.

CONTENIDO

CAPÍTULO 1

Si quieres hacer las paces con tu enemigo, tienes que trabajar con tu enemigo. Entonces él se vuelve tu compañero. *Mandela, Nelson*

.

AUDITORÍA DE SEGURIDAD INFORMÁTICA UTILIZANDO UN SMARTPHONE

CAPÍTULO 1

1.1 INTRODUCCIÓN

La seguridad informática es un área que ha estado cobrando mayor importancia dentro de las organizaciones que usan las tecnologías de información y la comunicación (TICs) para realizar sus actividades (comerciales, financieras, sociales, médicas, etc.) y la preocupación por este tema va en aumento ya que hay miles de maneras para sabotear una red informática, sus dispositivos de comunicación, aplicaciones, bases de datos, redes sociales, etc. Los propósitos pueden ser muy variados: robo de información, sabotaje, espionaje, diversión, para probar nuevas técnicas y casi cualquier motivo que una persona pudiera tener. Por ejemplo ¿qué pasaría si una persona decidiera hoy atacar los sistemas de su compañía u organización?, esta es una de las preguntas que se plantean para asegurar la información, ¿cómo las organizaciones pueden saber si sus medidas de seguridad son realmente robustas y suficientes? Para esto pueden usar una prueba de penetración o (*Penetration Test* o *PenTest* en inglés) que es una herramienta de diagnóstico que revela la manera de operar de un intruso para lograr el acceso no autorizado a los sistemas de información en otras palabras se simula un ataque tal como lo haría un hacker.

Los *Smartphone* son dispositivos diseñados con características de un equipo informático, además de las funciones habituales de un teléfono móvil (hacer llamadas, revisar correo, ver videos, entrar a las redes sociales, etc.); tienen capacidades más parecidas a una computadora.

Este proyecto explorará la capacidad de un *Smartphone* para lograr *PentTest* usando las herramientas necesarias y soportadas por un *Smartphone*.

1.2 PLANTEAMIENTO DEL PROBLEMA

Hoy en día la delincuencia cibernética y el hacking es muy común por lo tanto la perdida de información en grandes empresas o de uso personal ha sido demasiado actualmente, la información es muy importante por eso hay que buscar todos los métodos posibles por los cuales un hacker puede atacar algún sistema informático. Existen infinidad de ataques por lo tanto se requiere de diferentes pruebas y diferentes escenarios que los atacantes puedan utilizar.

1.3 PROPUESTA

La capacidad de cómputo en los dispositivos móviles ha aumentado rápidamente en los últimos años, superando incluso algunas configuraciones de equipos portátiles. Cabe destacar que son pequeños, fáciles de transportar y siempre están a la mano para reaccionar frente a cualquier incidente rápidamente. En el mundo de la seguridad informática trabajar desde estos dispositivos proporciona un ventaja ya que pueden pasar desapercibidos en situaciones donde sea necesario, por ellos se propone utilizar herramientas de *Pentest* en un *Smartphone.*

Un Smartphone puede brindar una primera (y muy buena) impresión de la configuración y del estado de algunos sistemas informáticos identificando problemas, amenazas, configuraciones no adecuadas, y que necesariamente sería profundizado más adelante con un equipo especializado y más sofisticado.

¿Por qué utilizar un *Smartphone* para obtener una primera impresión? Al ser un dispositivo portable, en cualquier momento que sea requerida una pequeña prueba de seguridad se podría utilizar el dispositivo ya configurado con las herramientas necesarias para hacer pruebas de seguridad *in situ* e identificar las áreas prioritarias que requieran pruebas de penetración más robustas.

1.4 OBJETIVO GENERAL

Realizar *pentesting* en una red informática utilizando herramientas de monitoreo en un *Smartphone* para determinadas áreas.

Objetivos Particulares

1. Configurar un *Smartphone* con SO basado en Unix.
2. Instalar una suite de herramientas de *pentesting.*
3. Determinar las herramientas pertinentes para las pruebas de *pentesting* soportadas en el *Smartphone.*
4. Realizar un *pentesting.*
5. Publicar los resultados de la prueba.

1.5 ALCANCE

El proyecto se ha diseñado para realizar una prueba de *pentesting* en las aulas informáticas del edificio L de la División de Ciencias e Ingeniería, y publicar su resultado con el administrador de la red correspondiente.

CAPÍTULO 2

“Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoidance of danger is no safer in the long run than outright exposure. Life is either a daring adventure, or nothing.”

—Helen Keller, The Open Door (1957)

Traducción:

"La seguridad es principalmente una superstición. No existe en la naturaleza, ni los hijos de los hombres en su conjunto la experimentan. Evitar el peligro no es más seguro a largo plazo que la exposición directa. La vida es una aventura atrevida o nada. "

CAPÍTULO 2

2.1 PENTESTING

En el mundo digital, las empresas siguen teniendo dificultades para proteger la confidencialidad de la información que manejan (de sus activos, clientes, proveedores, etc.), manteniendo una presencia pública en Internet. Para mitigar los riesgos, es habitual que las empresas recurran a las pruebas de penetración (*PenTest)* para la evaluación de vulnerabilidades. El *PenTest* es la práctica de una empresa de terceros de confianza para intentar poner en peligro la red informática de una organización con el propósito de evaluar su seguridad. Mediante la simulación de un ataque directo, los gerentes pueden presenciar el potencial de un atacante malicioso que puede obtener o causar daños a los activos de datos de esa empresa.(Newman, 2005)

DEFINICIÓN DE PRUEBAS DE PENETRACIÓN

PenTest es como comúnmente se denomina a los "Test de penetración" y son en conjunto la forma de denominar una serie de técnicas utilizadas para evaluar la seguridad de redes, sistemas de computación y aplicaciones involucradas en los mismos(Maulini, 2010).

El término piratería se originó en el Instituto Tecnológico de Massachusetts (*MIT*) en 1960 con el *Tech Model Railroad Club* (TMRC) cuando intentaron modificar el desempeño de sus modelos de trenes al "*hackear* " los circuitos; es decir, *hacking* es una palabra que se utiliza para señalar que algo se ha modificado para que se comporte de manera distinta para lo cual fue diseñado. *Hackear* con el tiempo llegó a significar usar la ingeniería inversa de programas con el propósito de aumentar la eficiencia. En contraste además, hacking se refiere a propósitos ofensivos tales como entrar en una red informática sin autorización. Un hacker es aquel que realiza *hacking*, ya sea de forma maliciosa o defensiva.(Newman, 2005)

Los hackers a menudo llamados hackers de sombrero negro (*Black Hathackers*) realizan actos delictivos. Por otra parte, los hackers de sombrero blanco son aquellos que usan sus conocimientos para la práctica defensiva. Un probador de

penetración (*Pentester*) es un hacker ético que es contratado para evaluar la seguridad de datos de una organización o empresa.

Realizar *PenTest*, no es tarea fácil y requiere de un conocimiento sólido y profundo de las tecnologías involucradas en los sistemas, aplicaciones y servicios, además de una óptica y experiencia amplia en el comportamiento de varios sistemas operativos. Mediante estas técnicas, el *black hat hacker*, *white hat hacker o ethical hacker* pueden descubrir vulnerabilidades en el sistema estudiado, y usarlas para obtener acceso al mismo, por lo que está técnica se diferencia entre otras cosas del "análisis de vulnerabilidades" en que en este último una vez detectadas las vulnerabilidades no son usadas para penetrar el sistema.

Cualquier sistema o aplicación, por bien o mal protegidos que se piense que se encuentren, pueden ser objeto de un *PenTest* con o sin su consentimiento en cualquier momento, por lo que es importante descubrir las fallas de los mismos mediante el uso de las herramientas y esto puede ser una gran ventaja a la hora de defenderse de futuros intentos de penetración.

TIPOS DE PRUEBAS

Black-box test: es una prueba de penetración donde no se tiene conocimiento previo de una empresa. Por ejemplo, si se trata de una prueba de este tipo, el *pentester* podría obtener una dirección del sitio web o la dirección IP para intentar comprometer el sitio web como si fuera un hacker malicioso exterior.

White-Box test: El *pentester* tiene un conocimiento completo de la red interna. Se le han brindado diagramas de red o una lista de los sistemas operativos y las aplicaciones antes de realizar las pruebas. Aunque no es el más representativo de los ataques externos, esto es el más preciso, ya que presenta un escenario del peor caso, donde el atacante tiene conocimiento completo de la red.

Gray-box o *Cristal-box test*: El *pentester* simula ser un empleado. Se le da una cuenta en la red interna y acceso estándar a la red. Esta prueba evalúa las amenazas internas de los empleados.

¿DÓNDE SE UTILIZA?

Las pruebas de penetración podrían utilizarse en cualquier ambiente informático, ya que ninguna computadora está a salvo de un ataque por lo tanto pueden ser utilizadas en compañías que pueden tener el riesgo a perder mucha información o cualquier tipo de negocio que quiera saber el estado actual de su red.

Las pruebas de penetración podrían tener ramificaciones muy graves si no se realizan correctamente. Normalmente, las empresas siguen funcionando de manera normal mientras se está realizando la prueba. Esto aumenta el impacto en la empresa si un sistema se cae o es involuntariamente inutilizado. Para estos clientes, estos sistemas deben ser considerados "críticos" y abordarse con el debido cuidado. La gerencia de la empresa se enfrenta a mantener un equilibrio entre asegurarse de que la prueba se ha completado y la garantía de que todavía son capaces de hacer negocios de manera que los ingresos no se pierda.(T. J. Klevinsky, 2002)

¿QUÉ SE NECESITA?

Las herramientas disponibles para efectuar estas pruebas de penetración pasan por varios grados de complejidad, y el manejo de algunas de ellas puede ser todo un reto a la inteligencia y sagacidad del atacante o "*Pentester*". Entre ellas se incluyen desde scanner de puertos, complejos algoritmos para descifrar claves, sistemas de intrusión por fuerza bruta, herramientas de *sniffing* de redes y penetración de firewalls, así como también herramientas de escaneo de vulnerabilidades de aplicaciones web y mucho más. Todo un mundo de aplicaciones en su mayoría desarrolladas para entorno Linux (el entorno preferido para este tipo de trabajo) con las cuales el proceso de intento de penetración se hace mucho más "simple". Estas herramientas suelen estar agrupadas en lo que se conoce como "*Toolkits*" o juegos de herramientas(Maulini, 2010).

Algunos "*Toolkits*" son muy famosos en el medio por la eficiencia de sus herramientas y por haber sido utilizados en penetraciones de alto nivel a sistemas que se consideraron es su tiempo fortalezas impenetrables. Algunos además se consiguen inclusive en formato de LIVE CD o ISO, de forma que las herramientas ya están integradas e instaladas en un CD de arranque del sistema operativo con el que trabajan y son portátiles.

Entre estos *toolkits* podemos encontrar el famoso backtrack uno muy bueno para este tipo de pruebas y su sucesor es el Kali Linux del cual hablaremos un poco más adelante sobre este sistema que contiene más de 300 herramientas.

NOTIFICACIÓN DE INTENCIONES Y ACCIONES EN UN PENTEST.

Se debe poner en conocimiento al cliente y a todos aquellos con el derecho legal de saber el impacto y las implicaciones de una Prueba de Seguridad.(Herzog, 2003)

• Los Auditores de Seguridad deben poner a disposición del cliente la información detallada asociada a las acciones que se tomarán como parte de la Prueba de Seguridad.

• Si se descubre la presencia de atacantes (hackers) en el sistema de un cliente durante la Prueba de Seguridad, los Auditores deben informar al cliente tan pronto como sea posible.

• Cualquier tercera entidad a la que pudiera afectar la Prueba de Seguridad debería ser informada de la naturaleza

Puede ser un requisito legal en algunos países el entregar notificaciones de intenciones y acciones referidas a la Prueba de Seguridad. En el Reino Unido, los auditores son responsables por una variedad de razones si no proveen dichas notificaciones. Esto supone una violación de los acuerdos contractuales, un acto de negligencia o una infracción a la legislación vigente, como el Acta de Uso Inapropiado de Ordenadores de 1990.

ACTIVIDADES QUE COMPRENDE

Una *PenTest* comprende múltiples etapas con diferentes tipos de actividades en distintos ámbitos y entornos. La profundidad con que se lleven a cabo las actividades dependerá de ciertos factores, entre los que se destaca el riesgo que puede generar hacia el cliente alguno de los métodos que se apliquen durante la evaluación.(Catoira, 2012)

Se establece un previo acuerdo con el cliente para llevar a cabo las diferentes fases del análisis, que se describen a continuación:

Fase de reconocimiento. Posiblemente, esta sea una de las etapas que más tiempo demande. Se definen objetivos y se recopila toda la información posible que luego será utilizada a lo largo de las siguientes fases. La información que se busca abarca desde nombres y direcciones de correo de los empleados de la organización, hasta la topología de la red, direcciones IP, entre otros. Cabe destacar que el tipo de información o la profundidad de la pesquisa dependerán de los objetivos que se hayan fijado en la auditoría.

Fase de escaneo. Utilizando la información obtenida previamente se buscan posibles vectores de ataque. Esta etapa involucra el escaneo de puertos y servicios. Posteriormente se realiza el escaneo de vulnerabilidades que permitirá definir los vectores de ataque.

Fase de enumeración. El objetivo de esta etapa es la obtención de los datos referente a los usuarios, nombres de equipos, servicios de red, entre otros. A esta altura de la auditoría, se realizan conexiones activas con el sistema y se ejecutan consultas dentro del mismo.

Fase de acceso. En esta etapa finalmente se realiza el acceso al sistema. Esta tarea se logra a partir de la explotación de aquellas vulnerabilidades detectadas que fueron aprovechadas por el auditor para comprometer el sistema.

Fase de mantenimiento de acceso. Luego de haberse obtenido el acceso al sistema, se busca la manera de preservar el sistema comprometido a disposición de quien lo ha atacado. El objetivo es mantener el acceso al mencionado sistema perdurable en el tiempo.

BENEFICIOS DEL PENTEST

Los *PenTest* permiten priorizar riesgos y proponer acciones, con acento en las áreas alrededor de las amenazas principales. Las buenas pruebas ayudan a entender por qué los problemas pueden ser críticos, mientras dan sentido y dirección a los cambios sugeridos. El plan de acción que derive de las pruebas debe considerar el impacto desde el punto de vista de la probabilidad de ataques, vulnerabilidad y valor de los activos, así como el esfuerzo a realizar en materia de planeación, implementación y administración.

En todo caso, las pruebas de penetración más eficaces permiten correlacionar el impacto de los riesgos y su probabilidad, encontrando el punto óptimo para cada empresa.

Los *PenTest* sirven también para motivar el cambio hacia el incremento de controles, enfocar los esfuerzos técnicos, generar conciencia y sentido de urgencia. Pero, si de verdad se quiere lograr esto es necesario organizar una demostración final de los ejercicios de irrupción.

Finalmente para cerrar el círculo conviene también organizar una reunión técnica con el fin de valorar a detalle los hallazgos, definir la forma de presentarlos a la alta dirección y trazar la estrategia a seguir. Entre las prohibiciones a fijar entre quienes ejecutarán las pruebas están: no instalar jamás puertas traseras (back doors), ni ocultar aplicaciones de acceso remoto (*bots*, troyanos, *rootkits* y demás); no borrar,

alterar o inhabilitar registros y, desde luego, no apagar o modificar el comportamiento de las herramientas de detección establecidas.

Entre los puntos que debe contener el informe posterior a las pruebas de penetración están: un resumen para la alta administración; un análisis de los riesgos principales; recomendaciones agrupadas por tipo de dispositivo, sistema operativo, bases de datos o servidores de dominio y las acciones concretas a seguir.

2.2 HERRAMIENTAS DE PENTESTING QUE SE USAN ACTUALMENTE

NMAP

Nmap ("*Network Mapper*") es un software libre y de código abierto de gran utilidad para el descubrimiento de red y para realizar auditorías de seguridad. (Lyon G. "., 2008)

Una gran cantidad de administradores de red lo utilizan para tareas como inventario de la red, los horarios de actualización de servicios administrar y monitorear host o servicio del tiempo de actividad. *Nmap* utiliza paquetes IP crudos en formas novedosas para determinar qué hosts están disponibles en la red, que servicios los anfitriones están ofreciendo (nombre de la aplicación y versión), qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes / cortafuegos están en uso, y decenas de otras características. Fue diseñado para escanear rápidamente grandes redes, pero funciona bien contra los ejércitos individuales. *Nmap* se ejecuta en todos los sistemas operativos de computadora, y los paquetes binarios oficiales están disponibles.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que unos cortafuegos, filtro, u otro obstáculo en la red están bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap,

pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado open | filtered y closed | filtered cuando no puede determinar en cuál de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).(Lyon G. , 2010)

Además de la tabla de puertos interesantes, *Nmap* puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC.(Lyon G. "., 2008)

WIRESHARK

Wireshark es analizador de protocolos de red, permite ver lo que está sucediendo en la red a un nivel microscópico. Es el más usado estándar en muchas industrias e instituciones educativas". El desarrollo Wireshark prospera gracias a las aportaciones de expertos de todo el mundo en red. Es la continuación de un proyecto que se inició en 1998.(Peines, 2013)

Con esta herramienta podremos analizar todos los paquetes de datos que entren y salgan de cualquiera de nuestras interfaces de red (tarjetas Ethernet o Wi-Fi). Se puede ver esta información en tiempo real, y puede ser filtrada en tiempo real también. Se encuentra en los repositorios de las otras más populares.

La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. Así, permite ver todo el tráfico que pasa a través de una red (usualmente una red Ethernet, aunque es compatible con algunas otras) estableciendo la configuración en modo promiscuo. También incluye una versión basada en texto llamada tshark.

Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Se puede analizar la información capturada, a través de los detalles y sumarios por cada paquete. Wireshark incluye un completo lenguaje para filtrar lo que queremos ver y la habilidad de mostrar el flujo reconstruido de una sesión de TCP.

BURP SUITE

Burp Suite es una plataforma integrada para la realización de las pruebas de seguridad de aplicaciones web. Sus diversas herramientas funcionan perfectamente juntas para apoyar todo el proceso de prueba, de cartografía y el análisis iníciales de la superficie de ataque de una aplicación, a través de la búsqueda y explotación de vulnerabilidades de seguridad."(Ltd, 2013)

Burp le da control total, lo que le permite combinar técnicas manuales avanzadas con la automatización de state-of-the-art, a hacer su trabajo más rápido, más eficaz, y más divertido.

Burp Suite contiene los siguientes componentes clave(Kamel, 2012):

- Un Proxy intercepta, lo que le permite inspeccionar y modificar el tráfico entre el navegador y la aplicación de destino.
- Una araña con reconocimiento de aplicaciones, para el rastreo de contenido y funcionalidad.
- Un escáner de aplicaciones web avanzadas para automatizar la detección de numerosos tipos de vulnerabilidad.
- Una herramienta de intrusión, para realizar poderosos ataques personalizados de encontrar y explotar vulnerabilidades inusuales.
- Una herramienta de repetidor, para manipular y volver a enviar peticiones individuales.
- Una herramienta secuenciador, para probar la aleatoriedad de las credenciales de sesión.
- La capacidad de guardar su trabajo y reanudar el trabajo más tarde.
- Extensibilidad, lo que le permite escribir fácilmente tus propios plugins, para realizar tareas complejas y personalizadas muy dentro de Burp.

La versión gratuita te permite Opciones:

- En primer lugar, tiene un PROXY local interceptando, esta le permite capturar el tráfico entre el navegador y el sitio de destino. A continuación, puede inspeccionar el tráfico capturado y pasarlo a otras herramientas de la suite para su posterior análisis y pruebas.

- El reconocimiento de aplicaciones SPIDER. Esta herramienta se puede utilizar para rastrear sitios de destino a revelar el contenido del sitio, detrás de la estructura y otras funcionalidades.
- La herramienta REPETIDOR le permite reenviar manualmente las solicitudes HTTP individuales. Esta es una herramienta muy útil ya que le permite realizar cambios rápidos sobre la marcha y ver cómo responde el servidor.
- La herramienta INTRUDER se centrará en la actualidad. Esta herramienta le permite realizar cargas a medida para ser utilizados en el ataque a la meta. Es altamente personalizable y limitado sólo por su imaginación.
- La herramienta SECUENCIADOR es útil si desea probar la aleatoriedad de las credenciales de sesión. Esto puede ser usado para descubrir la entropía débil que podría conducir a algo así como la explotación de Sesión Jacking o un tipo similar de escenario. No voy a estar cubriendo esto hoy, pero usted debería ser capaz de recoger los desechos de este tutorial básico y luego empezar a probar por su cuenta.
- La herramienta DECODER es otra útil para tener alrededor, ya que puede ser utilizado para decodificar material que usted puede venir a través de su prueba o también puede ser utilizado para realizar tareas comunes como la conversión de texto a HEX. Esto vale la pena jugar con como yo no lo va a cubrir aquí hoy, pero es sencillo y bastante simple de recolección.
- La herramienta COMPARTER está diseñada para permitir llevar a cabo la comparación visual de cualquiera de los dos artículos.

Versión PRO:

- Incluye una aplicación web avanzado escáner de vulnerabilidades que es muy precisa en la detección de todo tipo de vulnerabilidades que podrían ser explotadas.
- Permite guardar y restaurar en caso de que deje paso a mediados.

También tiene algunos adicionales de búsqueda, el descubrimiento de contenido y las características de programación de tareas que no están disponibles en la versión gratuita.

AIRCRACK-NG

“Aircrack-ng es un WEP 802.11 y claves WPA-PSK programa que puede recuperar claves una vez que se han capturado los paquetes de datos suficientes grietas. Implementa el ataque FMS (Fluhrer, Mantin y Shamir (Zero13, 2008) publicaron el primer ataque de recuperación sobre WEP en 2001. Su ataque se basó en las siguientes ideas: Un atacante que escuche pasivamente el tráfico de una red protegida con WEP puede grabar un montón de paquetes cifrados incluyendo los vectores de inicialización usados por dichos paquetes.)Estándar junto con algunas optimizaciones como ataques KoreK, así como el ataque PTW, con lo que el ataque mucho más rápido en comparación con otras herramientas de cracking WEP.

De hecho, Aircrack-ng es un conjunto de herramientas para la auditoría de redes inalámbricas.”(Aircrack-ng, 2009)

Las herramientas más utilizadas para la auditoría inalámbrica son:

Aircrack-ng. Descifra la clave de los vectores de inicio

Airodump-ng. Escanea las redes y captura vectores de inicio.

Aireplay-ng. Inyecta tráfico para elevar la captura de vectores de inicio

Airmon-ng. Establece la tarjeta inalámbrica en modo monitor, para poder capturar e inyectar vectores.

Con *aircrack-ng* sólo se puede intentar obtener claves pre-compartidas (*pre-shared keys*). Por lo tanto hay que asegurar que *airodump-ng* proporciona la autenticación de la red de tipo PSK, y en otro caso no se puede intentar averiguarla.

Hay otra diferencia importante entre crackear WPA/WPA2 y WEP. En las claves WEP, se pueden usar métodos “estáticos” de inyección para acelerar el proceso, pero para WPA/WPA2 solo se pueden utilizar técnicas de fuerza bruta. Esto se debe a que la clave no es estática, por lo que recogiendo IVs como para la encriptación WEP, no conseguiremos obtener más rápidamente la clave. Lo único que se necesita para poder iniciar un ataque es el *handshake* entre el cliente y el AP. El *handshake* se genera en el momento que el cliente se conecta a la red.

NESSUS

El Nessus es el escáner de vulnerabilidad, es el líder mundial en escáner activos, destacando el descubrimiento de alta velocidad, la revisión de configuración, el activo el descubrimiento de datos copiador, sensible y el análisis de vulnerabilidad de su postura de seguridad (valor). Nessus escáner puede ser distribuido en todas partes de una empresa entera, dentro DMZs, y a través de redes físicamente separadas.

Se compone de una estructura de cliente-servidor en la cual si vamos a usar nessus desde nuestro ordenador instalaremos ambos y nos conectaremos a nosotros mismos con la ip 127.0.0.1. El cliente sirve para conectar con el servidor y desde la interface del cliente lanzar los escaneos, esto sirve para si se quiere tener una maquina el servidor y en otra máquina en red el cliente y lanzar desde el cliente el escaneo conectados a la maquina servidor(Demon, 2008).

Sirve para detectar a través de la red vulnerabilidades en un sistema remoto, ya sea un cliente, un servidor, use linux, windows, mac, etc también detecta vulnerabilidades del software que tenga instalado por ejemplo que tenga la contraseña de vnc sin cambiar o posibles exploits que se puedan aplicar para romper total o parcialmente la seguridad.

En entornos empresariales Nessus se usa mucho para analizar sus propios equipos en lo que se llama una "Auditoria de Seguridad"

SNORT

Snort es un IDS o Sistema de detección de intrusiones basado en red (NIDS). Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos, etc conocidos. Todo esto en tiempo real.

Snort (http://www.snort.org/) está disponible bajo licencia GPL, gratuito y funciona bajo plataformas Windows y UNIX/Linux. Es uno de los más usados y dispone de una gran cantidad de filtros o patrones ya predefinidos, así como actualizaciones constantes ante casos de ataques, barridos o vulnerabilidades que vayan siendo detectadas a través de los distintos boletines de seguridad.

Este IDS implementa un lenguaje de creación de reglas flexibles, potente y sencilla. Durante su instalación ya nos provee de cientos de filtros o reglas para backdoor, ddos, finger, ftp, ataques web, CGI, escaneos Nmap.

Puede funcionar como sniffer (podemos ver en consola y en tiempo real qué ocurre en nuestra red, todo nuestro tráfico), registro de paquetes (permite guardar en un archivo los logs para su posterior análisis, un análisis offline) o como un IDS normal (en este caso NIDS)(Alfon, 2003).

NETCAT

Netcat es una utilidad de red aparece que lee y escribe datos a través de conexiones de red, utilizando el protocolo TCP / IP.

Está diseñado para ser una herramienta fiable " *back-end* " que se puede utilizar directamente o fácilmente impulsado por otros programas y scripts. Al mismo tiempo, se trata de una red de depuración y exploración herramienta rica en características, ya que puede crear casi cualquier tipo de conexión que pueda necesitar y tiene varias interesantes capacidades incorporadas.

Proporciona acceso a las siguientes características principales:

Conexiones salientes y entrantes, TCP o UDP, hacia o desde cualquier puerto. El modo de túnel destacado que permite también un túnel especial, como UDP a TCP, con la posibilidad de especificar todos los parámetros de red (puerto de origen / interfaz, puerto de escucha / interfaz, y el host remoto permitido para conectar con el túnel. Incorporadas capacidades de búsqueda de puertos, con aleatoriedad.

Opciones de uso avanzadas, tales como el modo de envío buffer (una línea cada N segundos), y hexdump (a un envió de error típico o a un archivo especificado) de datos tramitados y recibidos. Opcional RFC854 códigos telnet analizador y el respondedor.

El Netcat GNU se distribuye gratuitamente bajo la licencia GNU *General Public License* (GPL)(Giacobbi, 2006) .

La versión original de Netcat fue lanzada por Hobbit en 1995, pero no se ha mantenido a pesar de su inmenso renombre. A veces puede ser difícil encontrar nc110.tgz. La flexibilidad y la utilidad de esta herramienta han incitado a mucha otra gente a escribir otras implementaciones de Netcat - a menudo con las

características modernas no encontradas en la original. Una de las más interesantes es Socat, que amplía Netcat para soportar muchos otros tipos de sockets, cifrado SSL, proxys SOCK, y muchos más. También existe Ncat de Chris Gibson, que ofrece aún más características mientras que es tan portable y compacto como el resto.

METASPLOIT FRAMEWORK

Metasploit proporciona la información útil para poblar quien realiza pruebas de penetración, IDS el desarrollo de firma, y explota la investigación. Este proyecto fue creado para proporcionar la información sobre técnicas de proeza y crear un recurso útil para reveladores de proeza y profesionales de seguridad. Proporcionan los instrumentos y la información sobre este sitio para la investigación de seguridad legal y objetivos probadores sólo. Metasploit es un proyecto de comunidad manejado por Metasploit LLC.

Para empezar a hablar del metasploit, lo definiremos como una herramienta GNU escrita en perl y con utilización de diversos lenguajes de programación como C, Python, ASM, etc, para el desarrollo, testeo, mejora y penetración a diversos sistemas, entre ellos Windows.

Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo único que tenemos que indicarle a metasploit es que vulnerabilidad utilizaremos, que sistema atacaremos, que tipo de ataque utilizaremos y datos diversos que utilizara para atacar al host.

Se llama Metasploit Framework porque es todo un entorno de testeo para diversas plataformas, la cual trabaja con librerías, bases de datos, y diversos programas, shell codes, etc. Por tal deja de ser un simple software si no un framework(Salazar, 2011).

JOHN THE RIPPER

John the Ripper es un programa que nos permite recuperar contraseñas a partir de los datos que existen en nuestro sistema. Actualmente está disponible para Unix/Linux, Windows, DOS, BeOS y OpenVMS. El propósito principal de esta herramienta es la detección se contraseñas débiles por parte del administrador del sistema.

John the Ripper no es un simple programa de cracking de contraseñas por fuerza bruta, dispone de varios modos de funcionamiento que permiten una búsqueda "inteligente" de las contraseñas más inseguras. Por ejemplo, el modo single prueba como contraseñas candidatas el nombre de usuario, el nombre real, el nombre del home y combinaciones de estos nombres con números y letras(SRAMEKIM, 2010).

John the Ripper usa un ataque por diccionario: tiene un diccionario con palabras, que pueden ser contraseñas típicas, y las va probando todas. Para cada palabra, la cifra y la compara con el hash a descifrar. Si coinciden, es que la palabra era la correcta.

Esto funciona bien porque la mayor parte de las contraseñas que usa la gente son palabras de diccionario. Pero John the Ripper también prueba con variaciones de estas palabras: les añade números, signos, mayúsculas y minúsculas, cambia letras, combina palabras, etc.

Además ofrece el típico sistema de fuerza bruta en el que se prueban todas las combinaciones posibles, sean palabras o no. Éste es el sistema más lento, y usado sólo en casos concretos, dado que los sistemas anteriores (el ataque por diccionario) ya permiten descubrir muy rápidamente las contraseñas débiles.

ETTERCAP

Una de las herramientas más potentes que hacen uso del envenenamiento ARP en entornos GNU/Linux es Ettercap. Ésta es una herramienta con licencia GPL diseñada con el fin de analizar, filtrar, loguear y escuchar determinado tráfico circulando por la red. Soporta disección

activa y pasiva de muchos protocolos (incluso los cifrados). Es capaz de realizar ataques MITM (Man in the Middle) entre diferentes hosts de la red, con el fin de entrometerse en su comunicación y obtener información valiosa tipo contraseñas POP, SSH, Telnet, FTP, Https, etc…

Decir que la mayoría de los sistemas operativos (excepto linux 2.4 y solaris 8) no implementan estados en el protocolo arp (aceptan arp- replys sin haber enviado antes un request), por lo que fácilmente aceptan respuestas ARP y en consecuencia modifican su tabla ARP en caché con cada arp-reply recibido.

Pasamos pues a explicar el funcionamiento en la práctica de este potente software.

Ettercap tiene dos modos de sniffer:

UNIFIED: Analiza todos los paquetes que pasan por el cable. Es posible poner la interfaz de red en modo promiscuo y permitir que los paquetes que no vayan dirigidos a él, los re direcciona usando la capa 3 de enrutado. Así es posible lanzar un ataque MITM con otra herramienta y permitir que ettercap re direccione los paquetes a su destino verdadero.

BRIDGED: Utiliza dos interfaces de red y direcciona el tráfico de una a la otra mientras se Analiza y se filtra si interesa. Es un método absolutamente anónimo pues es imposible detectar un ataque MITM por parte de los otros hosts de la red. Se puede decir que se trata de un MITM a nivel de la capa física. Estarás en medio del cable entre dos entidades. No es recomendado en gateways pues transformará el gateway en un bridge.

Las características más relevantes de Ettercap son:

Soporte SSH1: Capacidad para analizar a un usuario y contraseña de conexiones ssh1. Ettercap es el primer software capaz de analizar este tipo de tráfico en modo Full-duplex.

Soporte SSL: Capacidad de sniffer de datos cifrados con SSL. Un certificado falso es presentado al host víctima y la sesión es des encriptado.

Inyección de caracteres en una conexión establecida.

Filtrado de paquetes: Por medio de scripts es posible buscar por cadenas específicas en paquetes TCP y UDP, con el fin de modificarla por una que nosotros deseemos, desechar paquetes, etc.

Mata conexiones: Capacidad para finalizar conexiones TCP.

Soporte de Plug-ins: Capacidad de creación de tus propios plugins utilizando las API de Ettercap.

Capturado de contraseñas: TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG.

***Fingerprint* pasivo:** Posibilidad de escanear la red local en modo pasivo (sin enviar ningún paquete) y obtener información detallada sobre los hosts, como el sistema operativo que utilizan, servicios en ejecución, puertos abiertos, IP, direcciones MAC y vendedor del adaptador de red(SRAKERIM, 2011).

2.3 KALI LINUX

¿QUE ES KALI?

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, se ha cambiado a Git para los VCS.(© Copyright 2014, Offensive Security, 2013)

CARACTERÍSTICAS

Más de 300 herramientas de pruebas de penetración: Después de revisar todas las herramientas que se incluyen en BackTrack, se han eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar. Kali Linux, al igual que su predecesor, es completamente gratis.

Git – árbol de código abierto. Partidarios de software de código abierto y el 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 archivos, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.

Amplio apoyo a dispositivos inalámbricos. Kali Linux soporta 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 el 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.

Paquetes firmados 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, Kali tiene un gran soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.

Totalmente personalizable. Los 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, el soporte de ARM de Kali tendría que ser tan robusta, 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 actualizadas en relación con el resto de la distribución.(© Copyright 2014, Offensive Security, 2013)

IMÁGENES DE KALI LINUX

Ficheros tipo ISO

Kali Linux está disponible como una ISO de arranque en formatos de 32 y 64 bits.

Imágenes de VMware

Kali 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.

Imágenes de ARM

Debido a la naturaleza de la arquitectura ARM, no es posible tener una sola imagen que funcione en todos los dispositivos ARM. Tenemos Imágenes Oficiales de ARM disponible para los siguientes dispositivos:

- rk3306mk/ss808
- Raspberry Pi
- ODROID-U2/X2
- MK802/MK802 II
- Samsung Chromebook

ARM es una arquitectura de 32 bits desarrollada en 1983 por la empresa *Acorn Computers Ltd* para usarse en computadoras personales que maneja un sistema de instrucciones realmente simple lo que le permite ejecutar tareas con un mínimo consumo de energía.

Siendo esta razón por la que actualmente ha tomado bastante fuerza en el mercado de dispositivos móviles, donde el bajo consumo de energía es el objetivo primordial. La característica más interesante es el uso de los 4 bits superiores como código de condición, haciendo que cualquier instrucción pueda ser condicional.(Xataka Mexico, 2012)

Esta arquitectura es la que usa el Smartphone con la que se trabajara en el proyecto.

2.4 ANDROID®

ACERCA DE ANDROID ®

Android® es un sistema operativo basado en el kernel de Linux diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes o tabletas, inicialmente desarrollado por Android®, Inc. Google respaldó económicamente y más tarde compró esta empresa en 2005.Android® fue presentado en 2007 junto la fundación del Open Handset Alliance: un consorcio de compañías de hardware, software y telecomunicaciones para avanzar en los estándares abiertos de los dispositivos móviles. El primer móvil con el sistema operativo Android® fue el HTC Dream y se vendió en octubre de 2008.

DEFINICIONES SOBRE ANDROID®

ROM o Firmware: En Android® una ROM es un archivo que contiene todo el sistema operativo listo para ser copiado en la memoria flash (ROM) del dispositivo. En este se encuentran todos los archivos necesarios para ejecutar el sistema operativo y las aplicaciones pre instaladas, como el kernel de linux, iconos e imágenes.

APK: un APK (Android® Application Package) es el equivalente a la extensión .EXE de Windows que nos permite instalar aplicaciones en el sistema operativo.

Este formato es en realidad un empaquetado derivado de JAR que contiene los archivos necesarios para la ejecución de una aplicación o juego en Android®. En su estructura, en realidad son un simple archivo Zip

ROOT: Probablemente este sea un término familiar en los usuarios de linux, donde root es el “superusuario” que puede modificar el sistema, cambiar configuraciones, borrar archivos protegidos etc. Por ello al ser root, podrás modificar el sistema operativo de tu dispositivo a tu antojo y utilizar aplicaciones como autostart que te permite deshabilitar aplicaciones ya sea de usuario o de sistema, para que no se carguen al iniciar, disminuyendo el consumo de memoria y batería.

Bootloader: El Bootloader es el “gestor de arranque” en Android®, este se encarga de iniciar el kernel y todos los procesos necesarios para iniciar el sistema operativo. Como Android® es un sistema operativo de código fuente libre, el bootloader suele

variar entre los diferentes fabricantes de dispositivos, y muchos de ellos no permiten desbloquear el bootloader, ya que esto permite modificar el sistema operativo.

UnlockedBootloader. Para instalar un Recovery, ROM, o Kernels modificados es necesario tener el Bootloader desbloqueado, ya que en la actualidad, las operadoras suelen pedir a los fabricantes que pongan seguridad en sus dispositivos, con una clave cifrada, de modo que no es posible “firmar digitalmente” los archivos necesarios para cargar el SO o kernel sin conocerla.

CAPITULO 3

"Pienso que los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva"

-- *Stephen Hawking*

CAPÍTULO 3

3.1 DESARROLLO DEL PROYECTO

Introducción

En esta capitulo se describen los pasos que se tienen que seguir para modificar el Smartphone y así poderlo hacerlo configurable para la instalación del sistema operativo Kali. Para esto necesitamos tener todos los privilegios en el Smartphone para ellos se requiere ser tener el Smartphone en modo Root. Al igual que se indicara como instalar el Kali y sus herramientas paso a paso.

ROOT

Metodología

Para hacer Root un Smartphone

a) Desbloquear bootloader
b) Instalar firmware
c) Flashear la imagen de inicio “boot.img”
d) Instalar el super usuario en el recovery
e) Flashear excluyendo el sistema y las comunicaciones

Root Xperia V lt25i

Primero debemos ser usuarios Root en nuestro teléfono Android®, para cada dispositivo la manera de hacer Root es muy diferente en cada dispositivo móvil dependiendo la marca y el modelo tiene su forma en este caso lo que se mencionará solo se puede llevar acabo en el Xperia V lt25i de Sony®, para hacer Root otro teléfono investigar de qué manera se puede Rootear.

Requisitos:

a) Bootloader desbloqueado
b) FlashTool.
c) Descargar Firmware
d) Descargar "boot.img" de la última KXP.
e) Decargar Archivo del SuperSU,

Desbloqueo del Booloader

Verificar lo siguiente: Marcar en el teléfono *#*#7378423#*#* y así se accederán al menú *service*.

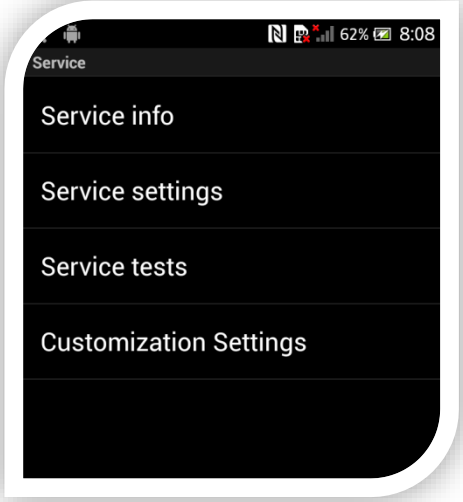


Figura 1 Menú Service 1

En este menú ingresamos a *service info* luego a *configuration* y seguido a *Rooting* Status si en el *Bootloader Unlock allowed* dice *Yes* pueden seguir de lo contrario no se puede continuar.

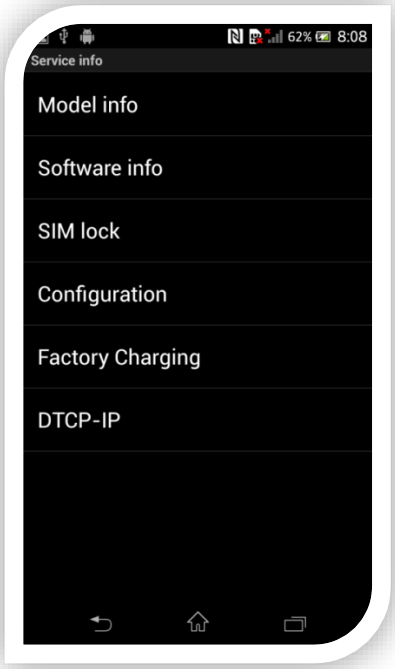


Figura 2 Menú services 2

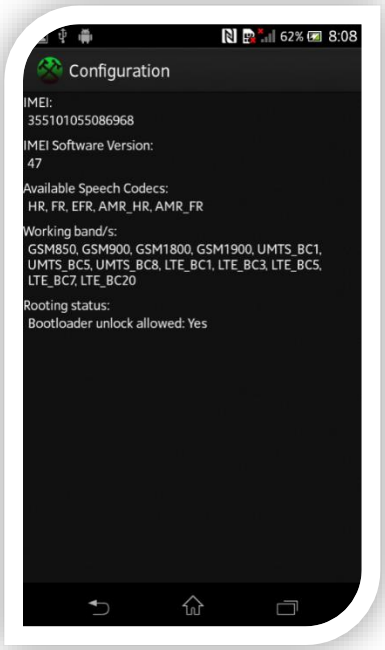


Figura 3 Menú services 3

Comprobado lo anterior hacer el *Unlocked Bootloader*

Paso 1.Se descarga el *Xperia V UnlockedBooloader.Zip*

Estos archivos se puedes localizar en internet en algún foro.

Paso 2. Lo siguiente después de descargar los archivos extraigan la carpeta y obtendrán los siguientes archivos

1. Drivers.zip
2. Fastboot_with_Android®_usb_file.zip
3. Unlockbootloader.Sony®mobile.com

Paso 3.Dirigirse al acceso directo que se descomprimió de Unlockbootloader.Sony®mobile.com

1. Se abrirá una página web en el navegador predeterminado. Desplácese hasta el final de las instrucciones de la página y verá un enlace que dirá "*Start unlocking the bootloader*", hacer clic en él.

2. Se abrirá otra página web. Desplácese también hasta el final de las instrucciones de la página y verá un enlace que dirá "Continúe", hacer clic.

3. En la ventana emergente, hacer clic en "Sí, estoy seguro" y luego hacer clic en la siguiente ventana tanto en las casillas de verificación y haga clic en "*Accept*".

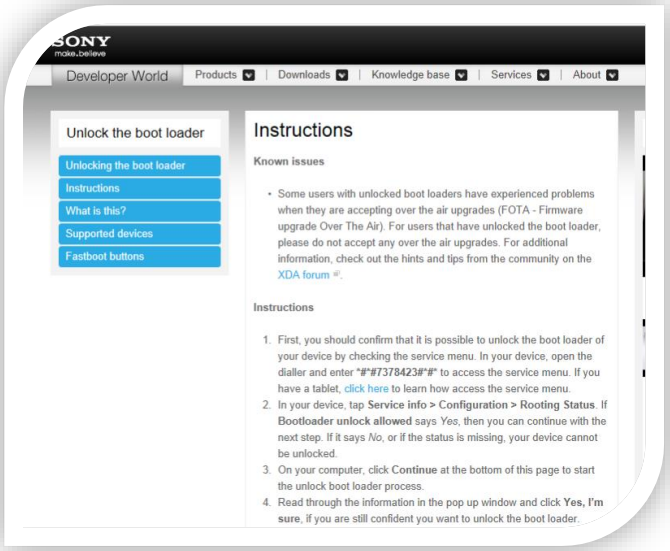
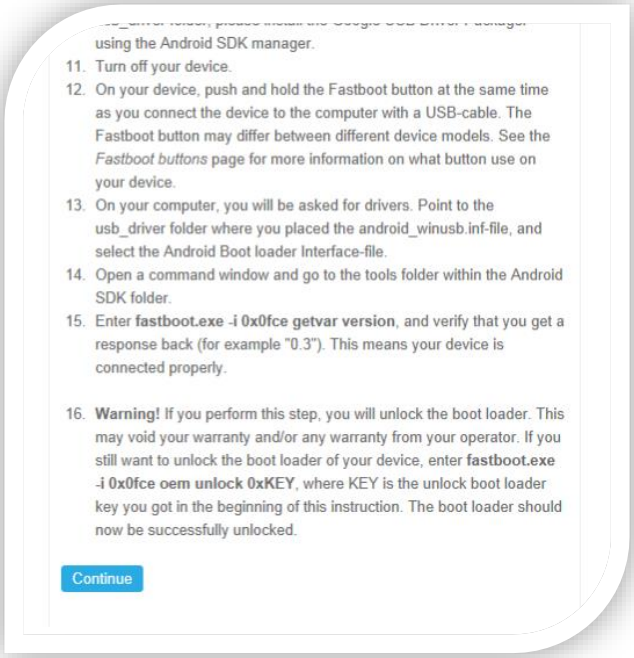


Figura 4 Página web Sony®


using the Android SDK manager.

11. Turn off your device.
12. On your device, push and hold the Fastboot button at the same time as you connect the device to the computer with a USB-cable. The Fastboot button may differ between different device models. See the *Fastboot buttons* page for more information on what button use on your device.
13. On your computer, you will be asked for drivers. Point to the usb_driver folder where you placed the android_winusb.inf-file, and select the Android Boot loader Interface-file.
14. Open a command window and go to the tools folder within the Android SDK folder.
15. Enter **fastboot.exe -i 0x0fce getvar version**, and verify that you get a response back (for example "0.3"). This means your device is connected properly.

16. **Warning!** If you perform this step, you will unlock the boot loader. This may void your warranty and/or any warranty from your operator. If you still want to unlock the boot loader of your device, enter **fastboot.exe -i 0x0fce oem unlock 0xKEY**, where KEY is the unlock boot loader key you got in the beginning of this instruction. The boot loader should now be successfully unlocked.

Continue

Figura 5 Términos y condiciones página web Sony®

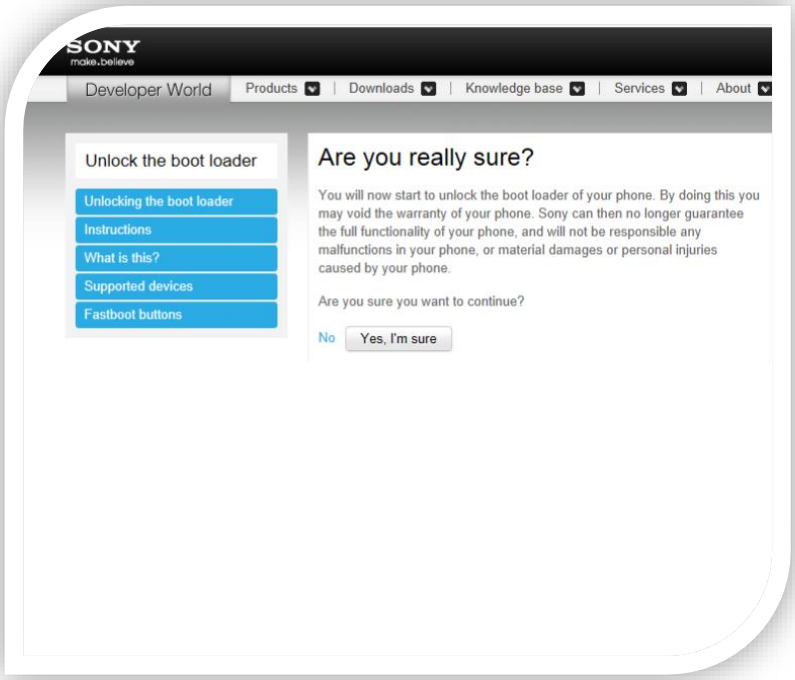


Figura 6 Términos páginaSony®

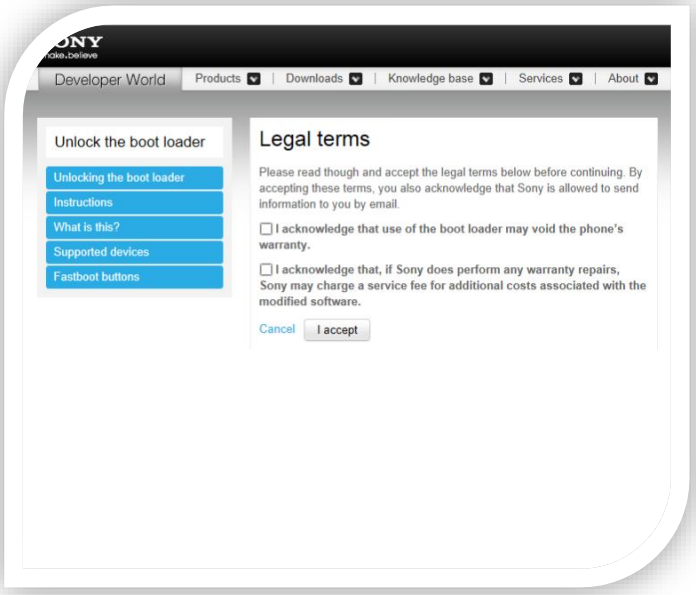


Figura 7 Aceptar términos páginaSony®

4. Introducir los datos conforme a las instrucciones.

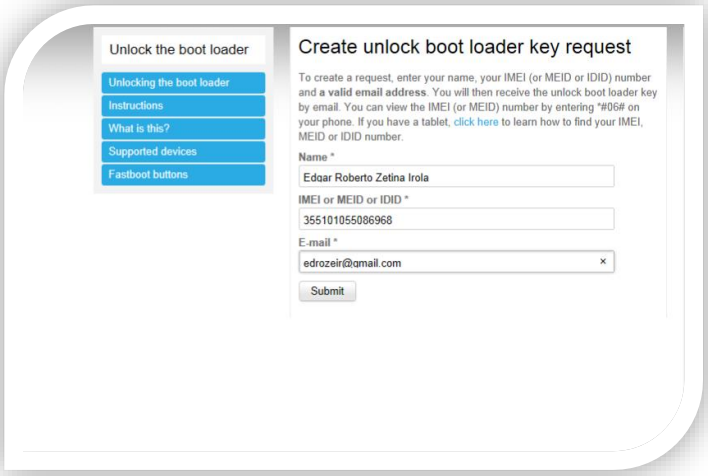


Figura 8 Creación de Bootloader páginaSony®

IMEI se puede encontrar marcando *#06# en el teclado del teléfono

Paso 4. Se Recibirá una KEY para desbloquear el bootloader en el correo. La KEY se encontrara en su bandeja de entrada.

Paso 5. Extraer todo los archivos que obtuvimos en el paso 2 en una carpeta

Paso 6. Poner el teléfono en modo fastboot

Modo Fastboot: Apague el teléfono. Mantenga pulsado el botón Subir volumen mientras conecta el teléfono al PC. Un LED azul se encenderá.

Paso 7. Instale el controlador de dispositivo

- 1: "Administrador de dispositivos" Buscar en el menú Inicio
- 2: Haga clic en el dispositivo (debe ser S1Boot Fastboot o teléfono Android®)
- 3: "Actualizar controlador''
- 4: Busque la carpeta de controladores (extraer 'Driver.zip')
- 5: Se instalará automáticamente.

Paso 8. Extraer el fastboot_with_Android®_USB_file.zip

Paso 9. En la misma carpeta en donde extraemos fastboot_with_Android®_USB_file.zip, abrir una ventana de comandos

Sostenga la tecla Shift mientras presionamos con el botón derecho en la carpeta 'fasboot' y seleccionar "Abrir ventana de comandos aquí"

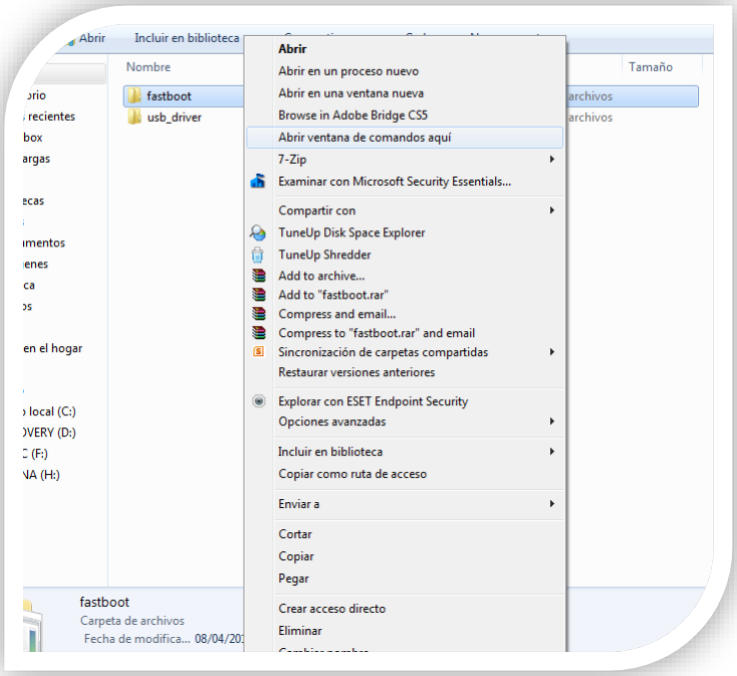


Figura 9 Carpeta Fastboot

Aparecerá la siguiente consola de comandos:

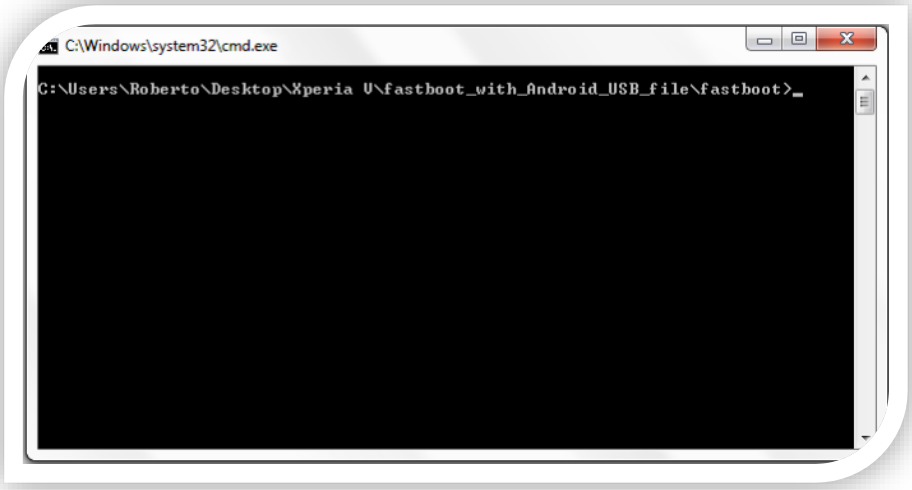


Figura 10 Fastboot línea de comandos

Paso 10. Está la parte importante. Escribir los siguientes comandos para desbloquear el bootloader

1) Escribir fastboot.exe -i 0x0fce getvar version

2) Se debe devolver un valor como "0,5". Esto asegura que el dispositivo está correctamente conectado

3) Luego escribir fastboot.exe -i 0x0fce oem unlock 0xKEY

el código que recibiste en tu correo Reemplazalo por KEY

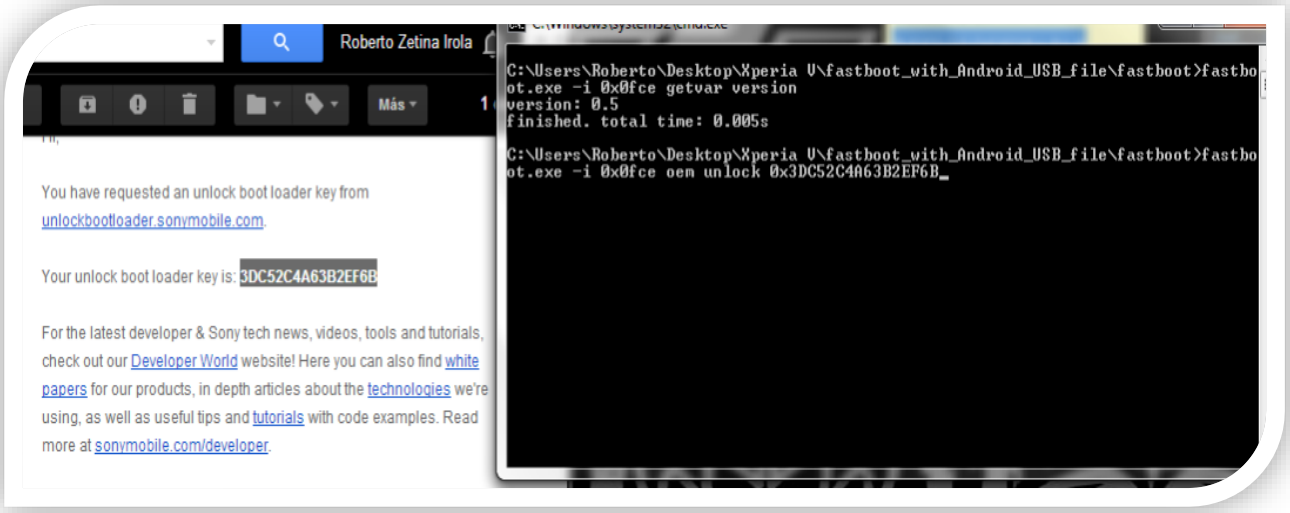


Figura 11 Código de desbloqueo y línea de comandos

Paso 11. Dar enter y cuando esté terminado, el bootloader del teléfono estará desbloqueado

Instalación de firmware

Previamente tenemos que tener descargado el programa flashtool e instalarlo, al igual que descargado el firmware.

Paso 1. Debemos mover el archivo e descargamos a la carpeta C: Flashtool>firmwares.

Paso 2. Abrir Flashtool.

Paso 3. Presionar botón de Flash

Figura 12 botón flash

Paso 4. Seleccionar el modo Flashmode.

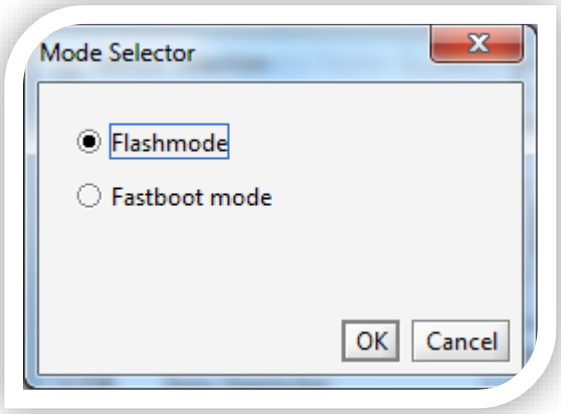


Figura 13 Flashmode

Paso 5. Seleccionar el firmware descargado y le damos a flash.

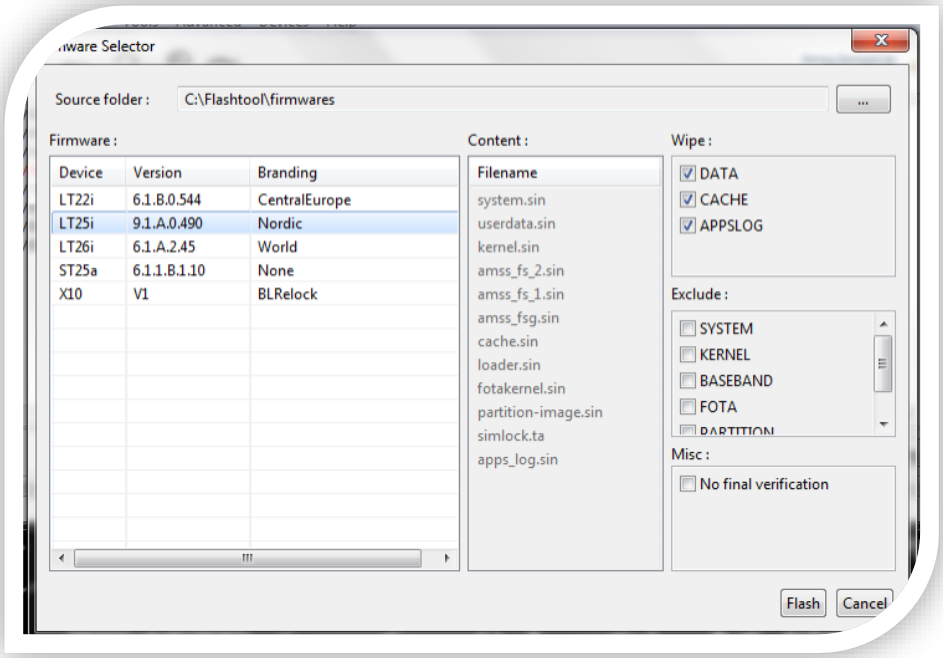


Figura 14 Selección de firmware

Paso 6. Luego cuando aparezca en la pantalla la siguiente ventana.

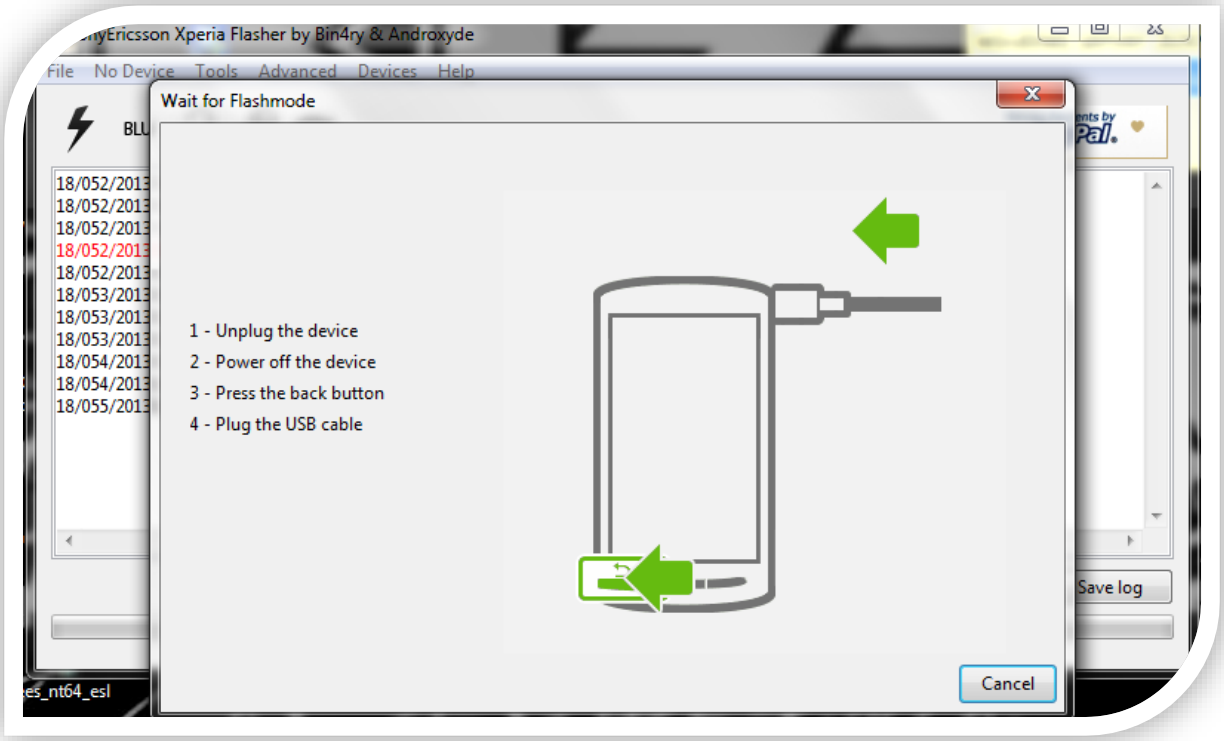


Figura 15 Poner teléfono en flashmode

Conectar el teléfono a la computadora en modo Flash, para ello con el teléfono apagado debemos mantener pulsada la tecla para bajar el volumen y sin soltarla conectar el cable a la computadora. Luego de esto comenzara a instalarse el firmware correspondiente.

Cuando termine tendremos instalado el firmware

Ahora proseguir con Flashear boot.img en Fastboot.

Paso 1. Conectar el teléfono en modo FastBoot.

Para esto antes de volver a conectar el teléfono al pc. Con el teléfono apagado mantener pulsada la tecla para subir el volumen, luego de esto sin soltar la tecla debemos conectar el teléfono con el cable Usb al Pc.

Paso 2. Volver a Flashtool.

Paso 3. Presionar botón de Flash.

Figura 16 botón flash

Paso 4. Seleccionar el modo Fastboot.

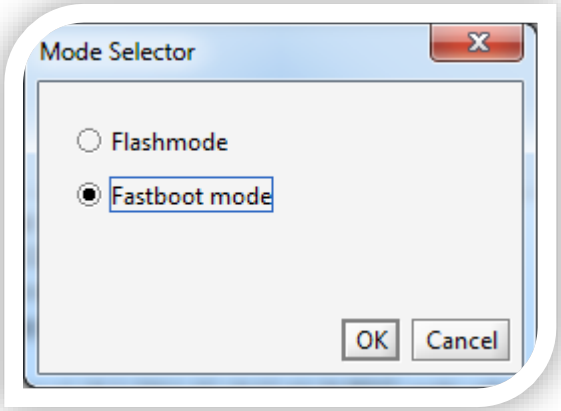


Figura 17 Fastboot mode

Paso 5. Seleccionar la opción "Select Kernel to Flash"

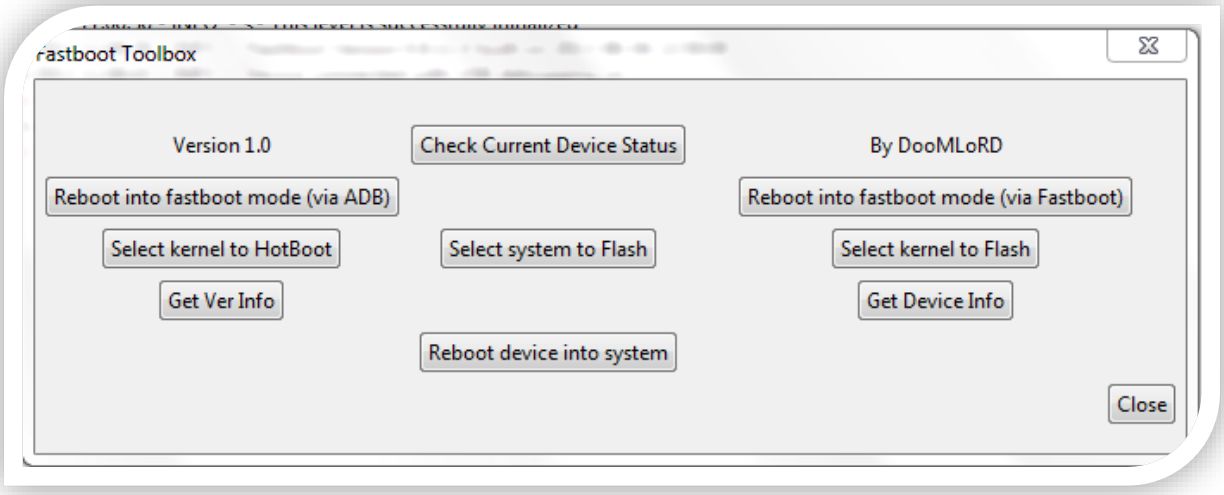


Figura 18 Fasboot Menú

Paso 6. Buscamos el archivo "boot.img" que descargamos y lo seleccionamos. Luego de seleccionarlo se instalará el Kernel y nos saldrá en el flashtool "Finished".

Instalación de la aplicación de Super Usuario "UPDATE-SuperSU-v1.04.zip" en el Recovery

Guardar en la tarjeta SD el archivo del SuperSu que descargamos "UPDATE-SuperSU-v1.04.zip".

Paso 1. Encender el teléfono y cuando nos salga el logo del Kernel presionar varias veces el botón de bajar el volumen del teléfono hasta que nos salga el recovery

Figura 19 Recovery Xperia

Paso 2. Dentro del recovery debemos seleccionar "install zip from sd-card" > luego choose zip from sd-card y nos saldrá un explorador en donde debemos seleccionar el archivo "UPDATE-SuperSU-v1.04.zip" que descargamos y le damos ***YES*** y el archivo empezara a instalarse

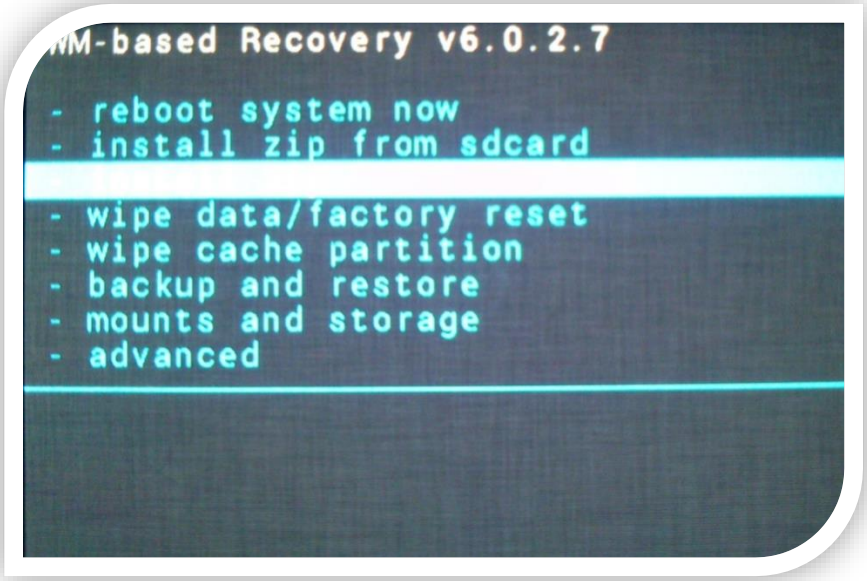


Figura 20 Menú recovery 1

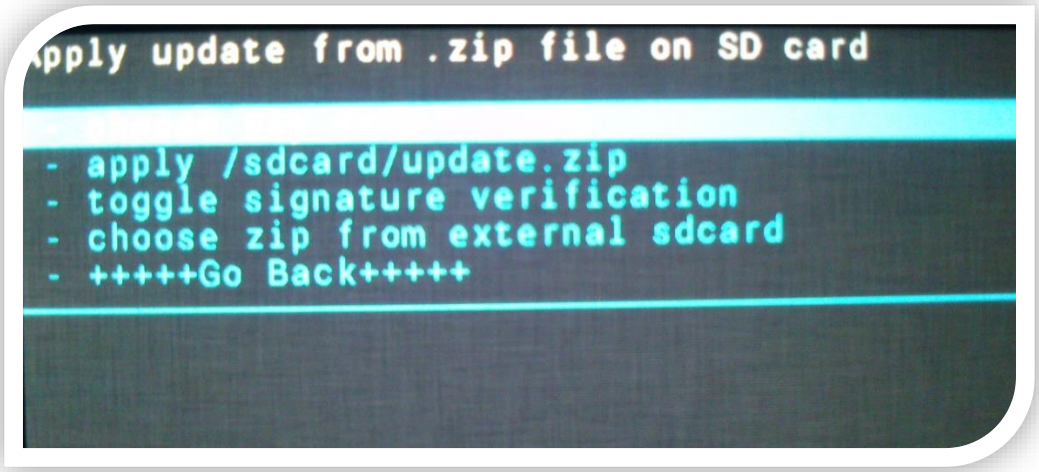


Figura 21 Menú recovery 2

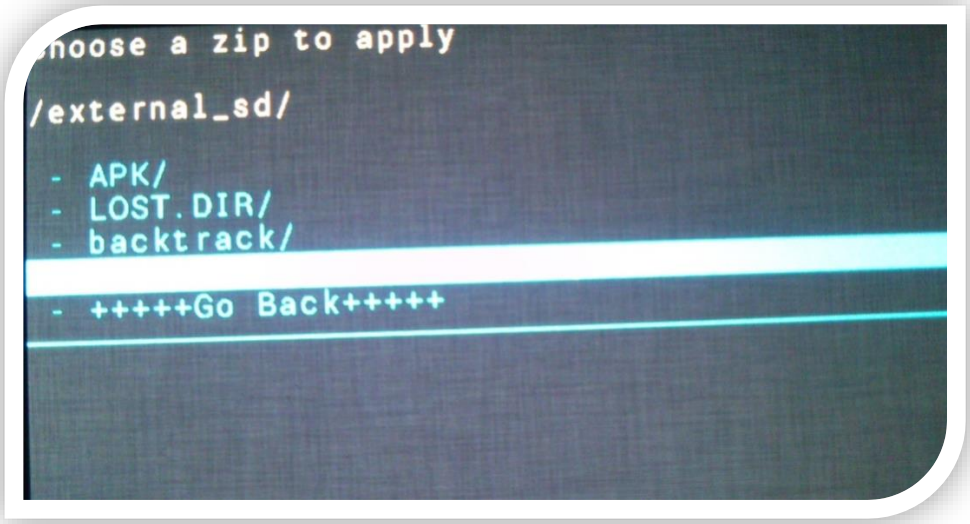


Figura 22 Menú recovery 3

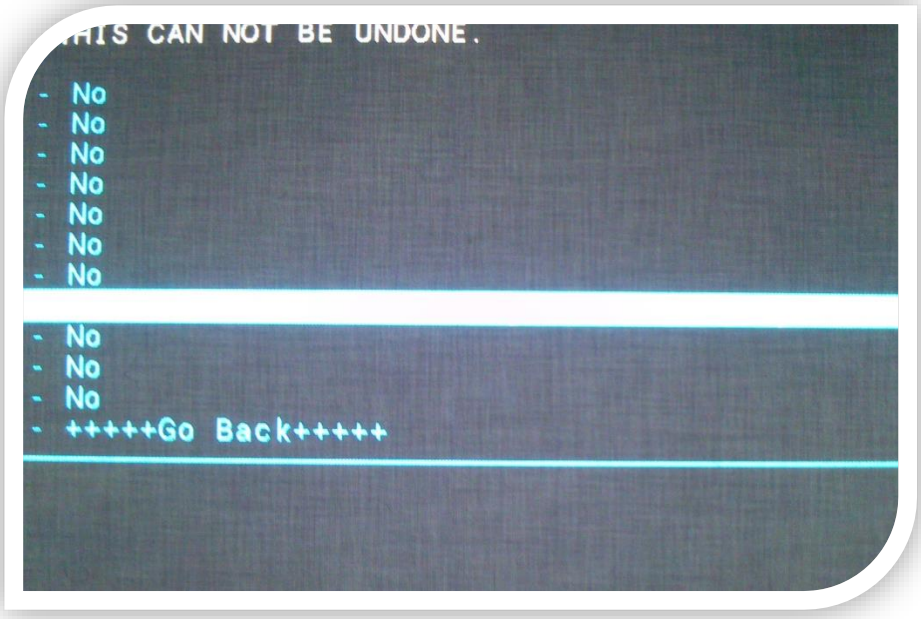


Figura 23 Menú recovery 4

Figura 24 Archivo Instalado Recovery

Paso 3. Después de haber instalado el archivo debemos apagar el teléfono.

Flashear el firmware con exclusiones

Paso 1. Volver al flashtool

Figura 25 Botón flash

Paso 2. Presionar botón de Flash.

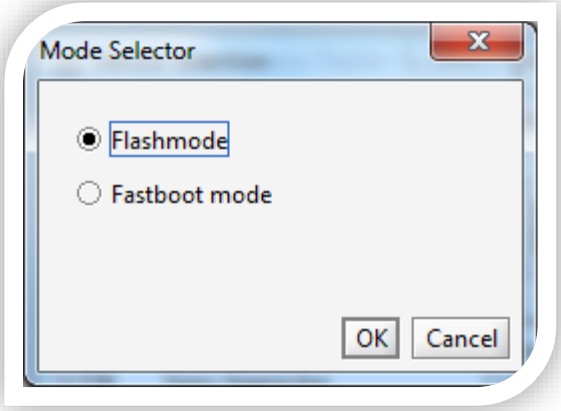


Figura 26 Flashmode

Paso 3. Seleccionar el firmware que descargamos, pero esta vez marcar las casillas "ExcludeSystem" y "ExcludeBaseband". Después de marcarlas le damos a OK.

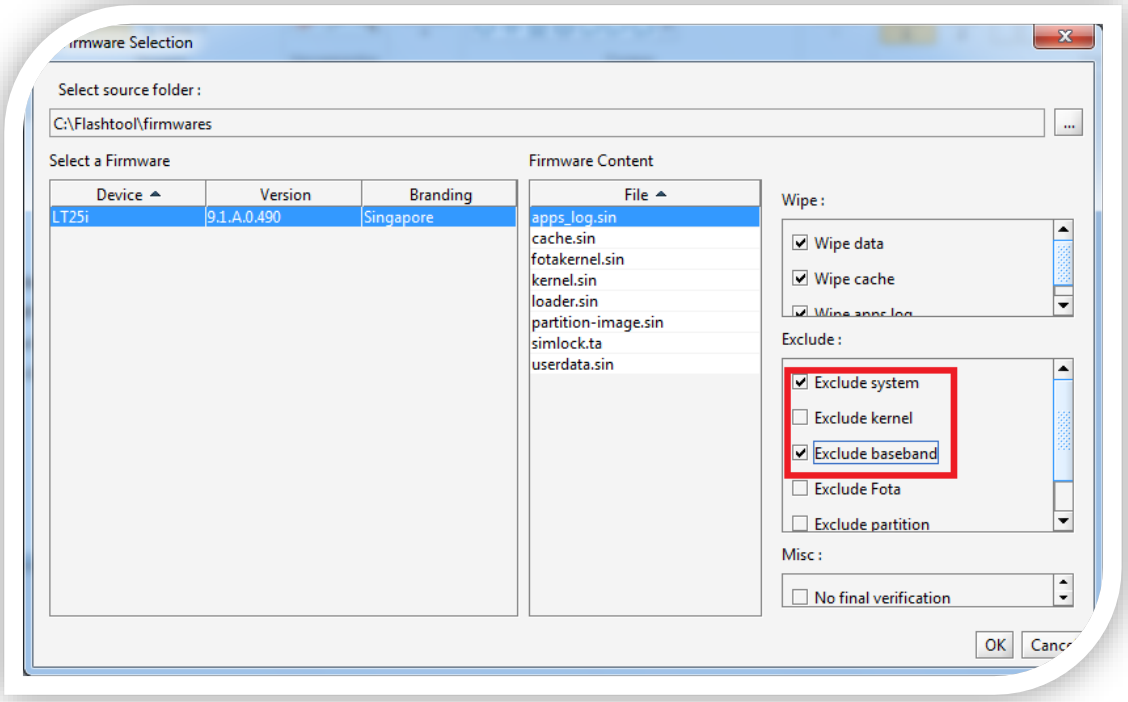


Figura 27 Menú firmware con exclusión

Paso 4. Luego cuando nos aparezca en la pantalla la siguiente ventana.

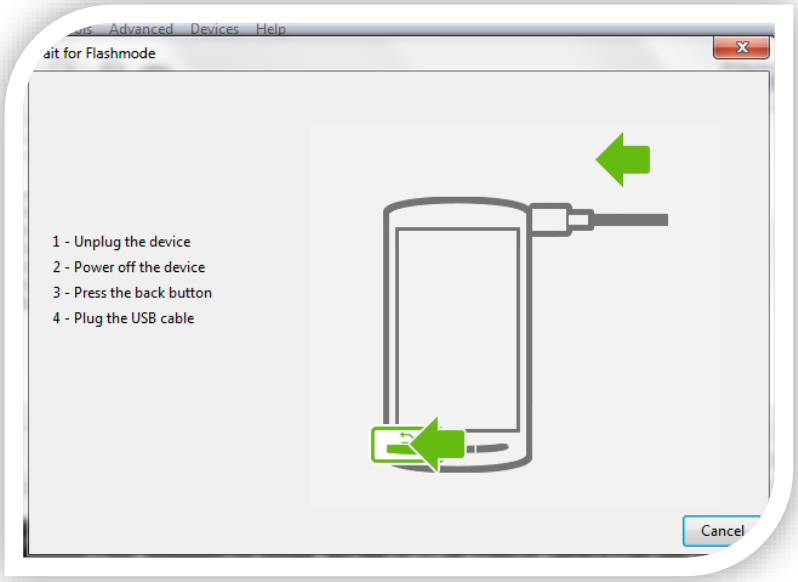


Figura 28 Poner teléfono en flashmode

Debemos conectar nuestro teléfono a la computadora en modo Flash, para ello con el teléfono apagado debemos mantener pulsada la tecla para bajar el volumen y sin soltarla conectar el cable a la computadora. Luego de esto comenzara a instalarse el firmware correspondiente.

Y al finalizar tendremos rooteado nuestro teléfono Xperia V

INSTALACION KALI LINUX EN EL SMARTPHONE

Teniendo el modo Root en el Smartphone instalar las siguiente aplicaciones que se pueden encontrar de manera gratuita en la playstore: Linux deploy, un VNC y el buxybox.

Configuración de Linux Deploy

Ya instalada las aplicaciones que utilizaremos para montar el sistema Operativo se procederá a la configuración del Linux Deploy y a la instalación del Kali Linux.

Paso 1. Ejecutamos el Linux Deploy y nos saldrá este recuadro tener conexión a internet para poder continuar).

Figura 29 Linux Deploy instalación 1

Paso 2. Una vez en Linux deploy seleccionar la flecha que apunta hacia abajo que se encuentra a un lado de stop. Aquí vamos a configurar las propiedades para la configuración.

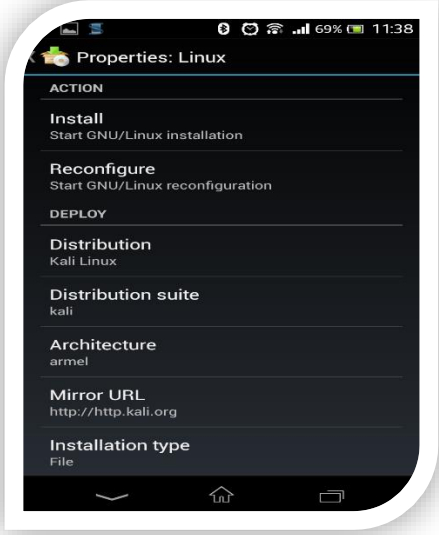


Figura 30 Linux Deploy instalación 2

Paso 3. Primero seleccionar donde dice distribución y ahí buscar en la lista que aparece la que dice Kali Linux.

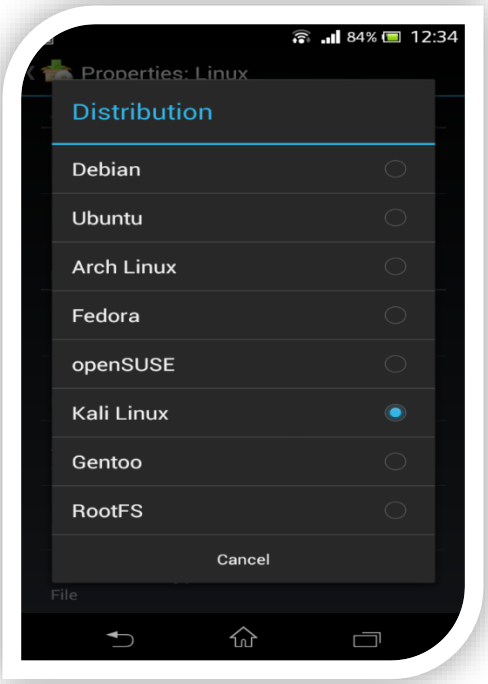


Figura 31 Linux Deploy instalación 3

Paso 4. Luego configurar donde se instalara. Para esto seleccionar donde dice *Installation path* poner en la tarjeta de memoria.

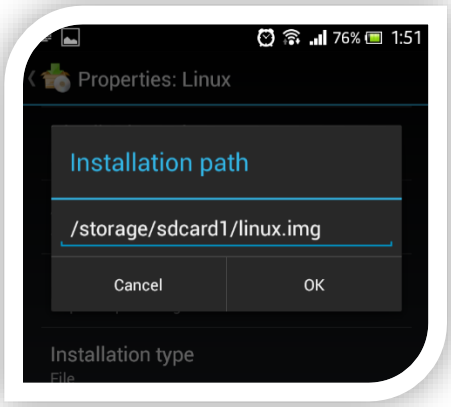


Figura 32 Linux Deploy instalación 4

Paso 5. Seguidamente bajamos en el menú de propiedades y nos vamos donde dice *Select Componets* ahí seleccionaremos lo básico que vamos a necesitar

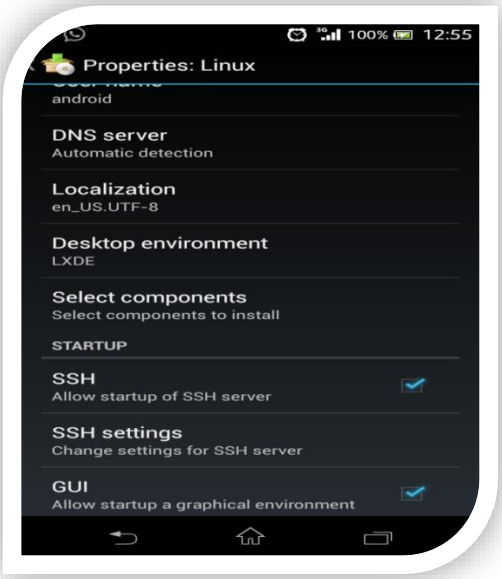


Figura 33 Linux Deploy instalación 5

Seleccionar *Desktop Enviroment* y *VNC* server. No podemos seleccionar *Kali components* por que en el sistema FAT32 solo nos permite tener un archivo de 4 Gb y no más grande y para que se instalen todos los componentes de Kali Linux necesitamos un archivo de 8 GB por lo tanto instalaremos las herramientas que se utilizarán dentro del Kali.

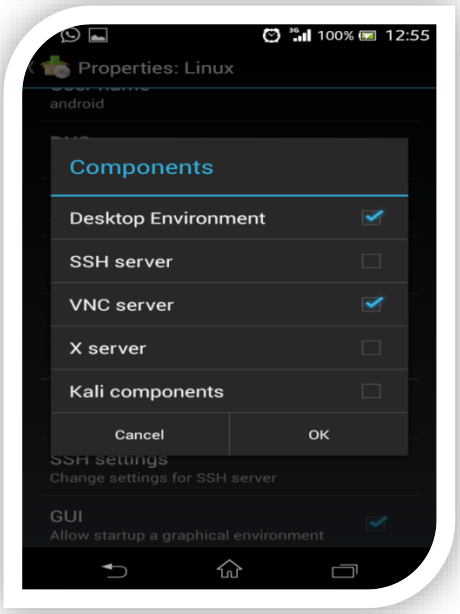


Figura 34Linux Deploy instalación 6

Paso 6. Luego configurar el archivo donde se configurara la resolución de Kali dependiendo de la resolución del teléfono para esto ir donde dice *GUI settings*

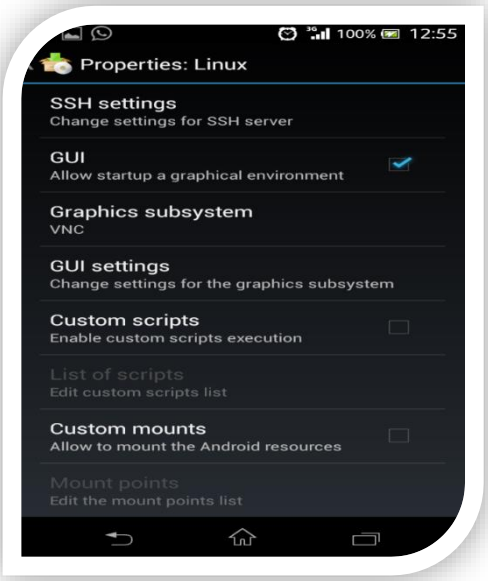


Figura 35 Linux Deploy instalación 7

En la ventana que aparecerá configurar la altura y la anchura de nuestra pantalla en pixeles.

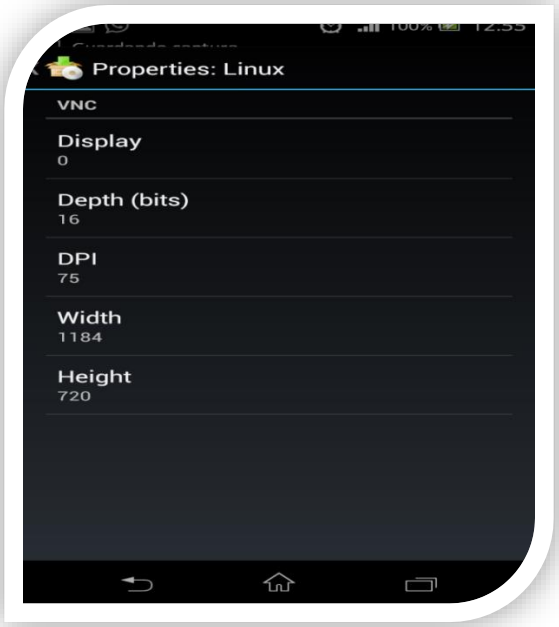


Figura 36 Linux Deploy instalación 8

Paso 7. Una vez realizadas estas configuraciones regresar al menú de propiedades y dar clic en *install*

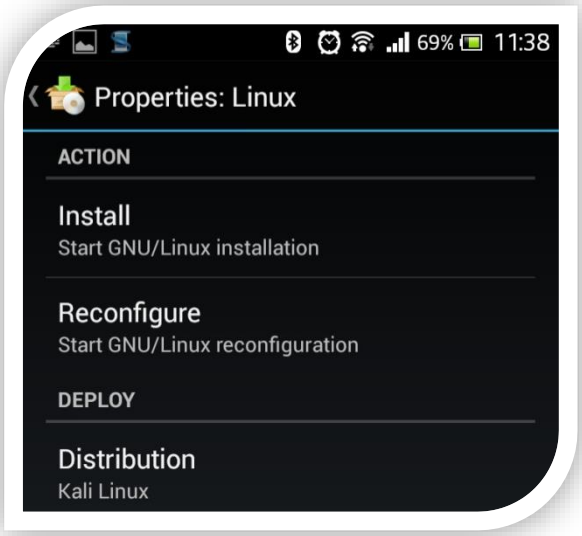


Figura 37 Linux Deploy instalación 9

Seguidamente comenzará la instalación primero empezará crear la imagen de 4 Gb en nuestra memoria donde se instalará el Kali Linux

Figura 38 Linux Deploy instalación 10

Ya creada la imagen comenzará a descargar e instalar el Kali Linux

Figura 39Linux Deploy instalación 11

Luego que termine de descargar nos dirá que se completó la instalación este proceso de instalación puede durar 30 m o más dependiendo de la velocidad de descarga.

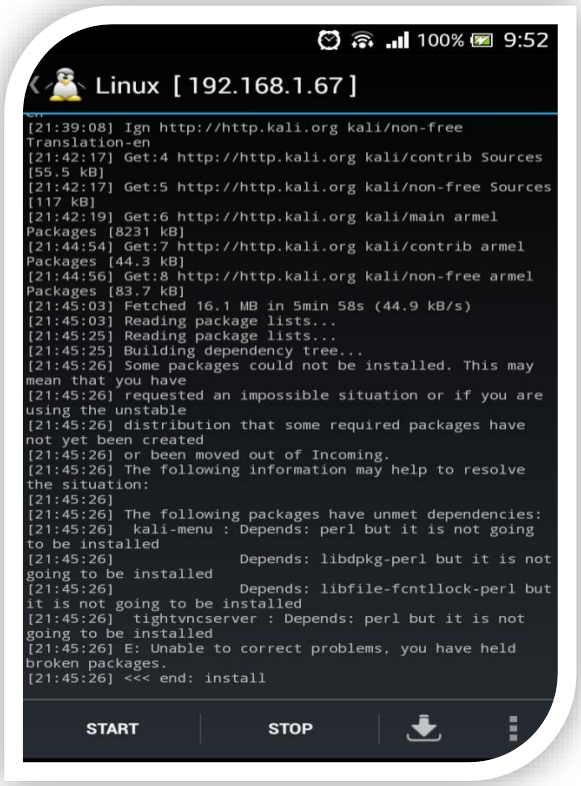


Figura 40Linux Deploy instalación 12

Iniciar Kali Linux

Ya que todo se instaló correctamente y se descargó el Linux proceder a correr el Kali

Paso 1. Abrir Linux Deploy dar clic en start. Si se instaló correctamente nos aparecerá lo siguiente:

Figura 41 Linux Deploy Start

Paso 2. Salir del Linux deploy con el botón de home y vamos al VNC que descargamos para configurarlo, una vez abierto el VNC solo configurar lo siguiente: en la conexión le poner el nombre de kali, en VNC *connection Type,* poner el nombre del servidor en este caso podemos escribir *localhost* porque se está ejecutando en el teléfono o la dirección 127.0.0.1 el puerto que se pondrá es el 5900 que utiliza el VNC del servidor, y en la contraseña escribir *changeme*.

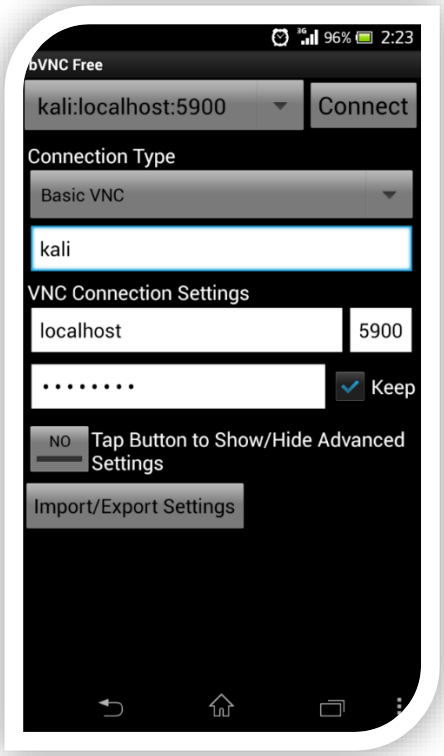


Figura 42 VNC configuración

Paso 3. Configurado lo que se indicó le damos clic en *connect* y abrirá Kali Linux corriendo si todo funcionó correctamente.

Figura 43 Kali encendido

Se puede observar la pantalla anterior cuando Kali se ejecuta.

Modo de operación

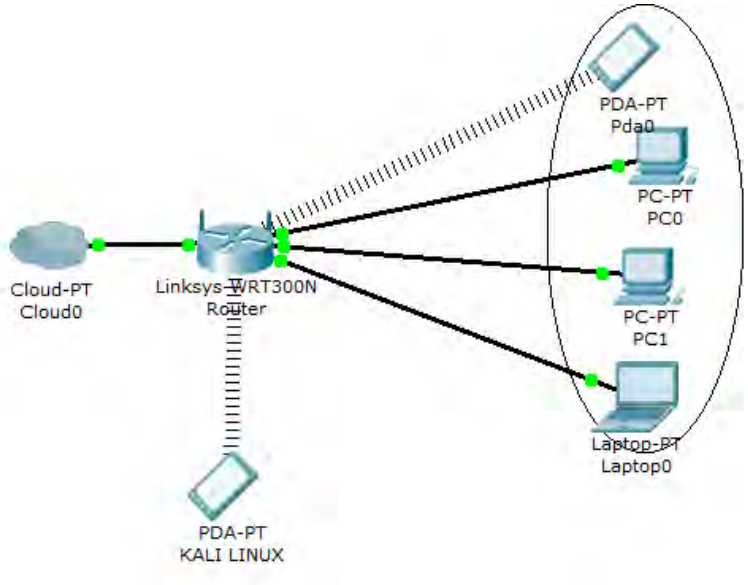


Figura 44 Diagrama comunicación

Como podemos ver en la figura 44 nuestro celular se conectaría al enrutador inalámbrico y todo lo que pase por ese enrutador será capturado por el celular. Se pueden observar las conexiones de las PC o las laptops, incluso los celulares que estén conectados.

Instalación de herramientas en Kali Linux

Ya que tenemos en ejecución el sistema operativo del teléfono procederemos a instalar algunas herramientas.

Instalación Nmap

Paso 1. Para la instalación del **nmap** abrir una terminal y entrar como modo súper usuario para esto en la terminal tecleamos $**su** y la contraseña, posteriormente tecleamos los comandos siguientes: $**apt-get install nmap**

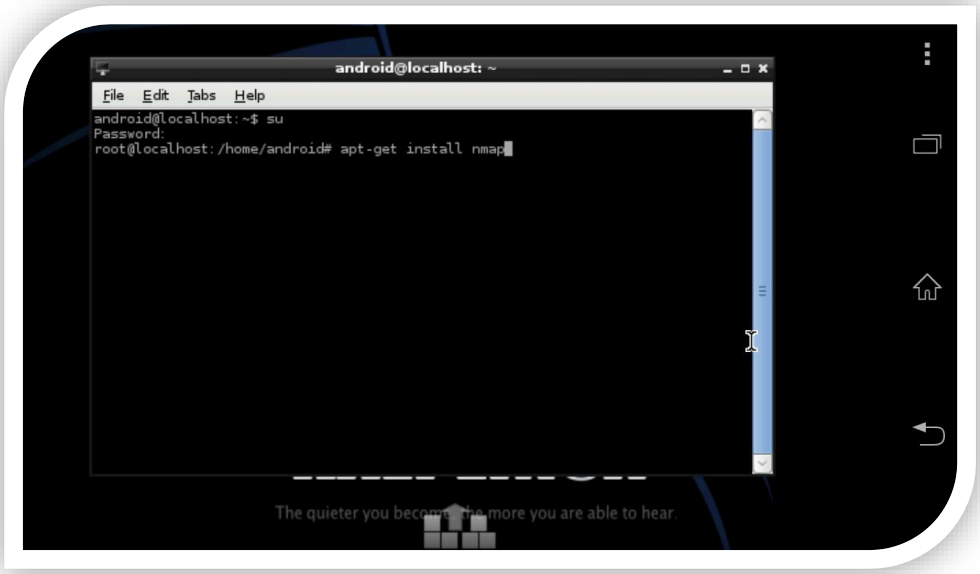


Figura 45 Instalación Nmap 1

Paso 2. Oprimir *enter* y empezará la instalación, preguntará si estamos de acuerdo que se instale y el tamaño que ocupará y le escribimos **Y,** respondiendo que sí**.**

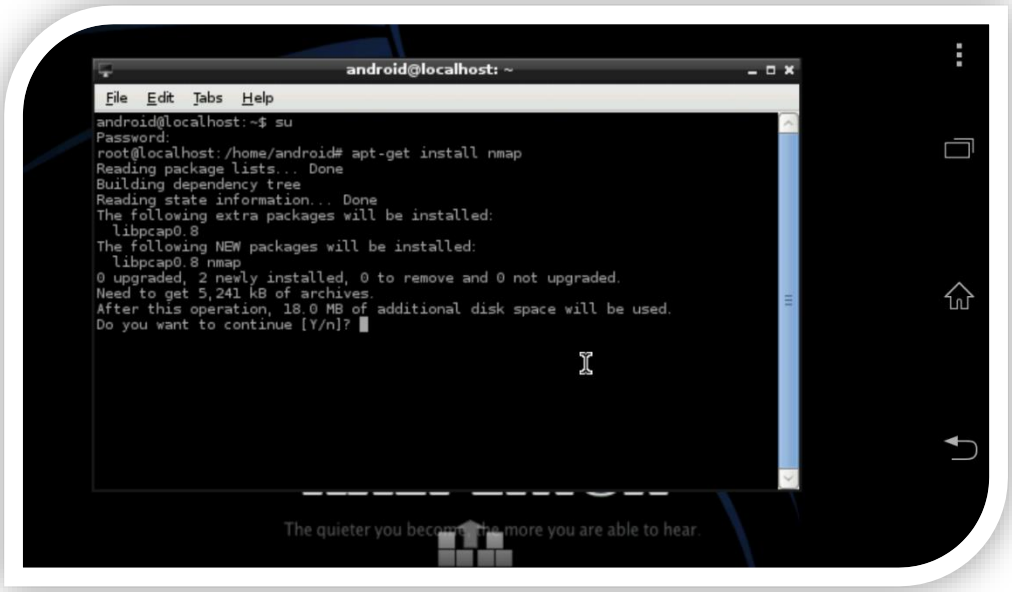


Figura 46 Instalación Nmap 2

Una vez que le demos que **si** para continuar procederá a descargar la aplicación y se instalará dentro nuestro Kali.

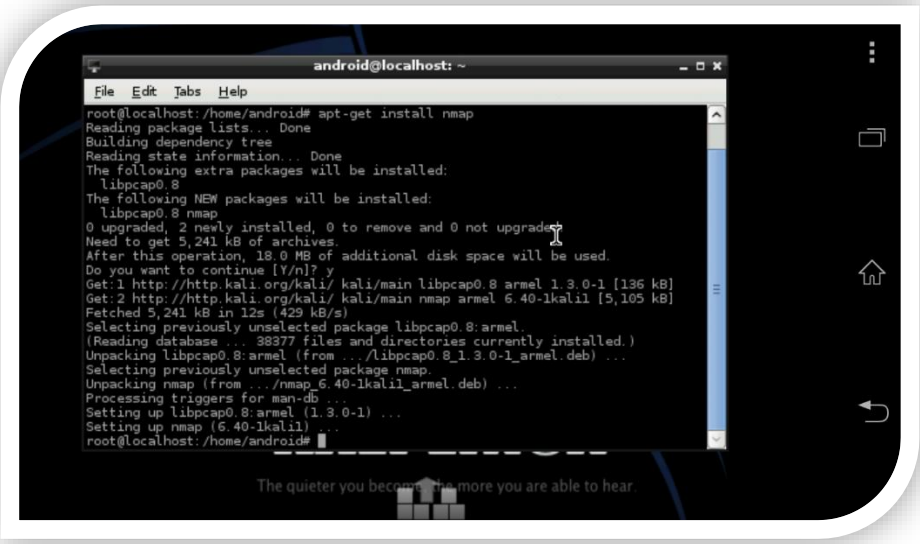


Figura 47 Instalación Nmap 3

Paso 4. Una vez instalada podemos hacer un escaneo sencillo a alguna ip de alguna pc que se encuentre dentro de la red para comprobar el funcionamiento de de nmap para esto podemos teclear lo siguiente $**nmap – Pn 192.168.1.74**

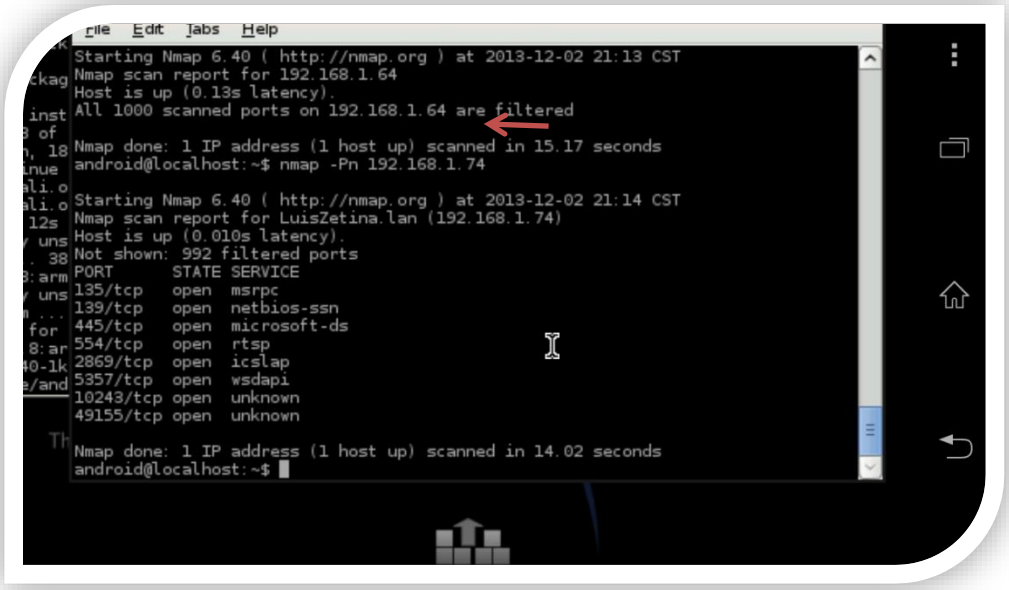


Figura 48 Nmap Prueba

Como se puede ver en la imagen 48 se analizó una ip con la paquetería Nmap y nos devolvió el nombre de la máquina y los puertos que tiene abiertos.

Instalación de Whireshark

Paso 1. Abrir la consola y ejecutamos el comando **#apt-get install wireshark** empezará la descarga y le damos Y para instalar el archivo.

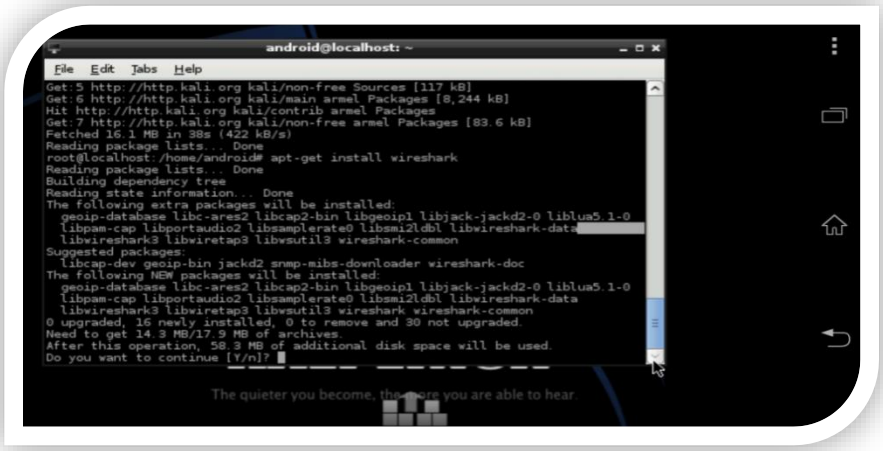


Figura 49 Instalación Wireshark 1

Empezará la descarga de las librerías

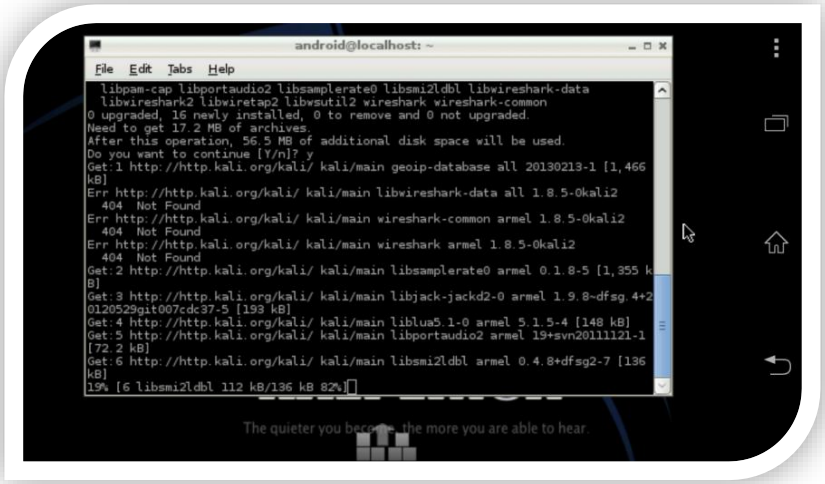


Figura 50 Instacion Wireshark 2

Paso 2. Al terminar ejecutamos el programa.

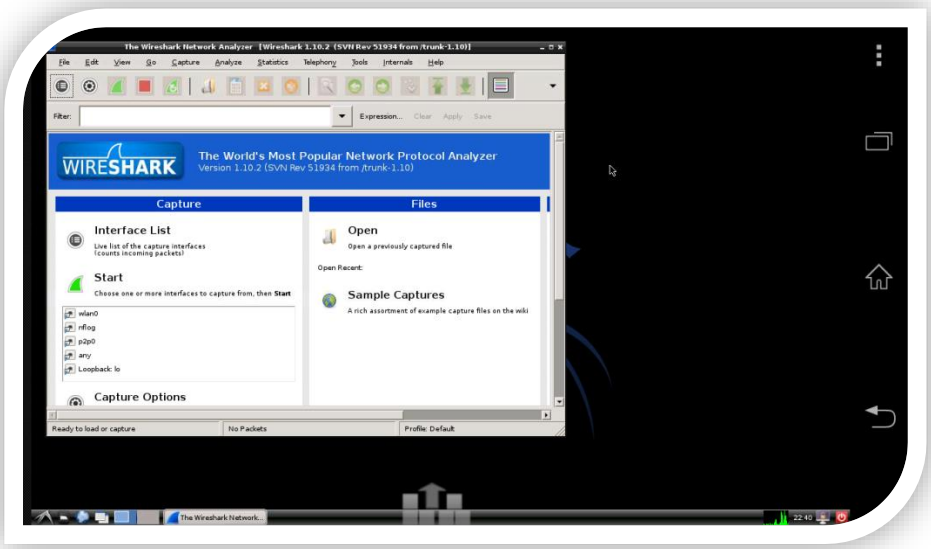


Figura 51 Wireshark Inicio

Paso 3. Nos vamos a la pestaña capture y seleccionar interfaces.

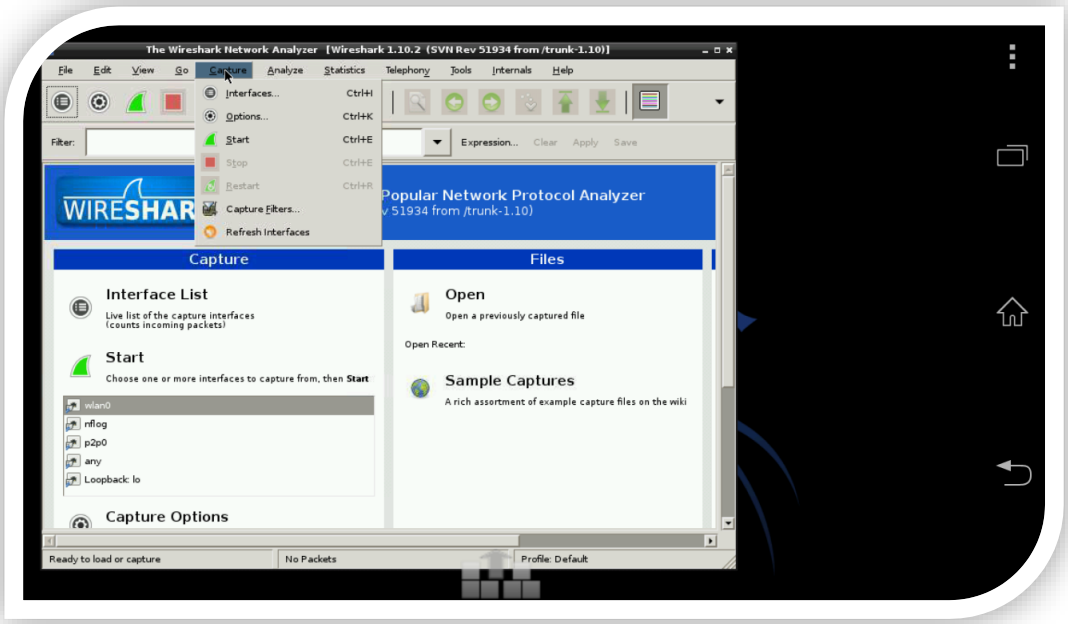


Figura 52 Wireshark configuración

Paso 4. Seleccionar la interface que vamos a analizar en este caso la inalámbrica y le damos en start

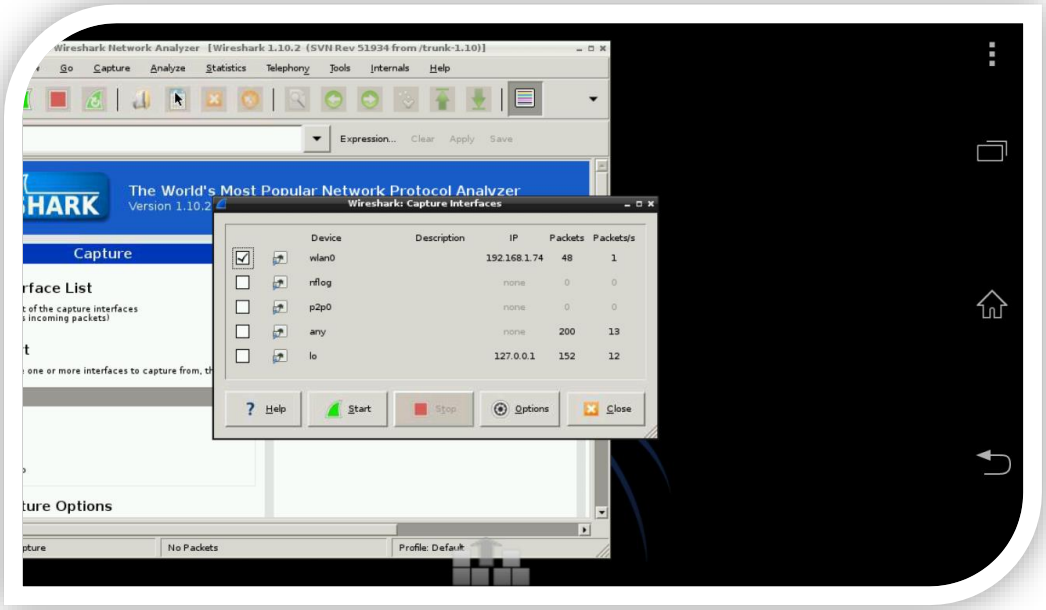


Figura 53 Wireshark Selección Interface

Ahora podemos ver todo lo que está pasando en la red donde estamos conectados

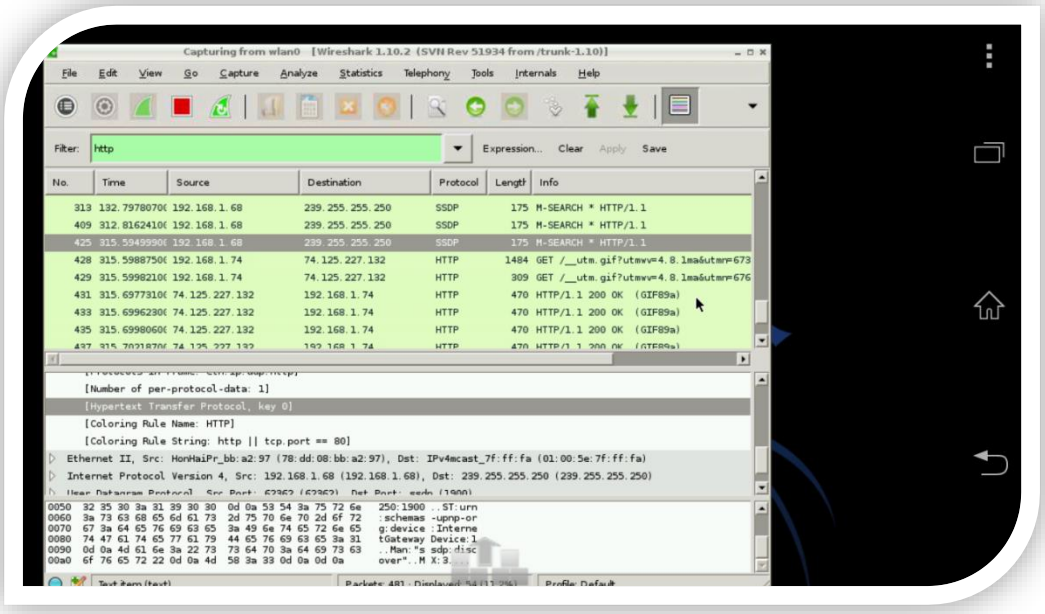


Figura 54 Wireshark prueba 1

Paso 5. En el filtro podemos indicar si queremos ver que hace un host o colocar un protocolo para ver con más detalle en este caso analizaremos lo que hace una IP puedes usar expresión para que te ayude a hacer el filtro

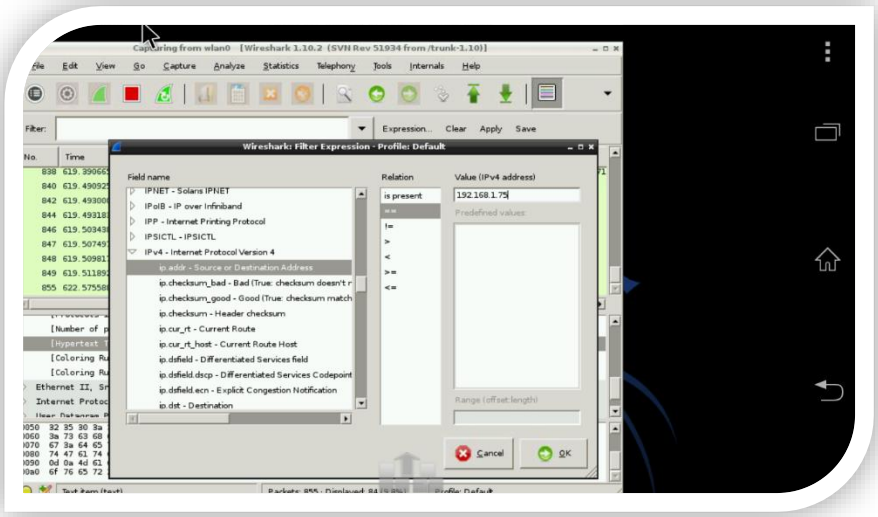


Figura 55 Wireshark prueba 2

Ya que colocamos nuestro filtro podemos ver todo lo que hace esa IP en la red y lo que está consultando y que protocolos, por ejemplo podemos ver como se sincroniza su *Dropbox.*

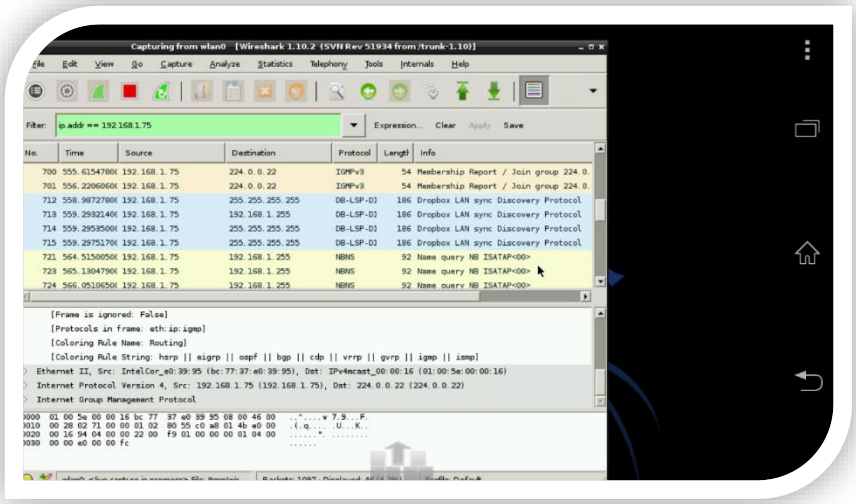


Figura 56 Wireshark prueba 3

CAPÍTULO 4

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores"

-- Kevin Mitnick

CAPÍTULO 4

4.1 PRUEBAS EN LA UNIVERSIDAD DE QUINTANA ROO

PENTESTING EN LA UQROO

El pentesting se realizará con el smartphone con sistema operativo Kali Linux y las herramientas mencionadas al principio del documento contenidas dentro de la distribución.

Prueba escaneo de vulnerabilidades

Las pruebas que se realizaron fueron de escaneo con Nmap la cual es una herramienta de escaneo de redes que permite identificar cuáles servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o firewalls, entre otros.

El propósito de esta herramienta es realizar distintos ataques en función del servicio, por ejemplo: un servidor web, un servidor de base de datos o un router perimetral. Por lo tanto, en cualquier despliegue, el primer paso será identificar los servicios en la infraestructura, para decidir cómo avanzar y cómo proceder.

Lo que se desea obtener con las pruebas de escaneo es identificar los host de la universidad, los servicios que están corriendo los y cuáles puertos tienen abiertos donde podrían ser atacados, así como los sistemas operativos que utilizan.

Prueba con Nmap 1.

Usando el comando **$nmap –PN** que significa como nombre tiene el no ping –PN no realiza ninguna técnica de descubrimiento, pasa directamente al análisis de puertos. Considera a todos los objetivos aptos para el análisis de puertos, como no se sabe la ip del servidor de la página de la Uqroo se realizó directo a la página utilizando el siguiente comando **$nmap –PN www.uqroo.mx**

Figura 57 Nmap prueba Uqroo 1

Da como resultado todos los puertos que abiertos y los servicios que se están ejecutando al igual que brinda la resolución DNS y así se pudo identificar cual es la dirección IP del servidor y cuál es la versión del sistema operativo.

Este resultado nos brinca bastante información de cuales puertos tiene abierto el servidor web de la universidad por lo cual los puertos que el atacante puede tomar para hacer un ataque esta información es importante para tomar medidas de cómo proteger los puertos que no se estén utilizando.

Prueba con Nmap 2.

Seguidamente una prueba para el sistema operativo la cual es un escaneo a un equipo en la cual nos dirá que sistema está usando el equipo

Para encontrar el sistema operativo se utiliza el comando -O el cual envía paquetes TCP y UDP al objetivo. Analiza las respuestas para conocer qué tipo de implementación de la pila TCP/IP tiene el objetivo.. El comando utilizado fue el siguiente para el servidor de la uqroo.mx **$nmap -O -osscan-supongo 192.100.164.38**

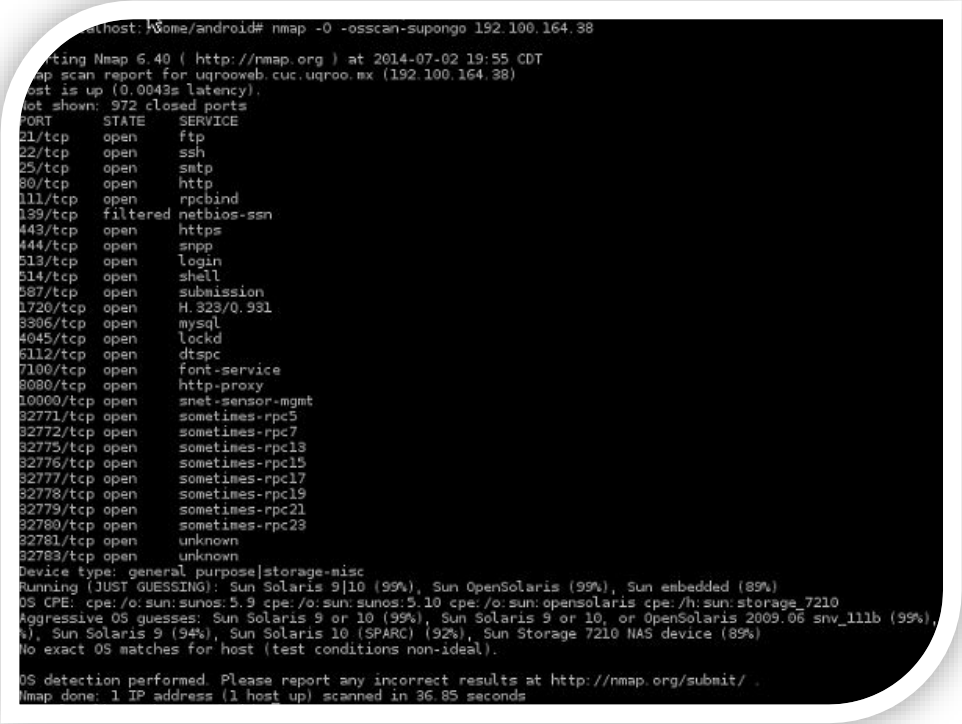


Figura 58 Nmap prueba Uqroo 2

El sistema operativo que utiliza el servidor donde está montada la página web de la Uqroo es Sun Solaris. Esta información puede ser muy importante para el atacante porque cada sistema operativo tiene sus diferentes vulnerabilidades con las cuales el atacante puede interactuar ya que no es lo mismo un ataque a un Windows que a un Linux.

Prueba con Nmap 3.

En esta prueba lo que se consiguió fueron ver cuáles son las versiones de las aplicaciones que están utilizando los puertos el estado, el servicio y la versión

El comando –sV interroga al conjunto de puertos abiertos detectados para tratar de descubrir servicios y versiones en puertos abiertos. **$nmap –sV 192.100.164.38**

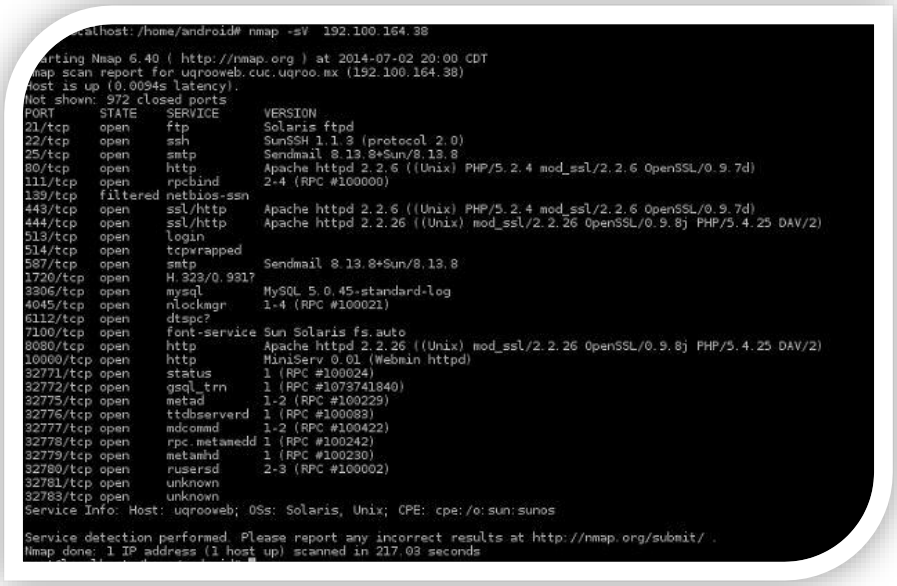


Figura 59 Nmap prueba Uqroo 3

La figura 69 indica los servicios que utiliza y cuáles versiones está usando.

Prueba con Nmap 4.

En esta prueba lo que se obtuvo fueron resultados de un segmento de red en el cual se obtuvieron que host están vivos y cuales son servidores y el nombre del Host, Para identificar si hay más servidores o que dispositivos se encuentran dentro de este segmento de red

Usando el siguiente comando **$nmap –sP 192.100.164.0/24**

Figura 60 Nmap prueba Uqroo 4

La figura 60 muestra todos los host que están encendidos y los servidores que se encuentran en el segmento 192.100.164.0/24.

Prueba con Nmap 5.

Por haberse detectado un firewall en la prueba anterior se realizaron pruebas en él utilizando **–sS** el cual envía un SYN. Es la técnica usada por defecto. Rápida, fiable y relativamente sigilosa. También denominada *half-open scan.* Al igual que el **–P0** Envía sondas IP con protocolo 1, 2 y 4. Acepta lista de protocolos**. –sV** para ver qué servicios estaban corriendo en él, y el **–O** para detectar el Sistema operativo.

Figura 61 Nmap prueba Uqroo 5

En esta prueba se pudo identificar a más detalle sin tanta información solo lo que se quería obtener que servicios y que puertos tiene abierto el firewall al cual le hicimos el escaneo.

Prueba con Nmap 6.

Se realizó pruebas a una IP cualquiera y se obtuvieron los siguientes datos:

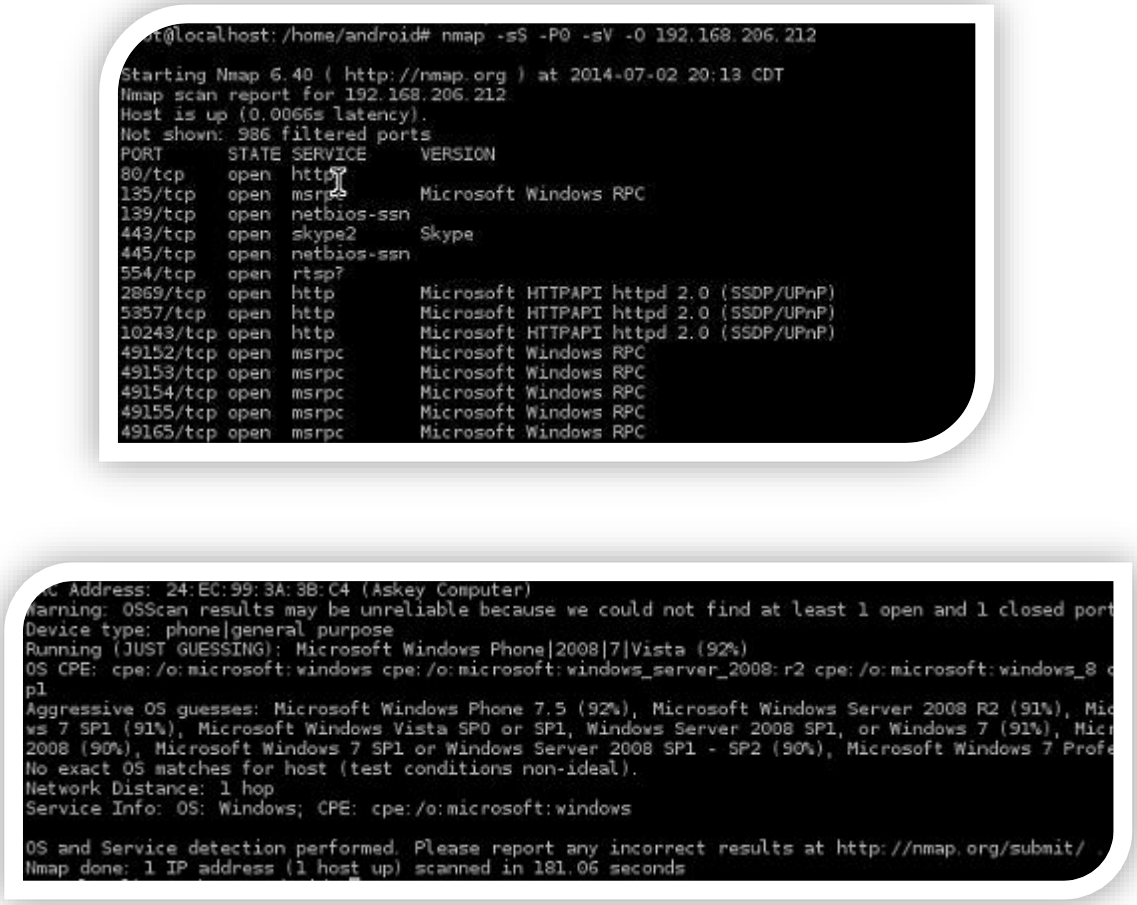


Figura 62 Nmap prueba Uqroo 6

Por lo que se puede apreciar en la figura 62 se trata de un teléfono móvil. El cual está ejecutando Windows móvil y aparte tiene activado su puerto de skype. En este caso un atacante podría utilizar esta información para utilizar programas que analice la comunicación de voz que se está teniendo en el skype .

Prueba con Nmap 7.

Se llevó a cabo una prueba al servidor de la página de la Uqroo para ver las rutas que tienen los paquetes para hacer esto se utilizó el comando –packet-trace **$namp –packet-trace 192.100.164.2**

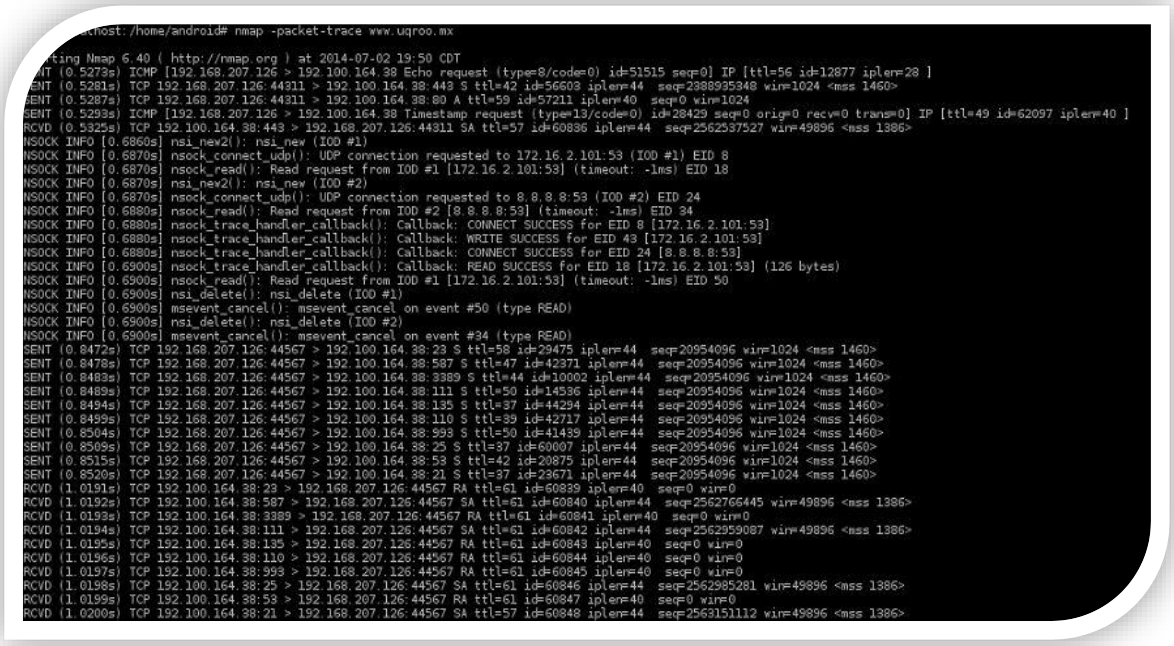


Figura 63 Nmap prueba Uqroo 7

Aquí nos muestra los paquetes de comunicación que envía y recibe durante el escaneo esta comunicación que existe se ve mejor con algunos programas de interfaz gráfica.

Pruebas de Sniffing

Para las siguientes pruebas se utilizó Wireshark el cual tiene la capacidad de capturar todos los paquetes que se envían y reciben a través de la red y se puede decodificar para su análisis. Al hacer cualquier cosa a través de Internet , tales como sitios web de navegación , utilizar VoIP , IRC , etc. , los datos siempre se convierte en paquetes cuando pasa a través de su interfaz de red o la tarjeta LAN . Wireshark la caza de esos paquetes en la capa de TCP / IP durante la transmisión y que se mantendrá, y presentar estos datos, en su " propia interfaz gráfica de usuario.

Es importante señalar que mientras que esta es una excelente herramienta para un administrador de red que necesita comprobar que sus clientes los datos sensibles se transmite de forma segura que también se puede utilizar ser utilizado por los piratas informáticos en redes no seguras

Prueba Wireshark

Para esta prueba se analizó el tráfico que pasaba a una IP en específico la cual es el servidor www.uqroo.mx

Se utilizó la expresión **ip.addrs** para ver la comunicación que va hacia el servidor web de la Uqroo cuando fue analizado con el Nmap, para utilizar la expresión solo se escribe **ip.addr** luego los operadores lógicos en este caso **==** y la ip del servidor.

.

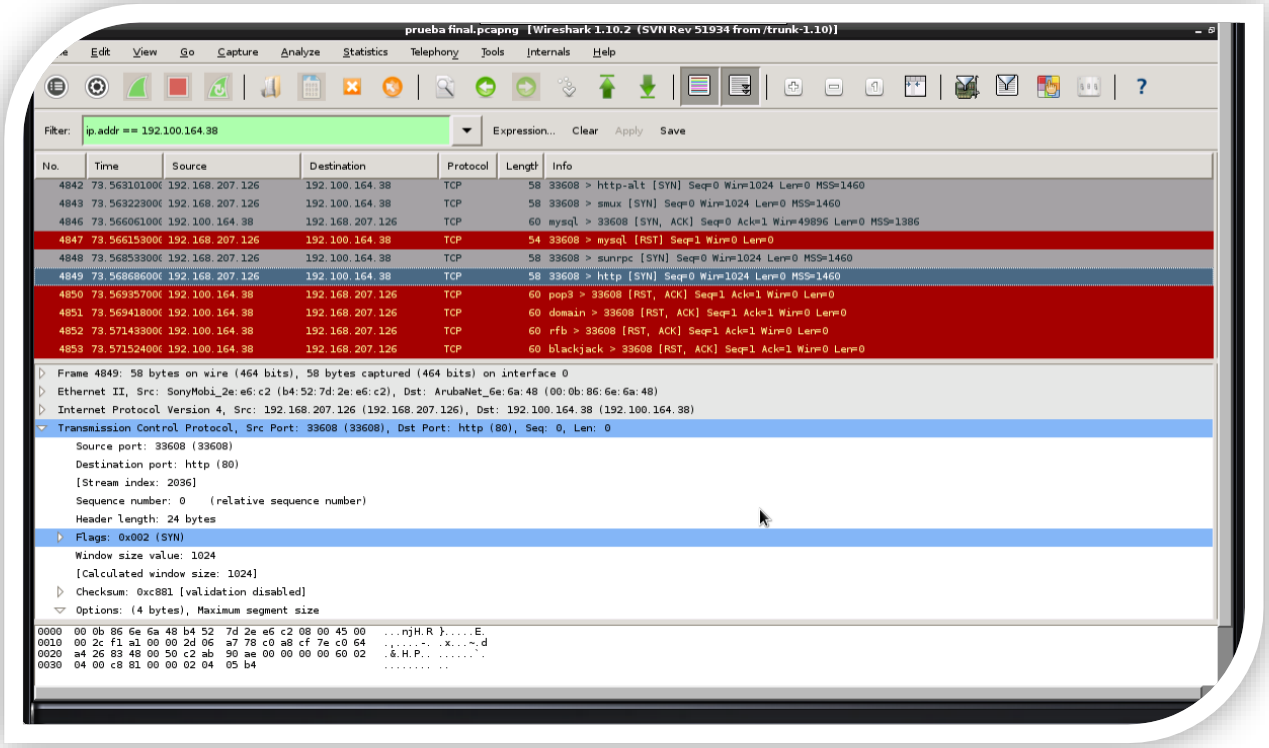


Figura 64 Wireshark análisis Uqroo 1

Se puede notar la comunicación TCP que hay entre el celular y el servidor de la Uqroo lamentablemente no se pueden ver otras comunicaciones que tiene ya que la tarjeta de red no permite estar en modo promiscuo y esas es una desventaja

En la imagen 65 se puede ver la comunicación entre el Smartphone y el servidor de la Uqroo en modo grafico la sincronización y la respuesta que se dan uno con el otro.

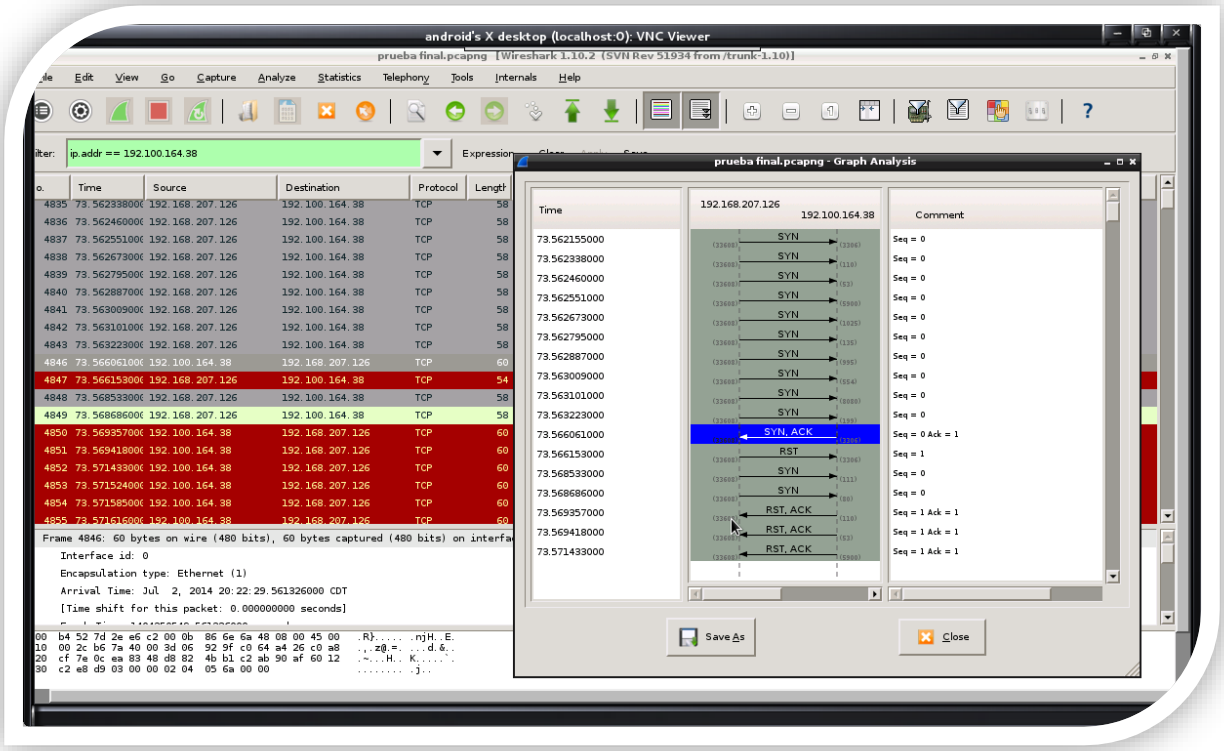


Figura 65 Wireshark análisis Uqroo 2

La imagen 66 muestra el protocolo http para ver las solicitudes de los host que hacen en la red hacia ese protocolo.

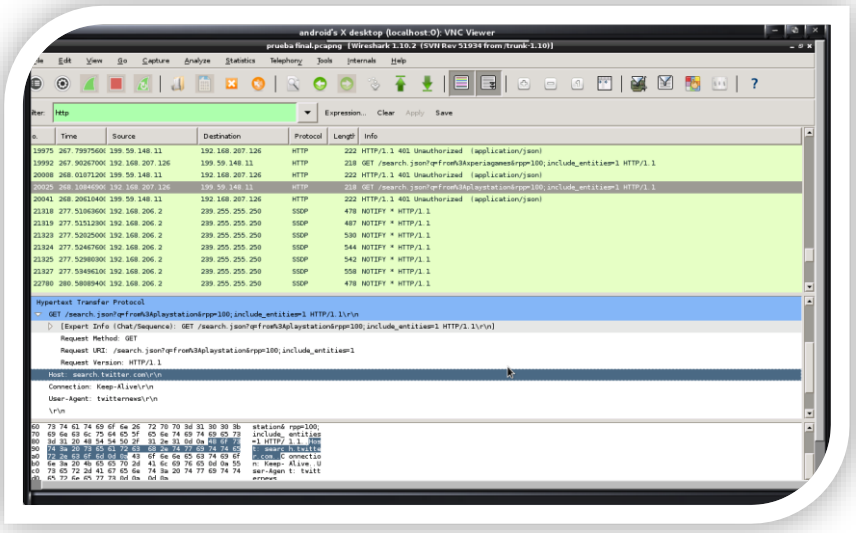


Figura 66 Wireshark análisis Uqroo 4

CONCLUSIONES

El *Pentesting* ha surgido con la finalidad de aprender de las vulnerabilidades de los dispositivos informáticos y es una buena herramienta para encontrar dónde están los puntos débiles y buscar una solución antes de sufrir un ataque, previniéndolo o en un determinado momento deteniéndolo, para esto está el hacking ético que se refiere a ser un hacker pero con ética profesional.

Con el desarrollo de este trabajo se puede apreciar que para contrarrestar el daño, que puede causar un hacker malicioso en cualquier dispositivo informático, los Smartphone y las tabletas son herramientas viables y muy útiles. Además presentan las ventajas de ser pequeños y discretos (condiciones que pueden ser muy importantes durante un ataque).

Presento un posible escenario de Pentest a través de un Smartphone, el cual pasa desapercibido, ¿quién se podría imaginar que estoy escaneando una red a través de él? Y no sólo se escaneo la red, también fue posible realizar pruebas y comprobar hasta donde pueden llegar y hasta donde se puede explotar este dispositivo inteligente. Sirve además para llevar al lector a adentrarse un poco más en el mundo del Pentesting y algunas herramientas las cuales puede utilizar para lograr este tipo de pruebas de seguridad.

La implementación de Kali Linux respondió bien a las limitaciones: se ejecutó sin problema alguno en un dispositivo móvil que no se diseñó para tal fin. Al utilizar un *Smartphone* se tienen muchas limitaciones como por ejemplo con el *kernel* del sistema del teléfono, la tarjeta de red inalámbrica que no era compatible al 100%, limitaciones de espacio, cantidad mínima de RAM y menor poder de procesamiento comparado con una computadora común.

Las pruebas obtenidas al realizar un escaneo de vulnerabilidades nos permiten identificar que:

- La red informática universitaria es susceptible de permitir escaneos de diferentes tipos sin presentar una estrategia para limitar estos.
- Permite identificar sistemas operativos activos.
- Permite identificar puertos abiertos, bloqueados o cerrados.
- Puede identificar que host están vivos en la red
- Se puede implementar una aplicación sniffer y espiar las comunicaciones

Con los resultados obtenidos ya se pueden llegar a conclusiones de cuáles serían los puntos débiles y empezar a trabajarlos con el administrador de la red para que

los ataques, se puedan prevenir tales como habilitar filtros o deshabilitar los puertos abiertos que no estén siendo utilizados.

Así como fueron identificados estas vulnerabilidades con un dispositivo de bolsillo con equipos más sofisticado se pueden hacer mayores cosas por lo tanto hay que prevenir estos ataques que van evolucionando constantemente, las herramientas y los métodos de hacking. Este escenario con el Smartphone es muy bueno para unas primeras pruebas y saber cuáles son las vulnerabilidades de la red para luego saber que otras herramientas se deberían usar para seguir el ataque.

Finalmente pienso que día con día estos dispositivos irán evolucionando a tal grado que no presenten tantas limitaciones y se puedan hacer pruebas más robustas a través de ellos pero como dispositivo para dar una primera impresión en una prueba de *Pentes*t lo considero todo un éxito.

Gracias.

REFERENCIAS

© Copyright 2014, Offensive Security. (28 de Febrero de 2013). *kali.org*. Recuperado el 10 de 01 de 2014, de http://es.docs.kali.org/introduction-es/que-es-kali-linux

Xataka Mexico. (12 de Febrero de 2012). Recuperado el 12 de febrero de 2014, de http://www.xataka.com.mx/sistemas-operativos/que-es-la-arquitectura-arm

Aircrack-ng, C. 2.-2. (25 de 09 de 2009). *aircrack-ng.org*. Recuperado el 2014 de 02 de 02, de http://www.aircrack-ng.org/doku.php?id=getting_started

Alfon. (17 de 08 de 2003). *http://www.maestrosdelweb.com*. Recuperado el 19 de 06 de 2014, de http://www.maestrosdelweb.com/snort/

Catoira, F. (21 de Agosto de 2012). *hackersenlared*. Recuperado el 02 de Febrero de 2014, de https://hackersenlared.wordpress.com/category/capacitacion/que-es-un-pentest/

Demon. (08 de 05 de 2008). *http://nuestrasfrikadas.blogspot.mx/*. Recuperado el 06 de 09 de 2014, de http://nuestrasfrikadas.blogspot.mx/2009/05/nessus-el-escaner-de-vulnerabilidades.html

Giacobbi, G. (1 de 11 de 2006). *http://netcat.sourceforge.net/*. Recuperado el 10 de 22 de 2014, de http://netcat.sourceforge.net/

Herzog, P. (2003). *Manual de la Metodología Abierta de Testeo de Seguridad.* OSSTMM.

Kamel, J. (11 de 2012). *http://antisec-security.blogspot.mx/*. Recuperado el 21 de 09 de 2014, de http://antisec-security.blogspot.mx/2012/11/burp-suite-professional-burp-suite-es.html

Ltd, C. ©. (1 de 10 de 2013). *portswigger.net*. Recuperado el 2014 de 01 de 03, de http://www.portswigger.net/burp/

Lyon, G. ". (2008). *NMAP Network Scanning.*Sunnyvale : Insecure.com.

Lyon, G. (07 de 05 de 2010). *http://nmap.org/*. Recuperado el 22 de 06 de 2014, de http://nmap.org/man/es/

Maulini, M. (4 de Diciembre de 2010). *http://tecnologiasweb.blogspot.mx/*. Recuperado el 01 de febrero de 2014, de

http://tecnologiasweb.blogspot.mx/2010/12/que-es-pen-test-herramientas-de-pen.html

Newman, A. W. (2005). *Pentration Testing and Network Defense.* Indianapolis: Cisco Press.

Peines, G. (18 de 06 de 2013). *wireshark.org*. Recuperado el 2014 de 02 de 05, de http://www.wireshark.org/about.html

Salazar, J. E. (1 de 04 de 2011). *http://siriushack.blogspot.mx*. Recuperado el 22 de 10 de 2014, de http://siriushack.blogspot.mx/2011/04/manual-basico-de-metasploit-by-thejez.html

SRAKERIM. (02 de 02 de 2011). *http://cursoredlocal.wordpress.co*. Obtenido de http://cursoredlocal.wordpress.com/2011/02/02/envenenamiento-arp-ettercap-iv/

SRAMEKIM. (30 de 01 de 2010). *http://cursoredlocal.wordpress.com*. Recuperado el 22 de 10 de 2014, de http://cursoredlocal.wordpress.com/2011/01/30/john-the-ripper-windows-v1-7-6/

T. J. Klevinsky, S. L. (2002). *Hack I.T.: Security Through Penetration Testing.* Addison-Wesley.

Zero13. (24 de 11 de 2008). *http://www.zero13wireless.net/*. Recuperado el 02 de 08 de 2014, de http://www.zero13wireless.net/foro/showthread.php?5608-Noticia-Seguridad-Ataques-practicos-contra-WEP-y-WPA-WPA-al-Descubierto-!!!