



Análisis de las comunicaciones móviles

Autor: Juan Pinilla Jiménez

Tutor: Joan Caparrós Ramírez.

Profesor: Helena Rifà Pous

Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones

(MISTIC)

Análisis de datos

Fecha de entrega: Junio 2020



Esta obra está sujeta a una licencia de Reconocimiento-NoComercial- CompartirIgual
[3.0 España de Creative Commons.](https://creativecommons.org/licenses/by-nc-sa/3.0/es/)

FICHA DEL TRABAJO FINAL

Título del trabajo:	<i>Análisis de las comunicaciones móviles</i>
Nombre del autor:	<i>Juan Pinilla Jiménez</i>
Nombre del colaborador/a docente :	<i>Joan Caparrós Ramírez</i>
Nombre del PRA:	<i>Helena Rifà Pous</i>
Fecha de entrega (mm/aaaa):	<i>06/2020</i>
Titulación o programa:	<i>Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones(MISTIC)</i>
Área del Trabajo Final:	<i>Análisis de datos.</i>
Idioma del trabajo:	<i>Español</i>
Palabras clave	<i>Proxy, IDS, SIEM, Móvil.</i>
Resumen del Trabajo:	
<p>La finalidad de este trabajo, se basa en analizar las comunicaciones móviles para detectar comportamientos extraños que delaten una posible infección o vulneración del dispositivo analizado. Para ello, se ha implementado con software gratuito Pila de Elastic y con hardware de bajo coste, una Raspberry Pi.</p> <p>En la Raspberry Pi, se ha instalado un Proxy MIM en modo transparente para recoger todas la comunicaciones que realiza el móvil, y además, un sistema de detección de intrusos Suricata para detectar cualquier posible amenaza, también, se ha instalado parte de la pila Elastic en este caso Filebeat.</p> <p>Para el posterior análisis de datos, se ha optado por la solución de Elastic que ofrece en la nube, en ella podemos realizar múltiples filtros (Logstash) vistas y Dashboard (Kibana) para analizar el comportamiento del dispositivo y sus posibles riesgos y amenazas.</p> <p>Finalmente, se hicieron distintas pruebas para demostrar que nuestro sistema era capaz de captar las vulnerabilidades y brechas que podrían presentar los dispositivos móviles, una vez que se captan esas vulnerabilidades, se informa mediante correo al usuario para que actúe consecuentemente a la amenaza recibida.</p>	
Abstract:	
<p>The main point in this proyect belongs to analyze the mobile communications to detect strange behaviors which brings out a possible infection or vulnerability of the analyzing device. Moreover it's been updated with a free software "Elastic Pila" and a low cost hardware, The Pi Raspberry.</p> <p>The Pi Raspberry has been installed with a invisible Proxy MIM to register every communication the device make, also an intruder detection Suricata system to detect any threat. It's been installed part of the "Elastic Pila" in our case the Filebeat one.</p>	

To make an later analysis of the data, it's chosen the cloud Elastic solution, there we can make multiple filters (Logstash) and Dashboard (Kibana) to analyze the device behavior and the posible risk and warnings.

Finally it had been made plenty of trials to demonstrate that our system is capable to capture vulnerability and open breaks that could be in the mobile devices, once the vulnerability is captured the information gets to the User by email to act consequently to the threat received.

Agradecimientos

Quiero dar las gracias a una persona, y a un animal/persona, gracias a ellos he podido sacar la fuerza y el tiempo para poder realizar este Master en tiempos de confinamiento:

-A ti Olivia, por ser la gran persona que eres, por el apoyo incondicional, por comprenderme siempre en cada momento y por los ratitos de lectura junto a mi dándome animo en el silencio de la tarde.

-A Rodolfo, por acompañarme en esos días de ordenador intensos con su cariño y mimos.

Índice

1. Introducción	12
1.1. Objetivos generales.....	13
1.2. Metodología y proceso de trabajo	14
1.2.1. Definición del Plan de Trabajo.	14
1.2.2. Amenazas de seguridad en el ámbito de los dispositivos móviles.....	14
1.2.3. Determinación de los requerimientos de información.	14
1.2.4. Análisis de las necesidades del sistema.	14
1.2.5. Diseño del sistema recomendado.	14
1.2.6. Pruebas y mantenimiento del sistema.	14
1.2.7. Implantación y evaluación del sistema.	14
1.3. Listado de las tareas	15
1.3.1. Fase de investigación.	15
1.3.2. Fase de desarrollo.....	17
1.3.3. Conclusiones y trabajo futuro.	19
1.3.4. Redacción de la Memoria.	19
1.3.5. Presentación del video memoria.....	19
1.3.6. Defensa del Trabajo Final de Master.	19
1.4. Planificación temporal detallada	20
1.5. Revisión del estado del arte	23
1.5.1. Factores del crecimiento del tráfico de datos a través de dispositivos móviles .	24
1.5.2. Las redes 5G, protagonistas del futuro tráfico de datos móviles	25
1.5.3. Vídeo móvil, Realidad Virtual y wearables, tendencias fuertes	25
1.5.4. Analítica móvil	25
1.5.5. Como se obtienen los datos.	26
1.5.6. Herramientas de analítica móvil.....	27
1.6. Posibles riesgos y soluciones que pueden afectar al desarrollo y cumplimiento de los objetivos del TFM propuesto.....	29
1.6.1. Riesgo 1 – Dimensionamiento temporal.....	29
1.6.2. Riesgo 2 – Fallos de hardware / software	29
1.6.3. Riesgo 3 – Implementación de la solución.....	29
1.6.4. Riesgo 4 – Implementación de la solución.....	29

1.7. Recursos necesarios.....	30
1.8. Presupuesto del proyecto.	31
1.9. Requisitos Legales	32
1.9.1. Directrices específicas para tratamiento de datos dispositivos móviles	32
2. Fase de investigación	35
2.1. Amenazas de seguridad en el ámbito de los dispositivos móviles.	35
2.1.1. Seguridad en Android:	35
2.1.2. Seguridad en iOS:	37
2.2. Medidas para proteger tu dispositivo:	39
2.2.1. Mantener el dispositivo actualizado.....	39
2.2.2. Protección frente accesos no deseados.....	39
2.2.3. Cifrado del contenido del dispositivo móvil	39
2.2.4. Gestión de contraseñas.....	40
2.2.5. Detección de accesos y/o usos no controlados de dispositivo	40
2.3. Amenazas de seguridad móvil:.....	40
2.3.1. Filtración de datos	40
2.3.2. Wi-Fi no asegurada.....	41
2.3.3. Suplantación de red	41
2.3.4. Ataques de phishing.....	41
2.3.5. Spyware	41
2.3.6. Criptografía quebrada.....	42
2.3.7. Gestión inadecuada de las sesiones.....	42
2.4. Sistema operativo dispositivo sonda.....	42
2.4.1. Raspbian Buster	43
2.4.2. Ubuntu.....	43
2.4.3. Elección.....	43
2.5. Arquitectura y flujo de datos.....	44
2.5.1. Escenario 1.....	44
2.5.2. Escenario2.....	45
2.5.3. Elección.....	46
2.6. Elección de herramientas MITM.....	46
2.6.1. Hyperfox.....	47
2.6.2. MitmProxy.....	48

2.6.3.	Elección.....	49
2.7.	Elección de herramientas IDS.....	49
2.7.1.	Snort.....	50
2.7.2.	Suricata.....	50
2.7.3.	Elección.....	51
2.8.	Envío de datos:	51
2.8.1.	Logstash.....	51
2.8.2.	Beats.....	52
2.8.3.	Elección.....	52
2.9.	Elección de Base de datos	53
2.9.1.	ElasticSearch	53
2.9.2.	Elastic Cloud	54
2.9.3.	Elección.....	54
2.10.	Interfaz gráfica	54
2.10.1.	Graylog	54
2.10.2.	Kibana.....	55
2.10.3.	Elección.....	56
3.	Fase de desarrollo	57
3.1.	Sistema operativo dispositivo sonda.....	57
3.1.1.	Preparar la tarjeta microSD y descargando NOOBS.....	57
3.1.2.	Instalando Raspbian en la Raspberry Pi	59
3.2.	Crear un proxy MITM para la captura de tráfico.	60
3.2.1.	Descripción.....	60
3.2.2.	Estructura.....	61
3.2.3.	Requisitos técnicos	63
3.2.4.	Configuración	64
3.2.5.	Ejecución	70
3.3.	Implementar IDS para análisis de datos.	74
3.3.1.	Instalación Suricata.....	74
3.3.2.	Configuración	74
3.3.3.	Ejecución	75
3.4.	Instalación de Filebeat en Raspberry.....	76
3.4.1.	Prerrequisitos	76

3.4.2.	Instalación de Filebeat.....	77
3.4.3.	Configuración.....	77
3.4.4.	Ejecución.....	78
3.5.	Elastic Cloud.....	78
3.5.1.	Registro.....	78
3.5.2.	Instalación.....	79
3.5.3.	Configuración de Kibana.....	80
3.6.	Análisis de datos.....	82
3.6.1.	Filtro Logstash.....	82
3.6.2.	Monitorización de datos en Kibana.....	84
3.7.	Envío de alertas con Kibana.....	88
4.	Conclusiones y trabajo futuro.....	92
4.1.	Problemas encontrados en la implementación del proyecto.....	92
4.1.1.	Configuración de Raspberry-pi como punto de acceso con MitmProxy.....	92
4.1.2.	Estudio de diseño final del sistema ELK.....	93
4.1.3.	Tareas pendientes en la implementación.....	93
4.2.	Trabajo futuro.....	93
5.	Bibliografía/Webgrafía.....	94

Índice de figuras

Figura 1: Escenario 1 TFM.....	17
Figura 2: Escenario 2 TFM.....	17
Figura 3: Tráfico datos móviles.....	23
Figura 4: Dispositivos conectados.....	24
Figura 5: Video móvil ocupación de los datos.....	25
Figura 6: Vulnerabilidades de criticidad alta en Android a lo largo de los años.....	35
Figura 7: Detecciones de malware para Android en 2019.....	36
Figura 8: Vulnerabilidades de criticidad alta en iOS a lo largo de los años.....	37
Figura 9: Detecciones de malware para iOS en 2019.....	38
Figura 10: 10: Escenario 1 TFM.....	44
Figura 11: Escenario 2 TFM.....	45
Figura 12: Diferencias entre los servidores en local y en la nube.....	46
Figura 13: Diagrama proxy Hyperfox.....	47
Figura 14: Diagrama proxy Hyperfox con SSL.....	47
Figura 15: Diagrama Proxy MitmProxy.....	48
Figura 16: Diagrama Proxy MitmProxy con SSL.....	49
Figura 17: Tabla comparativa Snort Suricata.....	51
Figura 18: Interfaz Gráfica Graylog.....	55
Figura 19: Interfaz Gráfica Kibana.....	55
Figura 20: Administrador de discos Windows.....	57
Figura 21: Administrador de discos Windows.....	58
Figura 22: Nuevo volumen simple.....	58
Figura 23: Finalización asistente.....	59
Figura 24: Instalador Raspbian.....	60
Figura 25: Raspbian instalado correctamente.....	60
Figura 26: MitmProxy con certificado Https.....	62
Figura 27: Raspberry Pi Especificaciones.....	63
Figura 28: RaspbianOS.....	64
Figura 29: Versión Raspberry.....	64
Figura 30: Archivo dhcpd.conf.....	65
Figura 31: Archivo dhcpd.conf.....	66
Figura 32: Archivo isc-dhcp-server.....	66
Figura 33: Archivo hostapd.....	67
Figura 34: Archivo hostapd.conf.....	68
Figura 35: Versión Mitmproxy.....	68
Figura 36: Archivo start_mitmweb.sh.....	68
Figura 37: Archivo mitmweb.service.....	69
Figura 38: Interface Gráfica MitmProxy.....	70
Figura 39: WiFi emitida Raspberry.....	71
Figura 40: Navegación sin certificado.....	71
Figura 41: Instalación tipo de certificado por SO.....	72
Figura 42: Certificado Instalado en IOS.....	72

Figura 43: Certificado.....	73
Figura 44: Web con certificado instalado.	73
Figura 45: Captura de paquetes MitmProxy.....	73
Figura 46: Instalación de Suricata IDS en Raspbian.....	74
Figura 47: Comprobación del estado del servicio Suricata.	74
Figura 48: Edición de suricata.yaml para establecer la interfaz de escucha.....	75
Figura 49: Descarga de repositorio de script para actualizar reglas.	75
Figura 50: Tarea programada.	75
Figura 51: Versión Python.....	76
Figura 52: Swap.	76
Figura 53: Filebeat.yml.....	77
Figura 54: Sección Elastic Cloud archivo filebeat.yml.....	78
Figura 55: Ejecución Filebeat.....	78
Figura 56: Acceso a Elastic Cloud.	78
Figura 57: Instalación Elastic cloud.....	79
Figura 58: Instalación Elastic cloud.....	79
Figura 59: Versiones disponibles Elasticsearch.	79
Figura 60: Despliegue Cloud disponible.....	80
Figura 61: Despliegue Cloud disponible.....	80
Figura 62: Cloud ID.	80
Figura 63: Creación Index Patterns.....	81
Figura 64: Creación Index Patterns.....	81
Figura 65: Pantalla de Discover.	81
Figura 66: Mensaje Kibana.	81
Figura 67: Estructura Logstash	82
Figura 68: Datos Kibana después de filtro.	83
Figura 69: Suricata-Event type.....	84
Figura 70: Suricata Alert Signature.	85
Figura 71: Suricata Alert Signature.	85
Figura 72: Suricata Geoip Country.....	86
Figura 73: Suricata AADispositivo.....	86
Figura 74: Suricata Dns.	87
Figura 75: Suricata top Ip destino.	87
Figura 76: Suricata top Puerto Destino.	87
Figura 77: Dashboard 1/2.	88
Figura 78: Dashboard 2/2.	88
Figura 79: Funcionamiento alerta.....	89
Figura 80: Tipo de conector.	90
Figura 81: Configuración servidor correo.	90
Figura 82: Alerta.....	90
Figura 83: Índice alerta.	91
Figura 84: Condición alerta.	91
Figura 85: Correo Alerta.....	91

1.Introducción

El impacto de las tecnologías de la información y las comunicaciones (TIC) no se limita al sector en el que son producidas, sino que abarca a todos los sectores de producción y consumo. Esto es válido también para la telefonía móvil. Además, su influencia aumenta según aumenta el efecto de las redes, es decir, cuando crece el número de personas que usan el servicio. Es más, con el tiempo muestran mejoras evidentes; los dispositivos móviles incorporan más y mejores servicios a la vez que también mejora la calidad de las comunicaciones. La cobertura de la infraestructura y los servicios crece, y al propio tiempo los precios siguen una clara tendencia de disminución. Por último, los teléfonos móviles también generan innovaciones porque promueven y facilitan la invención y producción de nuevos servicios, productos o procesos. Los ejemplos son comunes, desde la utilización de llamadas perdidas para actividades de la vida cotidiana hasta las operaciones bancarias móviles, tanto en las zonas rurales como en las zonas urbanas. Las redes móviles han experimentado una gran evolución desde sus comienzos, modificándose su arquitectura e inteligencia, con el fin de transmitir voz y datos con mayor calidad y capacidad, a mejor rendimiento.

La idea se basa en analizar el tráfico de datos saliente y entrante de un dispositivo móvil para detectar comportamientos extraños que delaten una posible infección o vulneración del dispositivo analizado.

Como bien sabemos, los dispositivos móviles pueden conectarse a una red de datos a través de la conexión 3G/4G o bien a través de una red WiFi. Por lo que en caso de estar filtrando información tendríamos que analizar ambas vías, pero en nuestro caso sólo se va a hacer a través de WiFi.

1.1. Objetivos generales

Los objetivos principales de este trabajo son los que se especifican a continuación:

Entender el concepto de amenaza:

Vamos a entender el concepto de amenaza de seguridad en el ámbito de los dispositivos móviles y analizar los tipos de amenazas de seguridad más comunes.

Creación de un Access Point:

Crear un sistema de Access Point que permita conectarse y tener acceso a internet, esta plataforma analizará el comportamiento de entrada y salida utilizando técnicas de man-in-the-middle para alertar al propietario del dispositivo de conexiones a servidores informados como vulnerables o susceptibles de haber sido comprometidos.

Analizar e interpretar el tráfico recogido:

Análisis e interpretación del tráfico del dispositivo móvil capturado. Además, para interpretar correctamente los datos necesitaremos unos conocimientos básicos de TCP/IP, que nos ayuden en la interpretación en las capturas de los datos que obtendremos.

Alertar al usuario de posible amenaza:

Las notificaciones y alertas tienen como objetivo comunicar a un usuario información referente a la ocurrencia de eventos de su interés en un sistema informático. Se basan en la emisión de mensajes y avisos por programas o servicios para advertir un evento o amenaza al usuario, teniendo la propiedad de no causar interrupciones en la ejecución de la tarea que se esté llevando a cabo. Permiten la recolección de datos sobre eventos producidos en cualquier esfera. Constituyen una parte orientada a sacar provecho de las experiencias y mejoran la toma de decisiones dentro del ámbito de trabajo.

1.2. Metodología y proceso de trabajo

La metodología a seguir para el cumplimiento de los objetivos viene definida por las siguientes etapas:

1.2.1. Definición del Plan de Trabajo.

Se trata de una de las fases más importantes ya que es la columna vertebral sobre la que se sustenta el Trabajo. En esta primera etapa se identifica el contexto del caso. Se definen los objetivos del proyecto, la metodología aplicada, las tareas necesarias para cumplir con los objetivos, se identifican los principales riesgos y se realiza una planificación temporal de las tareas a realizar.

1.2.2. Amenazas de seguridad en el ámbito de los dispositivos móviles.

La seguridad móvil juega un rol cada vez más importante en la protección de los activos de información, tanto para usuarios hogareños como corporativos. De hecho, con la llegada de Internet de las Cosas y de los miles de dispositivos no tradicionales que son controlados mediante aplicaciones móviles, la seguridad de nuestros teléfonos se vuelve cada vez más relevante para proteger los equipos que a ellos se conectan.

Realizaremos un análisis del panorama de la seguridad móvil con base en estadísticas obtenidas durante algunos meses, para evaluar cuáles son las nuevas tendencias en relación al pasado reporte de seguridad móvil de 2018.

1.2.3. Determinación de los requerimientos de información.

Se necesitará unir una serie de herramienta que pueda ayudar a mejorar la eficacia de los sistemas IDS y que este dedique sus recursos solo a analizar contenido potencialmente dañino.

1.2.4. Análisis de las necesidades del sistema.

Para reducir la carga de trabajo de los sistemas de detección, se deberá reducir el contenido de entrada, buscando una manera de eliminar contenido no relevante.

1.2.5. Diseño del sistema recomendado.

Se diseñará una infraestructura que cumpla con lo estipulado anteriormente, con módulos que permitan coger un tráfico de paquetes determinado y los reduzca al máximo, asimismo reduciendo el coste,

1.2.6. Pruebas y mantenimiento del sistema.

Con el Sistema ya en ejecución, se realizará una batería de pruebas para ver si es capaz de sustraer contenido relevante y se comprobará si supone una gran eficiencia para el sistema.

1.2.7. Implantación y evaluación del sistema.

Con las pruebas finalizadas, si son exitosas, dicho módulo será propuesto para ser anexionado a los sistemas de escudo de la empresa hogar o cualquier otra organización.

1.3. Listado de las tareas

En esta fase tiene como principal objetivo planificar las fases y tareas a realizar durante el análisis de las comunicaciones móviles. La principal tarea a realizar en esta fase es el Plan de Trabajo en el que se detallan los siguientes aspectos:

1.3.1. Fase de investigación.

Durante esta primera fase vamos a estudiar cual serían las herramientas más adecuadas para el estudio de nuestro proyecto, además veremos la manera de encajarlas y de si se despliegan físicamente o en la nube. La fase de investigación la hemos dividido en varias tareas.

Sistema operativo dispositivo sonda:

Una vez seleccionado el dispositivo hardware que se empleará como base del dispositivo y el software que se encargará de generar y enviar alertas, llega el momento de analizar cuál será el sistema operativo más adecuado como base.

Raspbian: es una distribución del sistema operativo Linux, libre y basado en Debian. Nació como un port no oficial de Debian para dar soporte a las CPUs basadas en ARM que empleaba este tipo de dispositivos.

Ubuntu: es una distribución del sistema Linux basado en Debian. Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario.

Elección de herramientas MITM:

En la elección del proxy MITM nos vamos a centrar en software libre tenemos dos posibles candidatos:

Hyperfox: es uno de los Proxy Man In The Middle más completos y fáciles de utilizar. Esta herramienta gratuita es capaz de capturar el tráfico HTTP y HTTPS de nuestra red local, y almacenar toda la información en una base de datos para su posterior tratamiento.

Principales características de Hyperfox

Cuando realizamos un ataque Man In The Middle para realizar una auditoría de seguridad en la red local, no solo se necesita hacer el típico ARP Spoofing, sino que tenemos que tener una herramienta para capturar toda la información y mostrarla de manera fácil al auditor. Hyperfox es compatible con el protocolo HTTP, por lo que todas las peticiones que nuestra víctima realice, nosotros seremos capaces de capturarla de manera fácil y rápida.

MitmProxy: es una aplicación proxy de código abierto que permite interceptar conexiones HTTP y HTTPS entre cualquier cliente HTTP(S) (como un navegador móvil o de escritorio) y un servidor web que usa un ataque típico | man-in-the-middle attack (MITM). De forma similar a otros proxies (como Squid), acepta conexiones de clientes y las envía al servidor de destino. Sin embargo, mientras que otros proxies generalmente se enfocan en el filtrado de contenido o la optimización de velocidad mediante el almacenamiento en caché, el objetivo de MitmProxy es permitir que un atacante monitoree, capture y altere estas conexiones en tiempo real.

Elección de herramientas IDS:

La elección del software IDS nos vamos a centrar en software libre que podamos instalar en nuestro dispositivo y estos son los candidatos:

Entre el amplio elenco de soluciones de detección de intrusos basados en red, cabe destacar dos productos sobre el resto: Snort y Suricata.

Snort: ha sido el motor de IDS de facto durante años. Este motor tiene una enorme comunidad de usuarios soportándolo y, un abanico aún mayor y en aumento de suscriptores a sus reglas.

Suricata: no tiene una vida tan larga en comparación con Snort, ha estado reclamando mercado como una respuesta evolucionada o alternativa a este, basando sus argumentos principalmente en sus capacidades de proceso multi-hilo.

Elección de Base de datos:

En lo tocante a la persistencia de datos y consultas parece no haber dudas, un producto domina el mercado del software libre: ElasticSearch.

ElasticSearch: es una solución de base de datos y servidor de búsqueda basado en Lucene. Este producto provee un motor de búsqueda distribuido y con capacidad multi-tenencia.

Envío de datos:

En este apartado se analiza las diferentes opciones para enviar las alertas generadas por Suricata desde nuestro dispositivo sonda a la base de datos de ElasticSearch.

Logstash: es un motor de recolección de datos de código abierto desarrollado por Elastic, creadores de ElasticSearch. Este puede unificar dinámicamente datos de fuentes dispares y normalizar los datos en destinos de su elección.

Beats: una serie de agentes ligeros de reenvío, de código abierto, desarrollados también por Elastic como una alternativa más ligera a Logstash. Originalmente, para la ingesta de datos era necesaria la inclusión de Logstash como nodo puente en la arquitectura. Desde la versión 5.0 en adelante, ElasticSearch admite la entrada directamente desde Beats, simplificando el diseño de esta.

Interfaz gráfica:

Por último, queda por debatir la capa más externa de nuestra arquitectura, la cual estará en contacto con el usuario: La interfaz gráfica.

Graylog: es una solución para visualizar registros almacenados en una base de datos ElasticSearch. Graylog permite realizar consultas avanzadas sobre los datos almacenados, crear tableros con los resultados de las mismas o incluso generar alarmas ante determinados datos o ausencia de ellos.

Kibana: es la alternativa a Graylog propuesta por Elastic. Esta solución es una potente herramienta pensada para el análisis masivo de datos almacenados en una base de datos ElasticSearch. Gracias a esta concepción, enfocada al Big Data, Kibana ofrece una infinidad de nuevas posibles representaciones gráficas para los eventos, como mapas de calor, localizaciones, etc.

Arquitectura y flujo de datos:

A lo largo de este apartado, se describe la arquitectura para el análisis de datos basado en red resultante de la toma de decisiones a lo largo de los puntos anteriores.

A continuación, se adjunta los dos posibles escenarios de nuestro proyecto, según analicemos las herramientas nos decidiremos por uno u otro.

Escenario1: Instalaremos en un servidor local ElasticSearch y Kibana.

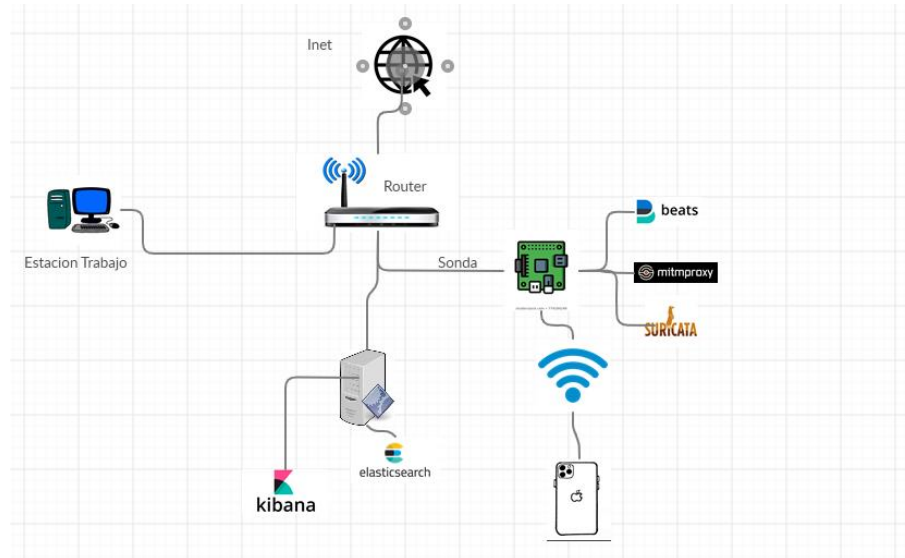


Figura 1: Escenario 1 TFM.

Escenario 2: Alojaremos en la Elastic cloud, ElasticSearch y Kibana.

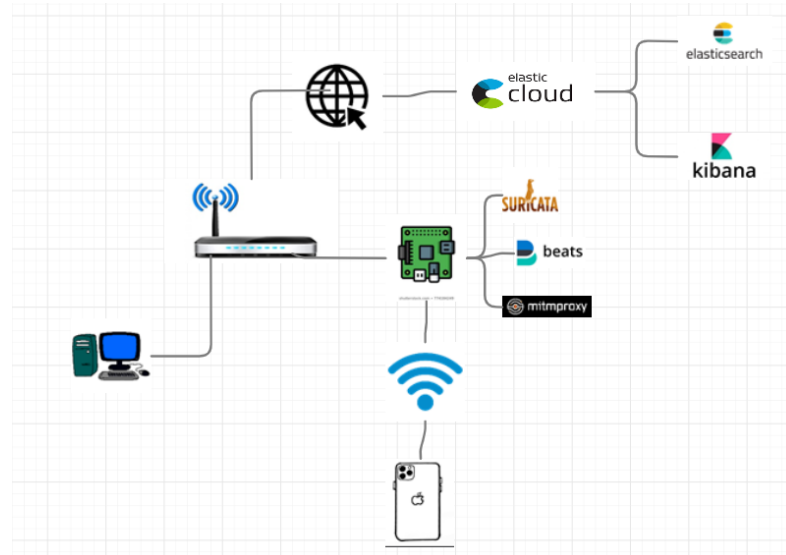


Figura 2: Escenario 2 TFM.

1.3.2.Fase de desarrollo

Una vez definida la arquitectura del sistema de detección de intrusos basado en red en el apartado anterior, se realizará un despliegue de la arquitectura mínima de la plataforma.

Con este despliegue se desea obtener un laboratorio del cual extraer información del funcionamiento del sistema más allá del permisivio papel, donde todo funciona correctamente.

De este entorno se obtendrá un manual de despliegue probado, con puntos a tener en consideración tras instalaciones fallidas, deficientes o mejorables.

A lo largo de este apartado se describen los diferentes puntos de la instalación llevada a cabo.

Sistema operativo dispositivo sonda.

Lo primero que vamos a hacer es instalar el SO a nuestro dispositivo sonda en nuestro caso Raspberry Pi 3 a través de un ordenador con sistema operativo Windows. Aunque existen muchas formas de llevar a cabo esta tarea, vamos a mostrar la forma más sencilla y rápida.

Vamos a necesitar como mínimo una tarjeta MicroSD 8GB y clase 6 completamente vacía ya que será el soporte físico encargado de almacenar el sistema operativo. Aunque los requerimientos mínimos hablan de 8GB y clase 6, consideramos que una tarjeta de 16GB y clase 10 arroja unos resultados y un balance calidad/precio mejor.

Los pasos a dar serán:

- Descargar NOOBS en nuestro PC.
- Insertar o conectar la tarjeta SD en ese mismo PC.
- Formatear la tarjeta SD.
- Descomprimir NOOBS que descargamos como fichero zip en esa SD.
- Una vez termina de copiarse todo sacamos la tarjeta SD y la insertamos en la Raspberry Pi.
- Conectamos el cable HDMI, teclado, ratón y cable de red. OJO todavía no funcionará con Wi-Fi.
- Conectamos el cable de alimentación eléctrica y empezará a arrancar la Raspberry Pi.

Crear un proxy MITM para la captura de tráfico.

Un proxy MITM es una pieza de software que se ejecuta en un dispositivo (por ejemplo, un punto de acceso Wi-Fi o un enrutador de red) entre un cliente (su teléfono, su computadora portátil) y el servidor con el que desea comunicarse. El proxy puede interceptar y analizar la información que se envía entre el cliente y el servidor. Incluso puede manipular la solicitud que se envía o modificar la información que se devuelve.

Implementar IDS para análisis de datos.

Un IDS es un sistema que intenta detectar y alertar sobre las intrusiones intentadas en un sistema o en una red, considerando intrusión a toda actividad no autorizada o no que no debería ocurrir en ese sistema. Según esta definición, muchos podrían pensar que ese trabajo ya se realiza mediante los cortafuegos o firewalls. El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Un modelo de ataque dirigido sobre todo a los usuarios de dispositivos móviles se basa en la simulación de un punto de acceso inalámbrico en una red inalámbrica pública, como las de las cafeterías o las de los aeropuertos. En ello, un atacante configura su ordenador de tal manera que este se convierta en una vía adicional para acceder a Internet (probablemente una con una calidad de señal mejor que el propio punto de acceso). De esta manera, si el atacante consigue

engañar a los usuarios más ingenuos, este puede acceder y manipular la totalidad de los datos de su sistema antes de que estos se transmitan al verdadero Access point o punto de acceso. Si este requiere autenticación, el hacker recibe para ello los nombres de usuario y contraseñas que se utilizan en el registro. El peligro de convertirse en el blanco de estos ataques man-in-the-middle se da particularmente cuando los dispositivos de salida se configuran de tal manera que se pueden comunicar automáticamente con los puntos de acceso con mayor potencia de señal.

Análisis del tráfico recogido.

La monitorización siempre se ha servido tanto de la administración de redes como del análisis de tráfico de red. Ambas disciplinas otorgan vías para obtener datos que permiten inferir información sobre el estado general de la plataforma.

Es fácil entender que frente a, por ejemplo, un problema de rendimiento de una aplicación, deseemos poder observar y evaluar el tráfico generado, y esto es justo lo que permite el análisis de tráfico de red.

Este primer impulso natural de observar el tráfico en realidad se ve justificado, ya que el análisis de tráfico ha probado ser útil para identificar problemas como errores de configuración, deterioro en rendimiento de servidores, problemas de latencia en algunos de los componentes de red y otras tantas condiciones de error.

Envío y notificaciones de alertas.

Las alertas son mensajes enviados a un determinado usuario sobre eventos que van a ocurrir en un sistema y que necesitan ser informados. Esta información debe ser chequeada, en tiempo real, porque está encaminada a mejorar la situación advertida. Las mismas deben persistir en el sistema hasta tanto no se le dé solución.

1.3.3. Conclusiones y trabajo futuro.

Conclusiones: Se enumeran las conclusiones que se desprenden de la realización de TFM.

Trabajo futuro: Se concluye introduciendo diversas opciones de trabajo futuro que pueden ayudar a complementar el trabajo presentado.

1.3.4. Redacción de la Memoria.

Maquetación de la memoria: Finalización de la memoria compilando toda la información anterior y completándola con el glosario bibliografía y anexos.

Entrega PEC4: Punto de control en el que se entrega en el aula la memoria completa del trabajo.

1.3.5. Presentación del video memoria

Preparar video: Elegir contenido del video presentando la memoria del TFM.

Grabación video: Realizar la presentación y grabación del video.

Entrega PEC5: Punto de control en la que entrega en el aula el video de presentación del TFM.

1.3.6. Defensa del Trabajo Final de Master.

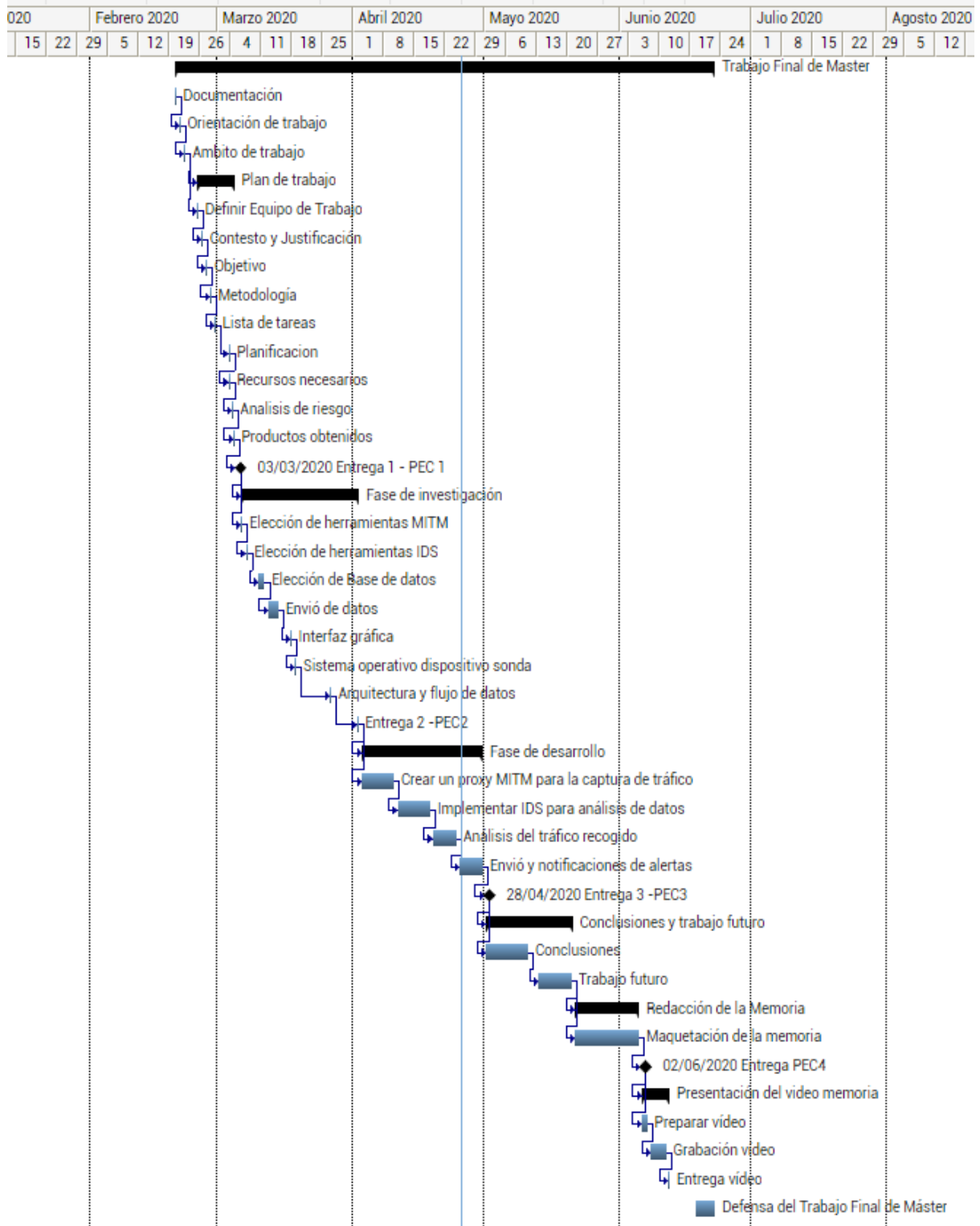
Periodo de ruegos y preguntas y dudas al respecto por parte del tribunal y a su vez dar respuestas a las mismas.

1.4. Planificación temporal detallada

A continuación de muestra la planificación temporal del desarrollo de Trabajo de Fin de Master en diferentes formatos para su comprensión. No se ha tenido en cuentas los periodos vacacionales ni fines de semana, ya que se considera que las tareas definidas en el plan de trabajo se realizan de manera organizada con el tiempo asignado a la actividad laboral y familiar. Aun así, se ha estimado un periodo de reserva de 10 días aproximadamente por si surgiera algún imprevisto que impidiera completar el Trabajo en los plazos indicados.

	EDT	Nombre	Duración	Inicio	Fin	Predecesoras
1	1	☐ Trabajo Final de Master	88 días	19/02/2020	19/06/2020	
2	1.1	Documentación	1 día	19/02/2020	19/02/2020	
3	1.2	Orientación de trabajo	1 día	20/02/2020	20/02/2020	2
4	1.3	Ambito de trabajo	1 día	21/02/2020	21/02/2020	3
5	1.4	☐ Plan de trabajo	7 días	24/02/2020	03/03/2020	4
6	1.4.1	Definir Equipo de Trabajo	1 día	24/02/2020	24/02/2020	4
7	1.4.2	Contesto y Justificación	1 día	25/02/2020	25/02/2020	6
8	1.4.3	Objetivo	1 día	26/02/2020	26/02/2020	7
9	1.4.4	Metodología	1 día	27/02/2020	27/02/2020	8
10	1.4.5	Lista de tareas	1 día	28/02/2020	28/02/2020	9
11	1.4.6	Planificación	0.5 día	02/03/2020	02/03/2020	10
12	1.4.7	Recursos necesarios	0.5 día	02/03/2020	02/03/2020	11
13	1.4.8	Análisis de riesgo	0.5 día	03/03/2020	03/03/2020	12
14	1.4.9	Productos obtenidos	0.5 día	03/03/2020	03/03/2020	13
15	1.4.10	Entrega 1 - PEC 1	0 día	03/03/2020	03/03/2020	14
16	1.5	☐ Fase de investigación	19 días	05/03/2020	31/03/2020	15
17	1.5.1	Elección de herramientas MITM	1 día	05/03/2020	05/03/2020	15
18	1.5.2	Elección de herramientas IDS	1 día	06/03/2020	06/03/2020	17
19	1.5.3	Elección de Base de datos	2 días	09/03/2020	10/03/2020	18
20	1.5.4	Envío de datos	3 días	11/03/2020	13/03/2020	19
21	1.5.5	Interfaz gráfica	1 día	16/03/2020	16/03/2020	20
22	1.5.6	Sistema operativo dispositivo sonda	1 día	17/03/2020	17/03/2020	21
23	1.5.7	Arquitectura y flujo de datos	1 día	25/03/2020	25/03/2020	22
24	1.5.8	Entrega 2 -PEC2	1 día	31/03/2020	31/03/2020	23

25	1.6	☐ Fase de desarrollo	20 días	01/04/2020	28/04/2020	24
26	1.6.1	Crear un proxy MITM para la captura de tráfico	6 días	01/04/2020	08/04/2020	24
27	1.6.2	Implementar IDS para análisis de datos	6 días	09/04/2020	16/04/2020	26
28	1.6.3	Análisis del tráfico recogido	4 días	17/04/2020	22/04/2020	27
29	1.6.4	Envío y notificaciones de alertas	4 días	23/04/2020	28/04/2020	28
30	1.6.5	Entrega 3 -PEC3	0 día	28/04/2020	28/04/2020	29
31	1.7	☐ Conclusiones y trabajo futuro	14 días	29/04/2020	18/05/2020	30
32	1.7.1	Conclusiones	8 días	29/04/2020	08/05/2020	30
33	1.7.2	Trabajo futuro	6 días	11/05/2020	18/05/2020	32
34	1.8	☐ Redacción de la Memoria	11 días	19/05/2020	02/06/2020	33
35	1.8.1	Maquetación de la memoria	11 días	19/05/2020	02/06/2020	33
36	1.8.2	Entrega PEC4	0 día	02/06/2020	02/06/2020	35
37	1.9	☐ Presentación del video memoria	5 días	03/06/2020	09/06/2020	36
38	1.9.1	Preparar vídeo	2 días	03/06/2020	04/06/2020	36
39	1.9.2	Grabación vídeo	2 días	05/06/2020	08/06/2020	38
40	1.9.3	Entrega vídeo	1 día	09/06/2020	09/06/2020	39
41	1.10	Defensa del Trabajo Final de Máster	5 días	15/06/2020	19/06/2020	



1.5. Revisión del estado del arte

Si ya resultan sorprendentes las previsiones sobre el crecimiento de la población mundial que periódicamente la Organización de Naciones Unidas publica, y que indican que el número de personas sobre la tierra crece, cada vez más, a un ritmo nunca visto hasta ahora, no menos sorprendentes resultan los pronósticos sobre el incremento a toda velocidad de otra 'especie', la de los dispositivos móviles y toda clase de objetos conectados, que provocarán que en los próximos cinco años, el tráfico de datos móviles se multiplique por siete.

Es la previsión del reciente Informe Cisco Visual Networking Index (VNI) sobre Tráfico Global de Datos Móviles 2016-2021 en su undécima edición, en la que calculan que para 2021, habrá en el mundo más teléfonos móviles, unos 5.500 millones, que suministros de agua corriente (5.300 millones) y cuentas bancarias (unos 5.400 millones).

En 2021, el tráfico global de estos datos alcanzará los 49 exabytes (49.000 millones de gigabytes) mensuales y 587 exabytes anuales, lo que supone un ratio de incremento interanual del 47% entre 2016 y 2021.

El incremento exponencial de usuarios móviles, Smart Phones y conexiones del Internet of Things (IoT), junto a las mejoras en velocidad de red y el mayor consumo de vídeo móvil son las causas, según indica el documento, de que en cinco años, el intercambio global de datos móviles pase a representar el 20% del tráfico IP total, desde el 8% que suponía el pasado año 2016.

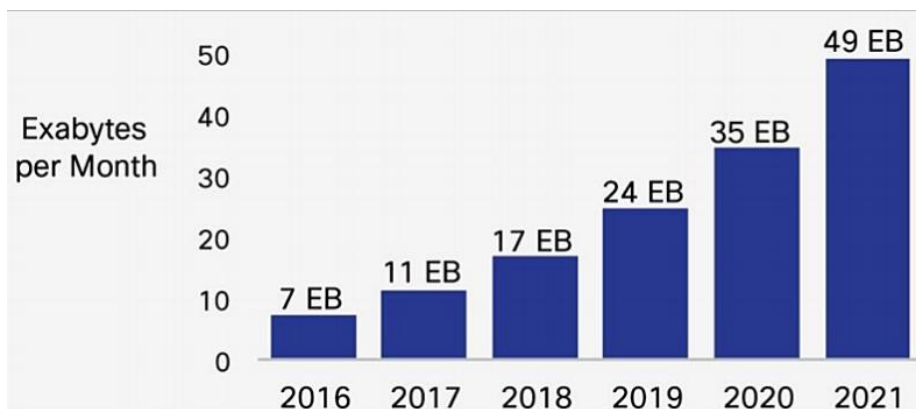


Figura 3: Tráfico datos móviles.

En esta tendencia, España no se queda atrás, teniendo en cuenta la gran penetración del Smartphone en la población española, en la que el pasado año ya se registraban más de 35 millones y en 2021 habrá 45,8 millones. El tráfico de datos móviles alcanzará los 4,5 exabytes (4.500 millones de gigabytes) anuales en 2021, con una tasa de incremento interanual del 47%. Lo mismo ocurre con el rápido incremento de la velocidad de las redes móviles, tal y como indicaba hace unos meses el informe La Sociedad de la Información en España 2015 de Telefónica, que indicaba cómo el 76% de los hogares ya tenían cobertura de 4G en el primer trimestre de 2015 y en las zonas de más de 50.000 habitantes ya alcanzaba a más del 97%, porcentaje que se incrementa a medida que aumenta el tamaño de las ciudades. De esta forma,

no es de extrañar que el informe de Cisco concluya que en España, el flujo de datos móviles representará para 2021 el 15% del total del tráfico IP, frente al 5% de 2016.

1.5.1. Factores del crecimiento del tráfico de datos a través de dispositivos móviles

En cinco años habrá 1,5 dispositivos móviles por persona, casi 12.000 millones de dispositivos móviles conectados, incluyendo los módulos M2M, para una población mundial estimada de 7.800 millones de habitantes (ONU), desde los 8.000 millones de dispositivos móviles y 1,1 dispositivos por persona registrados en 2016. En España habrá 101,4 millones de dispositivos móviles conectados (2 per cápita) incluyendo módulos M2M en 2021.

La velocidad media de las redes móviles se multiplicará por tres desde los 6,8 Mbps en 2016 hasta los 20,4 Mbps en 2021. En España, la velocidad media de las redes móviles alcanzará los 27 Mbps en 2021 (12 Mbps en 2016).

Las conexiones M2M supondrán el 29 por ciento (3.300 millones) del total de conexiones móviles, desde el 5 por ciento que representaban en 2016 (780 millones). M2M será el tipo de conexión móvil de más rápido crecimiento como resultado del incremento de aplicaciones del Internet of Things tanto en entornos empresariales como de consumo. En España, las conexiones M2M supondrán el 48% (48,3 millones) del total de dispositivos móviles conectados en 2021.

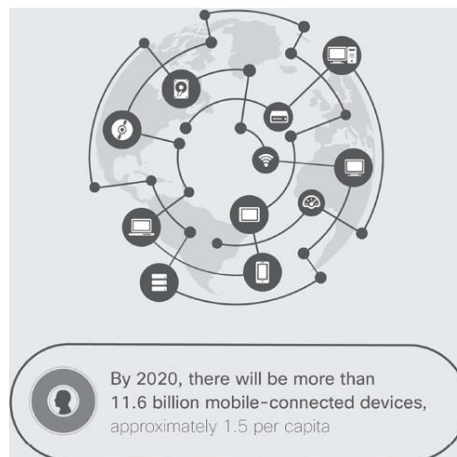


Figura 4: Dispositivos conectados.

Las redes 4G soportarán el 58% del total de conexiones móviles en 2021 (26% en 2016) y generarán el 79 por ciento de todo el tráfico de datos móviles. En España, las redes 4G soportarán el 64% del total de conexiones móviles en 2021 (37% en 2016) y generarán el 95 por ciento de todo el tráfico de datos móviles.

En cuanto al tráfico WiFi, si lo sumamos, teniendo en cuenta el tráfico procedente tanto de dispositivos móviles como de dispositivos sólo WiFi, supondrá casi la mitad (el 49%) de todo el tráfico IP a escala global en 2021 (42% en 2016). En España, la suma del flujo WiFi procedente tanto de dispositivos móviles como de dispositivos sólo WiFi supondrá el 63% de todo el tráfico IP (55% en 2016).

1.5.2. Las redes 5G, protagonistas del futuro tráfico de datos móviles

Según indica Doug Webster, vicepresidente de Marketing para Proveedores de Servicios en Cisco, “debido a la proliferación de aplicaciones de IoT, vídeo móvil y realidad virtual y aumentada, junto a experiencias más innovadoras para empresas y consumidores, la tecnología 5G será clave no sólo para la movilidad, sino para las redes en su conjunto. Con el fin de soportar las mayores funcionalidades que permite la tecnología 5G, las redes requieren también una mayor capacidad de programación y automatización, esencial para responder a las demandas de hoy y del futuro”.

Y es que el crecimiento exponencial de aplicaciones móviles y la adopción de conectividad móvil por parte de los usuarios finales está impulsado el crecimiento de 4G, a la que pronto le seguirá 5G. Cisco y otros expertos de la industria estiman que los despliegues de infraestructuras 5G a gran escala comenzarán en 2020.

Los proveedores móviles necesitarán la mayor velocidad, menor latencia y capacidades de provisión dinámica que se espera de las redes 5G para responder a la creciente demanda de los usuarios y ofrecer nuevos servicios en el segmento empresarial y residencial. Cisco prevé que la 5G supondrá el 1,5 por ciento del intercambio total de datos móviles a escala global en 2021, y generará 4,7 veces más tráfico que la conexión 4G media y 10,7 veces más tráfico que la conexión 3G media.

1.5.3. Vídeo móvil, Realidad Virtual y wearables, tendencias fuertes

El documento de Cisco considera que el vídeo móvil se multiplicará por 8,7 entre 2016 y 2021, siendo la categoría de aplicaciones móviles de mayor crecimiento. El vídeo móvil representará el 78 por ciento de todo el tráfico móvil en 2021. En España, el vídeo móvil se multiplicará por 9 entre 2016 y 2021 y representará el 80 por ciento de todo el flujo móvil en 2021 (62 por ciento en 2016).¹

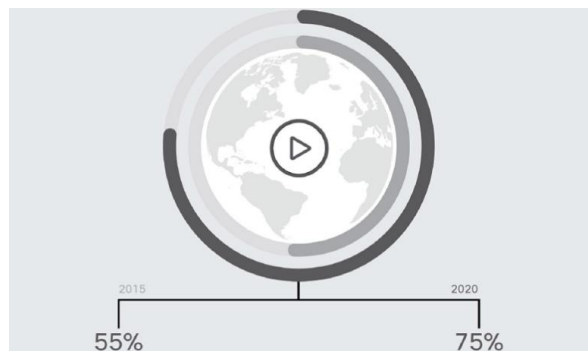


Figura 5: Vídeo móvil ocupación de los datos.

1.5.4. Analítica móvil

Trata de la medición y el análisis de ciertos datos importantes sobre el uso de teléfonos móviles; con respecto a la utilización de aplicaciones; esto con miras a tener datos precisos en cuanto al

¹ <https://cibersuite.com/la-revolucion-del-trafico-datos-moviles-los-proximos-cinco-anos/>

comportamiento del consumidor; para luego utilizarlo entre otras cosas a la publicidad digital; estos datos se pueden obtener a través de aplicaciones diseñadas con el fin de recabar estos datos.

Puedes medir la edad, navegación, compra, tiempo de uso, etc. Estos se extraen por medio de la activación de geolocalización y otras funcionalidades de algunas aplicaciones o del propio teléfono.

Y es que cada vez que autorizas a una app a utilizar algunas funciones de tu Smartphone, para su mejor funcionamiento de igual forma le das permiso para el uso de tu data.

Aunque mucho se ha dicho de la veracidad de algunos datos extraídos por ciertas aplicaciones, por no ser claros o imprecisos; pero lo cierto es que dentro del marketing online es fundamental incluir entre su estrategia anuncios que vayan enfocados a móviles.

1.5.5. Como se obtienen los datos.

Cuando le permites a una app a acceder a tu información; le estás dando luz verde para recabar más datos sobre tu comportamiento. Cada vez somos más dados a compartir la ubicación donde nos encontramos o los sitios que frecuentamos, generando una data de nuestras preferencias y costumbres.

De allí que muchas veces te aparece en las aplicaciones anuncios con sugerencias de sitios que visitar, donde comer, que comprar, etc. A veces pensamos que nos han leído la mente porque hemos ido a algún lugar o queremos visitar otro para compartir o comer algo y te aparecen los anuncios sobre lo que pensaste que querías; así no lo hayas buscado en internet o las redes sociales.

Bien es sabido el incremento de plataformas publicitarias como Google Ads, Facebook Ads, etc. que han apuntado las campañas de anuncios hacia los dispositivos móviles.

Estudiamos los parámetros que las compañías sacan de nuestros datos:²

Sexo	Puedes elegir si quieres que tu anuncio se muestre a hombres o mujeres, por ejemplo, si tienes una tienda de ropa femenina, debes orientar la campaña hacia las mujeres.
Ubicación.	Si tu negocio es local, nacional o internacional vas a elegir la ciudad o países donde se mostrará los anuncios.
Edad.	No es necesario precisar una edad específicamente, debes escoger un rango de edad donde está tu público objetivo. Por ejemplo: de 25 a 40 años de edad.
Sitios web que visitas.	Que páginas web o aplicaciones ve con frecuencia y cuánto tiempo dedica a ellas.
Intereses.	Cada vez que ingresa información a las apps le está diciendo entre otras cosas que le gusta y cuáles son sus intereses.

² <http://blog.fmb.mx/analitica-movil-segmentacion>

Navegador.	Qué tipo de navegador utiliza según el sistema operativo del dispositivo móvil, puede ser Safari, Opera, Google, entre otros.
Tipo de dispositivo.	Si es un Smartphone o Tablet; el dispositivo que es utilizado por el consumidor con mayor frecuencia y desde donde ingresa a las aplicaciones o páginas web.
Sistema operativo.	Según la marca del teléfono o Tablet puede ser Android, iOS, Windows, etc. Muy importante si vas a hacer anuncios en app, recuerda que no todas pueden instalarse en todos los sistemas operativos.
Marca y modelo del dispositivo.	Como sabrás este dato es importante para saber qué tipo de consumidor es al que te diriges, hay muchos que no son de estar a la par de la tecnología o el uso del equipo es básico.
¿WIFI o 4G?	Desde donde se conecta frecuentemente tu consumidor, desde una red inalámbrica o desde su celular haciendo uso de sus datos para navegar.
Operadora	También es importante saber cuál es la compañía de teléfono a la que está suscrito.

1.5.6. Herramientas de analítica móvil

Google Analytics	<p>Google Analytics es el estándar en monitorización de webs y también de apps, entre otras cosas, porque cada vez incluye más funcionalidades. Con ella puedes medir el número total de visitas, los usuarios únicos y recurrentes de tu app, las fuentes de tráfico, los compras in-app y el beneficio.</p> <p>No solo eso, sino que Google Analytics también te permite ver patrones de navegación. Una de las grandes ventajas del marketing online frente al marketing convencional es que en el primero puedes medir todos los datos para comprender el comportamiento online de los diferentes grupos de usuarios.</p> <p>Otra gran ventaja de esta herramienta es Google Play Campaign, que permite la atribución de campañas de publicidad y otros esfuerzos de marketing en los reportes de Google Analytics. Así, te indica cuáles de tus acciones de marketing están consiguiendo los mejores resultados y cuál es su valor, para que decidas en cuál invertir tu presupuesto de marketing.</p> <p>Es importante que compruebes que está funcionando correctamente antes de publicar tu app en Google Play para asegurarte de que desde el momento en el que tu app esté disponible ya tendrás acceso a esta analítica.³</p>
------------------	---

³ <https://kingofapp.com/es/blog/top-herramientas-analitica-movil-medir-exito-app/>

Flurry Analytics	<p>Flurry está disponible para la mayoría de plataformas de desarrollo de apps: iOS y Android, por supuesto, pero también para Windows Phone, HTML 5, BlackBerry y Java.</p> <p>Con Flurry puedes segmentar los usuarios de tus apps por uso, retención, ubicación, edad, género e intereses, pero además también puedes crear segmento personalizado. Con esto puede medir y mejorar la tasa de conversión de cada uno de tus funnels o embudos de conversión. También cuentas con la posibilidad de realizar informes personalizados y programar alarmas en función de eventos.</p> <p>Flurry te da la analítica de los fallos de una app, lo que te permite poder identificarlos y solucionarlos para que tus usuarios tengan una buena experiencia al usarla. Al detectar un bug, envía automáticamente un email al gestor de la app para que pueda resolver el fallo. Sin embargo, y debido a la fragmentación de Android, los desarrolladores de aplicaciones móviles sostienen que es muy difícil lograr una buena experiencia en todos los dispositivos que utilizan este sistema operativo.</p>
Apple App Analytics	<p>Una gran herramienta pero solo disponible para iOS; quizás su mayor beneficio sea que te permite analizar los pagos basados en los Apple ID en lugar de por dispositivo.</p> <p>Apple App Analytics también incluye un sistema de detección de errores por versión de app y sistema operativo. Te permite ver cuántos usuarios de pago tienes en un día, lo que facilita medir el impacto de cambios de precio por campañas.</p> <p>También incluye muchas otras funcionalidades como: filtros por fuente para identificar si los usuarios vienen por una campaña o desde una web, conecta diferentes medidas para entender mejor cómo está rindiendo una campaña de marketing, tasa de conversión, ventas por usuario o sesiones activas.</p>
Appsee Mobile Analytics	<p>Como Google Analytics, Appsee te da información de lo que está pasando en tu app. Sin embargo, la herramienta te da un enfoque algo diferente. Puedes ver el comportamiento de los usuarios con los mapas de calor, que te muestran las áreas o botones que más clics han recibido. Además, te ofrece una amplia información sobre la experiencia y el comportamiento de los usuarios, como informes de analítica in-app.</p>
Amplitude	<p>Este software analiza la navegación y hace el tracking del comportamiento de los usuarios de una app para ayudar al desarrollo del producto. Para esto, es quizás la herramienta más completa. Otras plataformas de software como Intuit, HubSpot y Square utilizan amplitud para validar sus nuevos productos y medir la experiencia de usuario.</p>

1.6. Posibles riesgos y soluciones que pueden afectar al desarrollo y cumplimiento de los objetivos del TFM propuesto

En este apartado se realiza un breve análisis de los riesgos que pueden hacer peligrar el seguimiento temporal planteado en el apartado de planificación generando una desviación de la continuidad del trabajo. Por cada riesgo identificado se realiza una valoración de probabilidad e impacto además de la propuesta de mitigación:

1.6.1. Riesgo 1 – Dimensionamiento temporal

- Definición: Una inadecuada asignación temporal a las tareas identificadas puede causar desviaciones graves debido al desconocimiento en profundidad de las herramientas.
- Probabilidad / Impacto (1/5): 4 / 5
- Mitigación: Tratar de simplificar el desarrollo de la tarea. Aprovechar el tiempo de investigación al máximo para minimizar los posibles retardos.

1.6.2. Riesgo 2 – Fallos de hardware / software

- Definición: Las herramientas se instalan sobre una plataforma en la nube o física, que a su vez albergara los hosts necesarios para implementar las herramientas.
- Probabilidad / Impacto: 3 / 5
- Mitigación: Instalación de un equipo UPS (sai) para evitar interrupciones eléctricas inesperadas. Realizar copias de seguridad externas de manera periódicas.

1.6.3. Riesgo 3 – Implementación de la solución

- Definición: Durante el proceso de implementación de los diferentes apartados pueden surgir incompatibilidades o discrepancias con la idea inicial de implementación que haga variar el rumbo del trabajo.
- Probabilidad / Impacto: 3 / 4
- Mitigación: Establecer un contacto constante con los tutores y profesores asociados para tratar de desbloquear las situaciones de riesgo. Por otro lado, se pueden consultar foros especializados para plantear las situaciones de compromiso.

1.6.4. Riesgo 4 – Implementación de la solución

- Definición: Se puede dar el caso en el que el nivel de detalle de la documentación y desarrollo del Trabajo de Fin de Máster sea demasiado extenso que pueda influir en el contenido y el formato final.
- Probabilidad / Impacto: 2 / 3
- Mitigación: Se propone simplificar el contenido. Orientar el contenido a los objetivos definidos y plasmas mediante anexos los detalles más técnicos si fuera necesario.






1.7. Recursos necesarios.

Se describen los recursos que serían necesarios en el caso de ofrecer una auditoría técnica de seguridad a un cliente en una situación real y estándar. Podría ser que bajo unas circunstancias especiales hicieran falta otros recursos adicionales.

- **Laboratorio:** siempre es interesante contar con un laboratorio que proporcione un entorno controlado sobre el que lanzar pruebas. Con esto se puede garantizar que las pruebas no generarán ningún daño sobre los sistemas de producción. También permitirá analizar y comparar mejor los resultados. Se recomienda contar como mínimo con dos máquinas virtuales, una para instalar y probar las herramientas de análisis de datos que se usarán, y otra máquina con aplicaciones contra las que lanzar las pruebas. Además, contaremos con una Raspberry pi 3 para ejecutar un proxy man-in-the-middle.
- **Documentación:** es necesario disponer de documentación sobre metodologías, manuales, guías, buenas prácticas, y demás documentación para guiar el proceso de análisis de datos.
- **Conexión a internet:** será necesario disponer de una conexión a Internet para consultar información, así como descargar herramientas, sistemas operativos, aplicaciones, etc.
- **Equipo portátil:** equipo desde el que se realizarán las pruebas y se generará la documentación.
- **Licencias:** en principio las herramientas que se usarán durante la ejecución del análisis de datos en el ámbito de este TFM no requieren licencia, pero en un entorno profesional quizás podría hacer falta la suscripción de algunas herramientas profesionales. Dependiendo de si se usan de manera personal o comercial se permite el uso de determinadas herramientas, esto lo determina la licencia a la que esté sujeta la herramienta. Este aspecto habría que tenerlo en cuenta sobre todo de cara a posibles violaciones de licencias y a la hora de generar un presupuesto del proyecto a ejecutar.

1.8. Presupuesto del proyecto.

Para el desarrollo de nuestro proyecto el precio de los recursos materiales utilizados es:

<p>Raspberry Pi 3 Modelo B - Placa base (1.2 GHz Quad-core ARM Cortex-A53, 1GB RAM, USB 2.0)</p> 	36.9€
<p>Ordenador Portátil Análisis de datos:</p> 	800€
<p>SanDisk Ultra - Tarjeta de memoria microSDHC UHS-I de 32 GB con adaptador SD, velocidad de lectura hasta 80 MB/s, Clase 10</p> 	14€
<p>Aukru Micro USB 5V 3000mA Cargador con interruptor +Transparente Caja + disipador de calor para Raspberry Pi 3 Modelo B</p> 	13€
<p>Conexión a internet.</p> 	30/mes
Total	893.9€

Se muestra un cálculo total de horas que nos va a llevar nuestro TFM este cálculo luego podría servir para calcular el precio del mismo. El trabajo sería de 8h día.

FASE	CANTIDAD (Días)	TOTAL HORAS
Fase 1: Plan de Trabajo.	7	56
Fase 2: Fase de investigación.	19	152
Fase 3: Fase de desarrollo.	20	160
Fase 4: Conclusiones y trabajo futuro.	14	112
Fase 5: Redacción de la Memoria.	11	88
Fase 6: Presentación del video memoria.	5	40
Total:	83	608

1.9. Requisitos Legales

1.9.1. Directrices específicas para tratamiento de datos dispositivos móviles

En cuanto al deber de información, del análisis de datos de dispositivos móviles se concluye que hay ciertos aspectos de cumplimiento que requieren de una especial atención por parte de los responsables de tratamiento:

1. La información proporcionada a los usuarios sobre el tratamiento de sus datos personales debe cumplir los requisitos establecidos en los artículos 13 y 14 del RGPD y el artículo 11 de la LOPDGDD, en particular con respecto a la información por capas, en los términos señalados en la “Guía para el cumplimiento del deber de informar” y el “Decálogo para la adaptación al RGPD de las políticas de privacidad en internet”.
2. La información, en forma de política de privacidad, debe estar disponible en la aplicación de análisis de datos. De esta forma, el usuario podrá consultarla antes de instalar la aplicación o en cualquier momento durante su uso.
3. El acceso a la política de privacidad debe poder hacerse de forma sencilla desde la aplicación, y requerir del usuario un número de interacciones reducido, a ser posible a un máximo de dos clics como recomienda el GT29 en sus directrices sobre la transparencia.
4. El responsable de tratamiento tiene que identificarse claramente en la política de privacidad, y en aquellos casos de responsables de tratamiento establecidos fuera de la UE y que ofrecen sus aplicaciones para usuarios en Europa, deben haber designado un representante en la UE e identificarlo igualmente en la política de privacidad.
5. La información sobre el tratamiento debe ser completa y consistente tanto en la tienda de aplicaciones, en su caso, como en la propia aplicación. No puede haber discrepancias entre ambas y por tanto también es aplicable en el caso de aplicaciones preinstaladas en los dispositivos que se comercialicen.
6. El lenguaje en el que se describen las políticas de privacidad debe ser adecuado para el usuario objetivo de la aplicación teniendo en cuenta su edad y su nivel de conocimiento, además, también se tendrá en cuenta el idioma empleado, por ejemplo, aplicaciones disponibles en castellano y destinadas por tanto a usuarios hispanohablantes, deben proporcionar la política de privacidad en castellano sin perjuicio de que pueda mostrarse en otros idiomas. Estos aspectos son especialmente relevantes en el caso de aplicaciones destinadas a menores.
7. Las políticas de privacidad deben ser concretas y específicas sobre el tratamiento de datos personales que se lleva a cabo. Para evitar la “fatiga informativa” se debe evitar proporcionar información de carácter genérico, no específica de la aplicación. La política de privacidad ha de evitar, por ejemplo, describir un conjunto de aplicaciones u otros servicios de la organización como su página web.
8. En la política de privacidad de la app debe proporcionarse al usuario toda la información sobre el tratamiento de los datos personales que pretende realizar, información precisa sobre qué datos y tratamientos son necesarios para el funcionamiento básico de la aplicación, cuáles son

opcionales, y toda la información adicional relevante del tratamiento que se va a realizar con los datos. Además, en la política de privacidad, se deberían indicar los permisos que puede solicitar la aplicación (directamente o a través de bibliotecas de terceros) para el acceso a datos y recursos, para qué tratamientos y finalidad se solicitan esos permisos y con qué extensión (lectura, escritura,...). Por ejemplo, ha de informar si la aplicación tratará los datos únicamente cuando se está ejecutando por acción del usuario en primer plano o necesita acceder también cuando se ejecuta en segundo plano. También se debe facilitar al usuario información relativa a la forma en la que puede gestionar los permisos otorgados a la aplicación de manera que pueda decidir en todo momento si decide otorgar o revocar dichos permisos, o en qué condiciones los otorga.

9. Cuando la legitimación para el tratamiento de los datos personales a través del análisis de datos sea el consentimiento, dicho consentimiento tiene que solicitarse de forma granular, es decir, de forma selectiva e independiente para los distintos tratamientos y finalidades. La instalación y utilización de la app no puede estar condicionada a la obtención de un consentimiento para un tratamiento no necesario para proporcionar el servicio definido en la misma.

10. No hay que utilizar cláusulas ambiguas o vacías como, por ejemplo, “cualquier dato puede ser recolectado o difundido, o retenido indefinidamente” o “recopilamos sus datos con el fin de mejorar su experiencia de usuario”.

11. Hay que incluir información concreta sobre los periodos de retención de los datos y el destino final de los mismos finalizados dichos periodos.

12. En el mismo sentido, hay que incluir información concreta relativa a la lógica aplicada en la elaboración de perfiles y toma de decisiones automatizadas, o un enlace para consultar dicha información, como la utilizada para personalizar los anuncios.

13. La definición de las finalidades del tratamiento y sus bases legales ha de ser clara y precisa, así como los datos personales que se recopilan para cada una de esas finalidades.

14. No hay que olvidar el proporcionar a los usuarios información sobre sus derechos en materia de protección de datos y proporcionar mecanismos y procedimientos para ejercerlos de forma efectiva.

15. En su caso, hay que informar de la existencia de transferencias internacionales de datos de forma concreta y específica.

Los responsables de tratamiento que encarguen el análisis de datos a terceras partes con acceso a datos personales, deben asegurarse de cumplir los requisitos establecidos en el RGPD para cada una de las partes. Para estos casos son particularmente útiles la “Guía del RGPD para responsables de tratamiento” y “Directrices para elaborar contratos entre responsables y encargados de tratamiento”.

Cabe destacar los siguientes requisitos:

16. El tratamiento debe estar regulado por un contrato o vínculo legal que establezca el objeto, la duración, la naturaleza, la finalidad del tratamiento, el tipo de datos personales, las categorías de interesados, y las obligaciones y derechos del responsable.

17. En el contrato de encargo se estipulará específicamente que el encargado tratará los datos personales únicamente siguiendo las instrucciones documentadas del responsable, por lo que el encargado de tratamiento no debe introducir en la aplicación otros tratamientos de datos personales que el responsable pueda desconocer, como aquellos que se pueden introducir al incluir en la aplicación librerías de terceras partes con fines publicitarios, analíticas, u otros.

18. El contrato de encargo estipulará que el encargado de tratamiento tomará las medidas indicadas por el responsable relativo a la seguridad del tratamiento, incluyendo específicamente buenas prácticas de desarrollo y teniendo en cuenta la privacidad desde el diseño y por defecto desde la concepción misma de la aplicación.

En particular, se deben tener en cuenta con especial consideración las siguientes prácticas:

19. Proporcionar granularidad en la gestión de permisos de acceso a recursos protegidos del sistema de acuerdo con lo establecido en la política de privacidad. Un ejemplo es limitar los permisos de acceso a un recurso, como podría ser la carpeta de imágenes en lugar de otorgar un permiso genérico de acceso al almacenamiento del dispositivo.

20. Respetar las preferencias del usuario en cuanto a privacidad, por ejemplo, en cuanto a la personalización de anuncios, evitando, en su caso, el acceso incluso a identificadores de publicidad.

21. Evitar el acceso a identificadores globales únicos junto al identificador de publicidad del dispositivo, lo que permitiría hacer asignaciones que permiten dejar sin efecto medidas de protección del usuario como cambiar su identificador de publicidad.

22. Evitar la difusión de datos personales hacia servicios de analítica y publicidad desde el mismo momento en que se inicia la aplicación, sin que el usuario mismo haya podido hacer ningún uso o ajuste.

23. Comprobar que no hay difusión de datos personales sin conocimiento del responsable de tratamiento, al tratarse de comunicaciones iniciadas desde librerías de terceros utilizadas por el desarrollador para ampliar la funcionalidad de la aplicación o rentabilizarla económicamente.

24. Evitar la cesión de datos personales hacia destinatarios no especificados o informados en la política de privacidad, que tengan el rol de responsables de tratamiento o corresponsables.

25. Evitar transferencias internacionales de datos no declaradas en la política de privacidad.

26. Utilizar métodos avanzados para el cifrado de las comunicaciones (ej.: certificate-pinning¹) supone una garantía adicional para la privacidad de los usuarios a considerar dependiendo de las características del tratamiento de datos⁴.

⁴ <https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf>

2. Fase de investigación

2.1. Amenazas de seguridad en el ámbito de los dispositivos móviles.

2.1.1. Seguridad en Android:

En lo que a vulnerabilidades en Android respecta, hasta junio del 2019 se publicaron 86 fallos de seguridad, lo cual representa el 14% del total de vulnerabilidades reportadas para esta plataforma en 2018, año en que la cantidad de CVE alcanzó los 611 fallos publicados. Con estos datos, pareciera que en 2019 la cantidad de vulnerabilidades descenderá de manera abrupta en comparación a años anteriores.

Sin embargo, el 68% de los fallos publicados en 2019 fueron de criticidad alta y el 29% de ellos permitía la ejecución de código malicioso. Esto resulta una desmejora considerable respecto a años anteriores, donde el porcentaje de fallos graves era más bajo. Por ello, es importante que los usuarios instalen a tiempo los parches de seguridad para evitar verse afectados por serias vulnerabilidades como las parcheadas el pasado julio por Google. En particular, mucho se habló del fallo CVE-2019-2107 capaz que vulnerar equipos mediante la reproducción de videos en el dispositivo víctima, descripción que nos recuerda a las pasadas vulnerabilidades Stagefright y Metaphor.

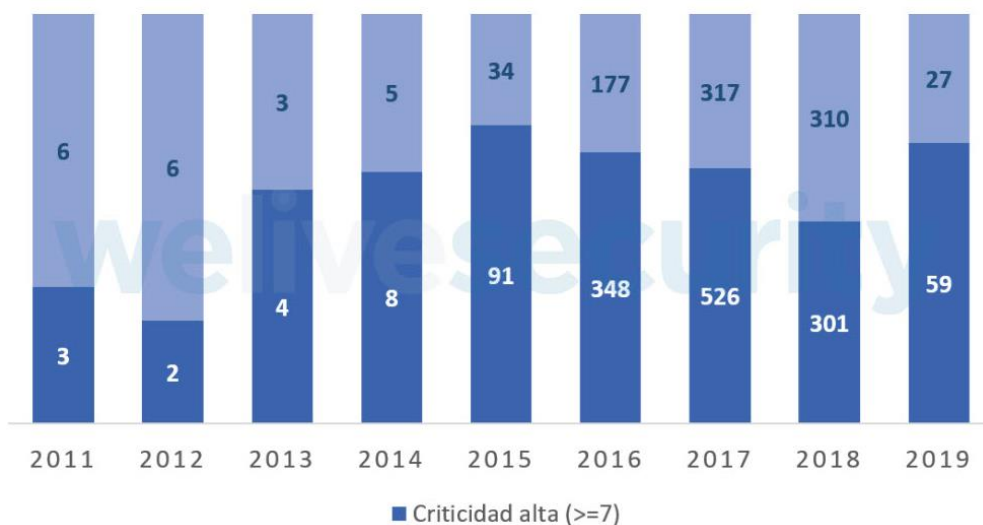


Figura 6: Vulnerabilidades de criticidad alta en Android a lo largo de los años.

En lo que a vulnerabilidades refiere, es interesante remarcar que el 90% de los dispositivos con Android utilizan versiones anteriores a Android Pie, mientras que el 74% de los Android no corren ni siquiera Oreo, según el sitio para desarrolladores de Android. Esto podría dejar expuestos teléfonos desactualizados ante fallos de gran envergadura que requieran cambios arquitectónicos en el sistema para repararse.

La buena noticia es que la cantidad de detecciones de malware ha decrecido un 8% con respecto al primer semestre de 2018 y un 10% respecto al segundo semestre del pasado año, quizás como resultado a los esfuerzos que Google e investigadores de seguridad realizan para detectar amenazas e impedir su propagación.

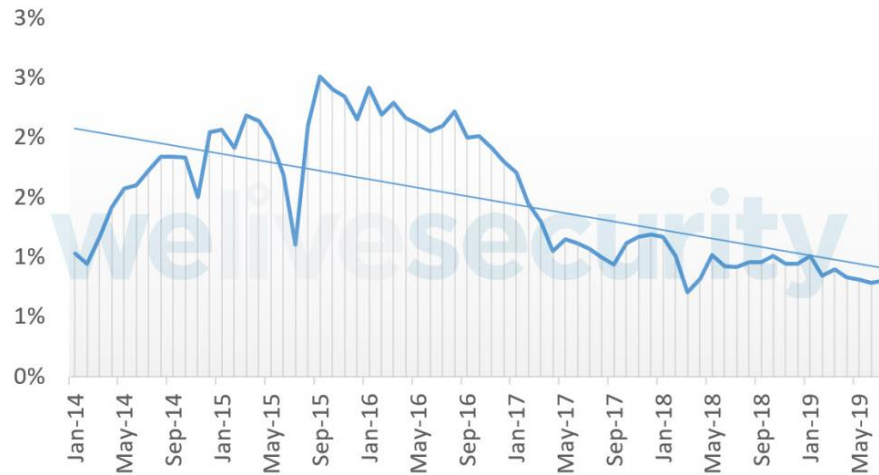


Figura 7: Detecciones de malware para Android en 2019.

Acompañando el decrecimiento en el número de detecciones, el promedio de nuevas variantes de códigos maliciosos para Android también ha disminuido a 240 nuevas variantes mensuales en comparación con las 300 nuevas variantes que encontrábamos años anteriores. Otro dato interesante es que Android resultó ser la cuarta arquitectura con mayor cantidad de nuevas variantes de malware, después de Win32, MSIL y VBA.

Uno de los tipos de códigos maliciosos que había experimentado un mayor crecimiento durante 2018 eran los criptomineros, representados con la firma Android/Coinminer, al punto que el 72% de las detecciones históricas de esta amenazas corresponden al pasado año. Afortunadamente, las detecciones de esta familia de malware han disminuido un 78% en el primer semestre de 2019.

A pesar de este decrecimiento, las criptomonedas siguen bajo la mira de los atacantes. Otra de las modalidades que usan para obtenerlas es mediante el robo de credenciales de acceso a billeteras en línea a través de troyanos inmiscuidos en Google Play Store, como ocurrió con estas falsas apps de billeteras electrónicas recientemente descubiertas.

Mientras, el malware bancario para Android también ha dado que hablar. Desde sus comienzos, la cantidad de nuevas variantes de spyware móvil y, particularmente, de troyanos dedicados al robo de datos financieros no para de aumentar. Variantes de Cerberus, un malware que superpone pantallas para robar credenciales bancarias, se han encontrado siendo vendidas mediante redes sociales en el último tiempo.

Respecto a este fenómeno común que es la propagación de malware en la tienda oficial de apps, un estudio desarrollado por ElevenPaths analizó el tiempo de permanencia de apps maliciosas en Google Play y reveló que estas apps maliciosas estuvieron un promedio de 51 días

disponibles para su descarga antes de ser eliminadas, llegando incluso a permanecer hasta 138 días en algunos casos.

Por su parte, el ransomware en Android ha mostrado una vez más un avance en su complejidad. Desde nuestros laboratorios descubrimos Android/Filecoder.C: una variante que utiliza tanto cifrado simétrico como asimétrico y que se propaga mediante mensajes SMS a la lista de contactos del equipo. Esto representa un salto en la complejidad del código comparado con otras familias de ransomware más antiguas, como DoubleLocker.

2.1.2. Seguridad en iOS:

Para iOS se publicaron 156 vulnerabilidades en lo que va de 2019, cifra que representan un aumento de 25% en la cantidad de fallos encontrados para este sistema operativo con respecto a 2018 y casi el doble de las encontradas en Android durante el corriente año. Es un claro indicador de que la cantidad de vulnerabilidades superará a fin de año la cifra obtenida en 2018. Sin embargo, el porcentaje de fallas de criticidad alta es inferior a Android, rondando el 20%.

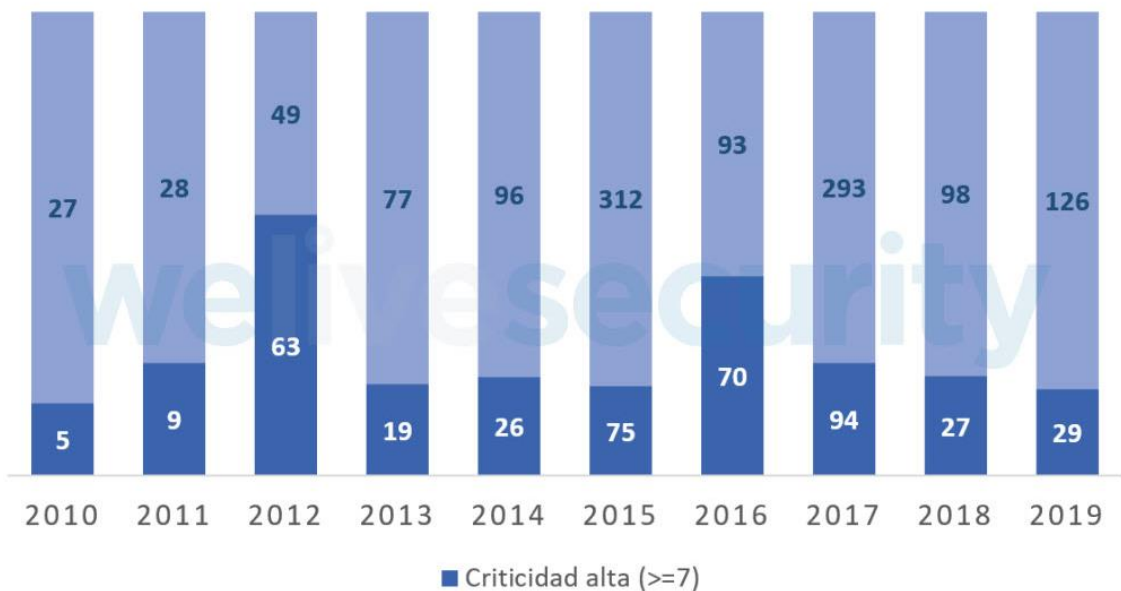


Figura 8: Vulnerabilidades de criticidad alta en iOS a lo largo de los años.

Por otro lado, las detecciones de malware para iOS aumentaron un 43% con respecto al primer semestre del pasado año. La cantidad de nuevas variantes de malware continúa siendo muy baja, lo cual nos indica que el interés de los cibercriminales continúa posándose sobre Android, donde se encuentra la mayor cantidad de usuarios.

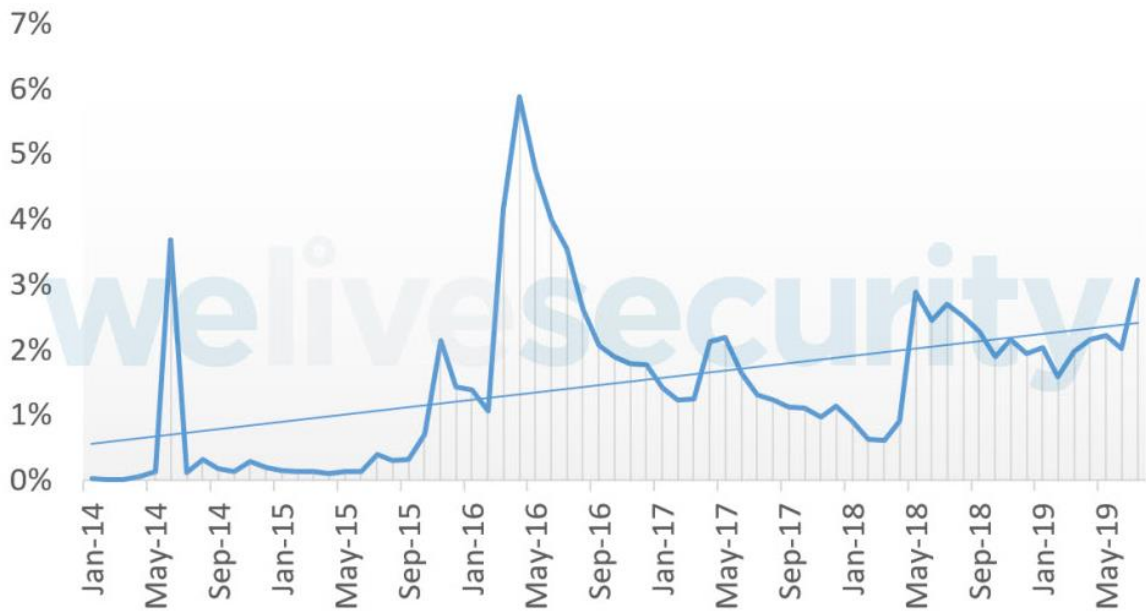


Figura 9: Detecciones de malware para iOS en 2019.

En este primer semestre del año, los teléfonos móviles de Apple también se vieron sujetos a vulnerabilidades que pusieron en peligro a sus usuarios, como ocurrió con el despliegue de versiones que accidentalmente reabrían fallos anteriormente corregidos y que permitieron la generación de un jailbreak para la versión 12.4. Otro ejemplo fue el bug en la aplicación FaceTime que permitía ser fácilmente explotado para espiar a terceros.

Aún más, el malware tampoco se ausentó en este sistema operativo y aparecieron masivas infecciones de spyware alrededor del mundo. Puntualmente, una variante denominada Exodus fue la que causó estragos hacia abril del corriente año, cuando varios usuarios descubrieron actividad maliciosa en sus equipos.

Además de todas estas amenazas creadas para cada uno de los dos sistemas operativos móviles más utilizados en el mundo, no debemos olvidar los riesgos multiplataforma asociados al uso de plataformas de terceros. Las vulnerabilidades encontradas en las aplicaciones de usuario pueden ser tan peligrosas como aquellas en el SO, como lo ejemplifica el fallo en WhatsApp últimamente descubierto que permitía alterar la respuesta en mensajes citados.

No podemos dejar de mencionar a los ataques de Ingeniería Social que intentan seducir a los usuarios mediante ciberestafas, como este engaño que suplanta identidad de WhatsApp ofrece 1000 GB para navegar por Internet. El furor por aplicaciones que se vuelven repentinamente tendencia como el caso de FaceApp también es aprovechado por cibercriminales para propagar malware y estafas en la web.

A pesar de que los sistemas móviles han sido diseñados desde una perspectiva de seguridad y son a veces más seguros que las tecnologías tradicionales, no debemos olvidar que los riesgos continúan latentes. Más allá del favoritismo, debemos siempre tener en mente que ningún

sistema es invulnerable y que la educación y prevención son ineludibles para usar las tecnologías móviles de forma segura.⁵

2.2. Medidas para proteger tu dispositivo:

2.2.1. Mantener el dispositivo actualizado

Un dispositivo actualizado es menos vulnerable. Las actualizaciones de software facilitadas por los fabricantes están orientadas, entre otras cosas, a mejorar la seguridad del dispositivo. Por tanto, mantener el dispositivo actualizado nos garantiza una seguridad más eficaz.

2.2.2. Protección frente accesos no deseados

La primera barrera de seguridad para proteger la privacidad de nuestros dispositivos móviles está basada en contraseñas y patrones de desbloqueo del dispositivo. Es fundamental que las claves de desbloqueo y acceso sean robustas (difíciles de romper), no predecibles y secretas.

En la guía:

Guía de Privacidad y seguridad en internet realizada por la Agencia Española de Protección de Datos (AEPD), el Instituto Nacional de Ciberseguridad (INCIBE) y la Oficina de Seguridad del Internauta (OSI), se enumeran consejos y recomendaciones sobre contraseñas, patrones y gestores de contraseñas.

Control de acceso al dispositivo móvil: Para evitar que la privacidad de nuestro dispositivo se vea comprometida es importante que esté bloqueado si no se está utilizando y que se desbloquee mediante el control de acceso que hayamos establecido: introducción de un código o patrón de desbloqueo o reconocimiento de patrones biométricos, como puede ser huella digital o reconocimiento facial. Además, es recomendable configurar el terminal para que se bloquee de forma automática tras un tiempo de inactividad. De esta forma se mitigan las amenazas a las que se puede ver expuesta nuestra privacidad por posibles descuidos.

Control de acceso a recursos del dispositivo móvil: Es interesante para proteger nuestra privacidad establecer, siempre que sea posible, un código de acceso a las aplicaciones y recursos de nuestro terminal, por ejemplo, al correo electrónico, galería gráfica, etc.

2.2.3. Cifrado del contenido del dispositivo móvil

Mediante el cifrado se asegura que el acceso al contenido se realizará sólo por quien conozca la clave de descifrado. El cifrado del contenido ofrece una barrera más de seguridad a nuestra privacidad.

La mayoría de las versiones de los sistemas operativos de Android e iOS ofrecen opción de cifrar el contenido del móvil, de tal forma que para acceder a cualquier información es necesario conocer la clave que permite que ésta pueda ser descifrada y mostrada.

⁵ <https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semester-2019/>

2.2.4. Gestión de contraseñas

Dado que gran parte de la seguridad la establecemos por medio del acceso controlado a nuestros dispositivos a través de contraseñas, es importante que dichas contraseñas sean seguras y robustas, es decir, elegidas de tal forma que no sean fácilmente predecibles ni sencillas de romper. Tener la precaución de no revelarlas a nadie.

En todo caso, cuando se maneja un elevado número de contraseñas puede resultar una tarea complicada recordar cada una de las claves elegidas. Para facilitar la gestión de las contraseñas y evitar su olvido, pero sin caer en la tentación de apuntarlas, utilizar claves fáciles de recordar o utilizar una misma contraseña para todos los accesos, existen herramientas que nos ayudan en esta tarea permitiendo almacenar todas nuestras claves de forma segura con tan sólo tener que recordar una única contraseña: la de acceso a nuestra herramienta de gestión de claves.

2.2.5. Detección de accesos y/o usos no controlados de dispositivo

Como ya se ha indicado, para detectar accesos y/o usos no controlados del dispositivo se recomienda revisar las aplicaciones instaladas en el terminal móvil para verificar que no haya ninguna aplicación que no hayamos instalado. Además, los dispositivos móviles suelen ofrecer utilidades para consultar el consumo de datos, la fecha y hora de acceso e incluso las aplicaciones que han utilizado esos datos. También es importante revisar la factura para comprobar que no haya ningún uso no controlado.

En los casos en que se produzca la pérdida o extravío del teléfono, existen herramientas antirrobo que ofrecen funcionalidades como facilitar la última ubicación del dispositivo móvil con conexión, reproducir un sonido incluso aunque esté en silencio, posibilidad de bloqueo en remoto del dispositivo y borrado del contenido, etc.⁶

2.3. Amenazas de seguridad móvil:

2.3.1. Filtración de datos

Las aplicaciones móviles a menudo son la causa de la filtración involuntaria de datos. Por ejemplo, como señaló eSecurity Planet, las aplicaciones "riskware" plantean un problema real para los usuarios móviles, que les otorgan amplios permisos, pero no siempre comprueban la seguridad. Por regla general, se trata de aplicaciones gratuitas que es posible encontrar en tiendas oficiales y que se ejecutan según su descripción, pero que también envían información personal (y tal vez, corporativa) a un servidor remoto, desde el cual los anunciantes o, incluso, los cibercriminales, pueden extraerla.

La filtración de datos también puede tener lugar a través de aplicaciones móviles con firma de empresas hostiles. En este caso, el malware móvil utiliza un código de distribución nativo en sistemas operativos móviles populares, como iOS y Android, para difundir datos valiosos en redes corporativas sin levantar sospechas. Para evitar este problema, procura otorgar a las

⁶ <https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas>

aplicaciones solo los permisos que necesitan y abstente de instalar cualquier programa que solicite más de lo necesario.

2.3.2. Wi-Fi no asegurada

Nadie quiere consumir datos de su celular si hay puntos de acceso inalámbrico disponibles; sin embargo, las redes Wi-Fi gratuitas generalmente son inseguras. De hecho, según V3, tres policías británicos que accedieron a participar en un experimento de seguridad asociado a redes inalámbricas gratuitas fueron fácilmente presa de ataques realizados por expertos en tecnología y vieron comprometidas sus cuentas de redes sociales, PayPal e, incluso, conversaciones a través de VoIP. Para mantenerte seguro, procura usar las redes Wi-Fi con prudencia en tu dispositivo móvil y no te conectes nunca a ellas para acceder a servicios confidenciales o personales, como sitios web de banca o información de tarjeta de crédito.

2.3.3. Suplantación de red

Suplantación de red es cuando los hackers configuran puntos de acceso falsos (conexiones que parecen redes Wi-Fi, pero que en la práctica son una trampa) en ubicaciones públicas concurridas, como cafeterías, bibliotecas y aeropuertos. Los cibercriminales asignan a estos puntos nombres comunes, como "Wi-Fi gratuita del aeropuerto" o "Cafetería", lo que anima a los usuarios a conectarse. En algunos casos, los atacantes exigen a los usuarios crear una "cuenta" para acceder a estos servicios gratuitos, usando una contraseña. No es de extrañar que numerosos usuarios utilicen la misma combinación de nombre de usuario y contraseña para múltiples servicios, lo que permite a los hackers comprometer su correo electrónico, credenciales de comercio electrónico y otra información confidencial. Además de recurrir a la prudencia cuando te conectes a cualquier red Wi-Fi gratuita, no proporciones nunca información personal y, si te solicitan crear credenciales de inicio de sesión, crea siempre una contraseña única, por si acaso.

2.3.4. Ataques de phishing

Como los dispositivos móviles están siempre encendidos, son las primeras líneas de cualquier ataque de phishing. Según CSO, los usuarios móviles son más vulnerables porque a menudo son los primeros en recibir correos electrónicos aparentemente legítimos y caer en la trampa. Los usuarios de equipos de escritorio que solo revisan su correo electrónico una vez al día o un día sí y otro no suelen conocer estos riesgos antes de hacer clic debido a la información compartida en sitios de noticias y boletines de seguridad. El monitoreo del correo electrónico es fundamental. No hagas nunca clic en enlaces de correo electrónico desconocidos. Pueden resultar aún más difíciles de verificar en la pantalla más pequeña de un dispositivo móvil. Ingresa siempre manualmente las direcciones URL para mantenerte lo más seguro posible.

2.3.5. Spyware

Según eWeek, a muchos usuarios de dispositivos móviles les preocupa el malware que envía flujos de datos a potencias extranjeras o a cibercriminales internacionales, pero existe una amenaza clave más cercana: el spyware. En numerosos casos, no es el malware lo que debe

preocuparles, sino el spyware instalado por cónyuges, compañeros de trabajo o empleadores para rastrear sus desplazamientos y patrones de uso. Descarga una solución antivirus potente (y legítima) y un paquete de detección de malware para detectar y eliminar estos programas antes de que puedan recopilar tus datos.

2.3.6. Criptografía quebrada

Según se señala en los materiales de capacitación del Infosec Institute, se pueden producir casos de criptografía quebrada si los desarrolladores de aplicaciones utilizan algoritmos de cifrado débiles o cifrado seguro sin una implementación adecuada. En el primer caso, los desarrolladores utilizan algoritmos de cifrado que ya poseen vulnerabilidades conocidas para acelerar el proceso de desarrollo de aplicaciones y el resultado es que cualquier atacante decidido puede descifrar las contraseñas y obtener acceso. En el segundo ejemplo, los desarrolladores utilizan algoritmos altamente seguros, pero dejan abiertas otras "puertas traseras" que limitan su eficacia. Por ejemplo, es probable que los hackers no puedan descifrar las contraseñas, pero si los desarrolladores dejan fallas en el código que permiten a los atacantes modificar funciones de alto nivel de la aplicación (como el envío o la recepción de mensajes de texto), los hackers puedan no llegar a necesitar las contraseñas para provocar estragos. En este caso, es responsabilidad de los desarrolladores y de las organizaciones aplicar estándares de cifrado antes de implementar las aplicaciones.

2.3.7. Gestión inadecuada de las sesiones

Con el fin de facilitar el acceso a transacciones en dispositivos móviles, numerosas aplicaciones usan "tokens", que permiten a los usuarios ejecutar varias acciones sin necesidad de volver a autenticar su identidad. De manera semejante a las contraseñas, estos son generados por las aplicaciones como una manera de identificar los dispositivos. Las aplicaciones seguras generan nuevos tokens con cada intento de acceso o "sesión", y estos deben permanecer confidenciales. Según el Proyecto de seguridad de aplicaciones de The Open Web, la gestión inadecuada de las sesiones se produce cuando las aplicaciones comparten involuntariamente tokens de sesión con entidades maliciosas, lo que les permite hacerse pasar por usuarios legítimos.⁷

2.4. Sistema operativo dispositivo sonda

Una vez seleccionado el dispositivo hardware que se empleará como base del dispositivo y el software que se encargará de generar y enviar datos y alertas, llega el momento de analizar cuál será el sistema operativo más adecuado como base.

Este dispositivo será el encargado de alojar el IDS Suricata y el agente ligero Beats, por lo que el sistema base deberá ser capaz de ejecutar estos servicios.

Con la creciente popularidad de los dispositivos Raspberry, han proliferado una gran variedad de sistemas operativos para estas placas. A continuación, exponemos los más representativos para un proyecto de estas características.

⁷ <https://latam.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store>

2.4.1. Raspbian Buster

Raspbian Buster es una distribución del sistema operativo Linux, libre y basado en Debían. Nació como un port no oficial de Debían para dar soporte a las CPUs basadas en ARM que empleaba este tipo de dispositivos. Para ello fueron modificadas multitudes de paquetes, mejorando el rendimiento respecto a la versión oficial en este tipo de plataformas. A pesar de esto, sigue empleando el sistema de paquetes DEB clásico de los sistemas Debían.

Con el lanzamiento de la Raspberry Pi 4 también llegó una nueva versión de su sistema operativo oficial: Raspbian Buster el Debían 10 para Raspberry Pi, desde su lanzamiento ya ha habido varias revisiones para incluir correcciones y funcionalidades.

Esta versión de Raspbian internamente es más compleja que las anteriores. Además de soportar el arranque con la partición `/boot/` de todos los modelos anteriores, tiene que incluir el arranque especial para Raspberry Pi 4 con soporte de la EEPROM (una especie de BIOS muy básica). Esta EEPROM es también una de las nuevas fuentes de problemas de arranque de la Raspberry Pi 4.

No hay grandes diferencias entre Debían Stretch y Debían Buster. En un triste reflejo de cómo es el mundo hoy en día, la mayoría de las diferencias son cambios de seguridad diseñados para hacer que Buster sea más difícil de hackear. Cualquier otra diferencia son en su mayoría pequeños cambios incrementales que la mayoría de la gente no notará.⁸

2.4.2. Ubuntu

Ubuntu es una distribución del sistema Linux basado en Debían. Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario. Ubuntu es una bifurcación del código base del proyecto Debían. El objetivo inicial era hacer de Debían una distribución más fácil de usar y entender para los usuarios finales, corrigiendo varios errores de este y haciendo más sencillas algunas tareas como la gestión de programas. Su primer lanzamiento fue el 20 de octubre de 2004 y su última versión es la 19.4 mediados de 2019, esta nueva versión es compatible con Raspberry.

Por primera vez, tenemos una versión de Ubuntu compatible con Raspberry Pi 4, esto significa que podemos aprovechar todo su potencial en un entorno de trabajo completo. Para poder usarlo, la imagen que tenemos que descargarnos es la misma que la de la Raspberry Pi 3. Y aunque funciona, una vez instalas un entorno gráfico no va todo lo fluido que debería. Quizás cuando lancen una versión de Ubuntu Mate para Raspberry Pi 4 si podamos usarla fluidamente, como si se tratara de Raspbian, pero con un escritorio más completo.⁹

2.4.3. Elección

Tras haber analizado y probado los sistemas previamente citados, Raspbian es el mejor SO disponible para Raspberry Pi, con una gran cantidad de información y recursos en la web. Esto

⁸ https://es.wikipedia.org/wiki/Raspberry_Pi

⁹ <https://es.wikipedia.org/wiki/Ubuntu>

es lo que la convierten en una excelente opción para trabajar con esta pequeña placa en continuo desarrollo.

Ojo, esto no quiere decir que Ubuntu sea un mal SO. También tiene toda la comunidad Ubuntu detrás, sólo tiene que optimizarse un poco, adaptarse a las posibilidades que tiene la Raspberry. Si siguen trabajando con ella, posiblemente acaben sacando un sistema operativo realmente bueno.

2.5. Arquitectura y flujo de datos

A lo largo de este apartado, se describe la arquitectura para el sistema de detección de intrusos y posterior análisis de datos, después de la experiencia durante la fase de investigación el software para Raspberry es más complicada que en un maquina con un procesador que no se ARM, mucho del software elegido lo vamos a tener que compilar con lo que conlleva ese trabajo. Otra de las opciones que hemos estado barajando y más importantes es implementar la instalación de la base de datos en un dispositivo físico o en la nube. Os mostramos los dos posibles escenarios para la arquitectura de nuestro TFM.

2.5.1. Escenario 1

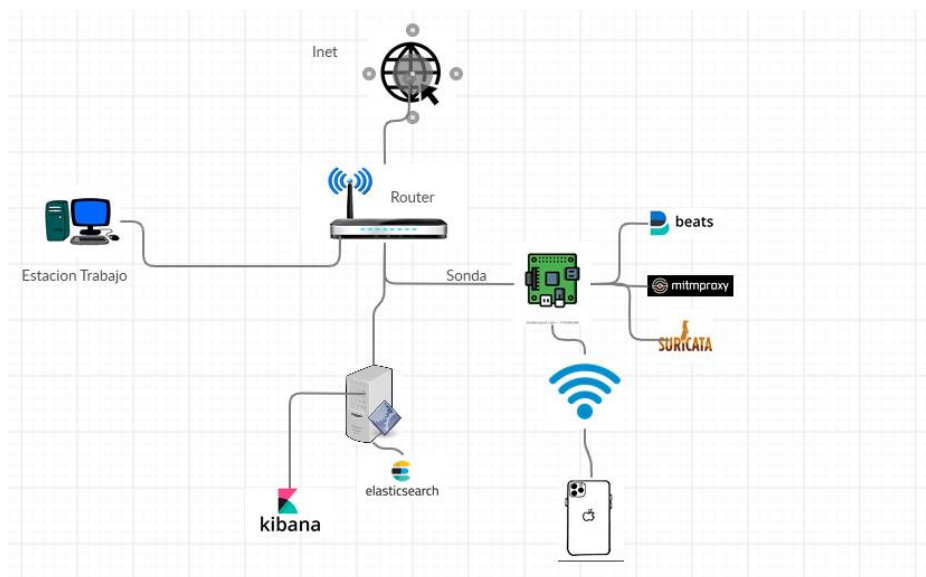


Figura 10: 10: Escenario 1 TFM.

Este primer escenario se basa en la instalación de todo el software necesario físicamente tanto en la Raspberry Pi como en un servidor Físico.

Ventajas:

- Costo, tener una "nube personal", es decir un servidor propio en la oficina o en la casa, resulta bastante económico. El único detalle es el gasto sustancial de la compra del servidor y su configuración inicial. Por supuesto, teniendo en cuenta que utilices sistemas operativos Open Source tales como Ubuntu Server no tendrás problemas.

- Privacidad, lo más importante es ser el dueño absoluto de tus datos. Los beneficios de tener tu propio server es que tú y solo tu pueden administrar la seguridad de los mismos (siempre y cuando conozcas como protegerla) y una de ellas es utilizando algún algoritmo de cifrado de datos a todo el disco y/o a los recursos sensitivos en el mismo.

Desventajas:

- Mayor coste debido a que se necesita equipos físicos, personal capacitado, conexión a Internet de alta velocidad, etc.
- Requiere de personal capacitado para mantener el sistema actualizado.
- El resultado final puede no cumplir con los estándares básicos del mercado.
- El sistema de respaldo es más difícil de implementar.
- El soporte depende del horario de trabajo de la persona a cargo del servidor físico.
- Las actualizaciones dependen del trabajo de la persona a cargo del servidor físico.

2.5.2. Escenario2

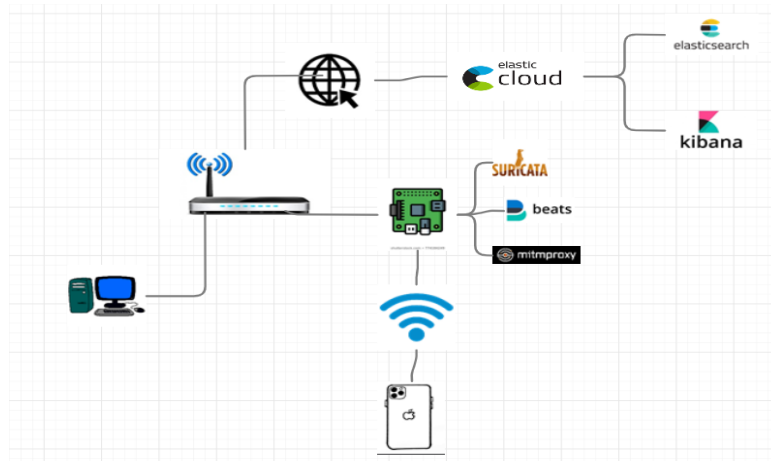


Figura 11: Escenario 2 TFM.

Este escenario se basa en la instalación del el software necesario físicamente en la Raspberry Pi y en el servidor de base de datos

Ventajas:

- Menor coste debido a que los equipos, personal y soporte lo proporciona la empresa que brinda el servicio.
- Personal altamente especializado (ya que la empresa tiene experiencia).
- El servicio cumple con los estándares básicos del mercado.
- Panel de administración intuitivo y herramientas sofisticadas.
- Sistema de respaldo sofisticado.
- Soporte 24 horas (muy útil en caso de fallos, ataques externos como malware, etc).
- Actualizaciones constantes y automáticas de la plataforma.

Desventajas:

- Se tiene un menor control y seguridad de la información.



Servidor en la nube 	Servidor local 
Precios más bajos y escalables	Altos costes de equipo y servicios
Actualizaciones automáticas	Costes de actualización y renovación
99,9 % accesibilidad	Susceptible de sufrir problemas o fallos
Sin coste de infraestructura ni soporte	Necesidad de un espacio físico
Sin necesidad de backup	Respaldo manual
Sin consumo energético	Alto consumo energético.
Información disponible 24/7/ 365	Coste por acceso remoto
Altos estándares de seguridad	La seguridad depende de la empresa
Pago por servicio SaaS	Coste de servidor + configuración
Escalabilidad infinita	Limitado al crecimiento de la empresa

Figura 12: Diferencias entre los servidores en local y en la nube.

2.5.3. Elección

En un primer estudio quizás el escenario 1 hubiera sido la mejor opción para nuestro proyecto, pero después de ver las soluciones de Cloud que nos ofrece Elastic nos vamos a decantar por el servicio en la nube, ya que no necesitamos contar con ninguna maquina física adicional, vamos a tener simplemente la Raspberry Pi, además de las numerosas ventajas expuestas anteriormente.

2.6. Elección de herramientas MITM

El primer elemento del sistema y pieza fundamental del mismo es el servicio de proxy-web. Este sistema es el intermediario entre los usuarios de una red y el acceso a internet. De manera general, estos sistemas funcionan según el proceso siguiente:

- El cliente solicita una página web al servidor proxy.
- El servidor proxy recibe la petición y consulta si la información solicitada la tiene guardada en su memoria cache.
- Si dispone de ella verifica si está actualizada, si es así se la ofrece al cliente.
- Si no es así, actualiza la información y se la ofrece al cliente.
- En caso de no disponerla en la memoria cache, la solicita, la almacena y se la ofrece al cliente.

Estos servicios tienen distintos modos de funcionamiento, como son:

- Transparente. Este modo no se configura en los navegadores o programas cliente. Por defecto, el tráfico web es remitido al servidor proxy que será el encargado de suministrar el contenido.

¹⁰ <https://blog.prodware.es/servidor-cloud-local-mejor-opcion-pymes/>

- Directo o Explícito. Este modo requiere que en los clientes se configure la dirección del servicio para poder funcionar.
- Inverso. Este modo, como su nombre indica, realiza el proceso contrario al explicado antes. Cuando un cliente solicita una web, el proxy es capaz de direccionarlo a distintos backend según su programación.

Nosotros nos vamos a centrar en dos software de proxy MITM Hyperfox: y MitmProxy.

2.6.1. Hyperfox

En el siguiente diagrama se puede ver cómo funcionaría Hyperfox es un esquema de red típico para la realización de ataques Man In The Middle.

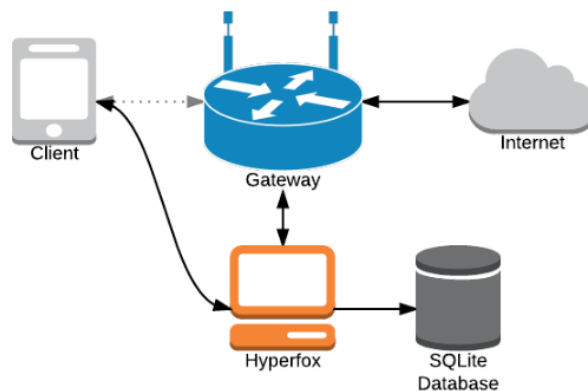


Figura 13: Diagrama proxy Hyperfox.

Esta herramienta también es capaz de capturar peticiones HTTPS, Hyperfox es capaz de crear certificados SSL al vuelo utilizando un certificado raíz auto firmado por el usuario. Si la máquina objetivo reconoce la CA como de confianza, la víctima no notará nada en su navegador, de lo contrario le saldrá el típico aviso de que el certificado digital no está reconocido por ninguna CA de confianza. Si la víctima acepta este certificado falso, todo el tráfico HTTPS será correctamente interceptado y guardado en una base de datos para su posterior tratamiento.

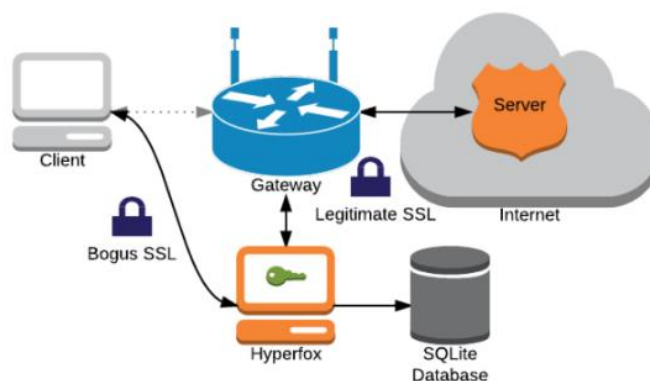


Figura 14: Diagrama proxy Hyperfox con SSL.

Esta herramienta guarda toda la información en una base de datos SQLite, además proporciona una interfaz gráfica de usuario muy sencilla donde podremos ver en tiempo real todos los mensajes intercambiados.¹¹

Sistemas operativos compatibles con Hyperfox

Este software es de código abierto, pero el equipo de desarrollo de la herramienta ha precompilado los ejecutables para sistemas Linux x64, Linux ARMv6, MacOS x64, FreeBSD x64 y también Windows de 32 bits. No obstante, siempre podremos descargar el código fuente de la página de GitHub para compilarlo nosotros mismos. Los requisitos para compilarlo es tener Go1.4, gcc y también Git. En la página de descargas de Hyperfox tenéis los pasos para compilar la herramienta sin problemas.

2.6.2. MitmProxy

En el siguiente diagrama se puede ver cómo funcionaría MitmProxy es un esquema de red típico para la realización de ataques Man In The Middle.

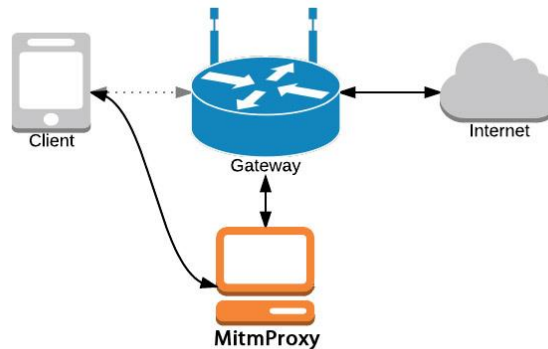


Figura 15: Diagrama Proxy MitmProxy.

Para las conexiones HTTP sin cifrar, esto es bastante simple: MitmProxy acepta una conexión desde el cliente HTTP, por ejemplo un navegador móvil, muestra la solicitud (y sus parámetros de solicitud) al atacante en la pantalla, y envía la solicitud al servidor web de destino como pronto como el atacante confirma - tal vez después de ajustar la solicitud de carga útil un poco. MitmProxy simplemente actúa como un intermediario.

Para el cliente, que parece como si el servidor MitmProxy estaba simplemente transmitiendo su conexión (como el router o servidores de su ISP hacer). Y al servidor, parece que el servidor MitmProxy es el cliente.

Características:

MitmProxy es una herramienta gratuita y de código abierto que nos va a permitir realizar auditorías de red fácilmente, este software nos permitirá crear un proxy HTTP/HTTPS para

¹¹ <https://www.redeszone.net/2016/10/02/hyperfox-uno-los-proxy-mitm-la-captura-trafico-http-https-mas-completos/>

capturar todas las peticiones web que un usuario realice, de tal forma que podamos leer todo lo que ocurra y modificarlas al vuelo.

Este software está disponible para sistemas operativos Microsoft Windows, Linux y también Mac OS X, únicamente es necesario contar con Python3 instalado en el sistema operativo para hacerlo funcionar, aunque próximamente van a portarlo a Python 3.5 en adelante para incorporar características nuevas. Respecto al funcionamiento en Windows, se ha incorporado un asistente de instalación que simplifica mucho el proceso, ideal para hacerlo rápidamente.¹²¹³

Una característica muy importante de este software es que tiene una interfaz gráfica de usuario basada en web, de esta forma, no tendremos que teclear comandos por consola, casi todo se puede hacer a través de dicha interfaz gráfica llamada mitmweb, pero las opciones más avanzadas solo estarán disponibles a través de la línea de comandos.

Algunas mejoras que se han realizado en el núcleo de MitmProxy es que han mejorado la interfaz de usuario a través de consola, ahora la indentación de los mensajes HTTP es mucho más visual, se pueden ordenar las diferentes columnas a nuestro antojo e incluso la barra de estado se ha mejorado. Aunque este Proxy es HTTP/HTTPS, también es compatible con HTTP/2, la nueva versión del conocido protocolo.

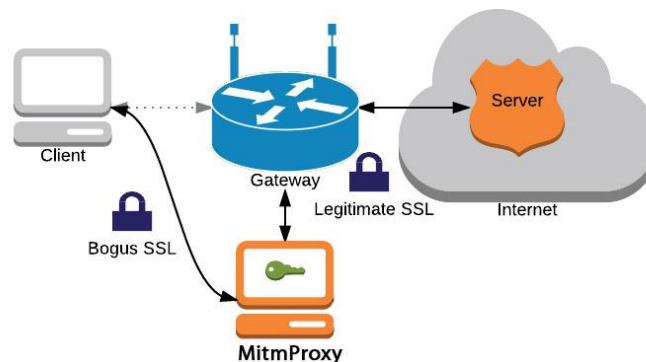


Figura 16: Diagrama Proxy MitmProxy con SSL.

2.6.3. Elección

Tras un pequeño análisis de los dos proxys que os mostramos vamos a elegir MitmProxy, ambos son muy similares pero la instalación de MitmProxy es más fácil para nuestro sistema.

2.7. Elección de herramientas IDS

Entre el amplio elenco de soluciones de detección de intrusos basados en red, cabe destacar dos productos sobre el resto: Snort y Suricata.

Snort ha sido el motor de IDS de facto durante años. Este motor tiene una enorme comunidad de usuarios soportándolo y, un abanico aún mayor y en aumento de suscriptores a sus reglas.

¹² <https://hacking-etico.com/2015/10/23/mitmproxy-mitm-de-trafico-web-for-fun-and-profit/>

¹³ <https://docs.mitmproxy.org/stable/>

Por otro lado, aunque Suricata no tiene una vida tan larga en comparación con Snort, ha estado reclamando mercado como una respuesta evolucionada o alternativa a este, basando sus argumentos principalmente en sus capacidades de proceso multi-hilo.

2.7.1. Snort

Hay infinidad de opciones a la hora de elegir motores IDS disponibles para automatizar y simplificar el proceso de detección de intrusiones, y Snort es una de las mejores opciones. Snort se ha convertido en la tecnología de prevención y detección más ampliamente extendida y confiable del mundo.¹⁴¹⁵

Snort utiliza un lenguaje basado en reglas que combina beneficios de inspección basados en firmas, protocolos y anomalías. Con su velocidad, potencia y rendimiento, Snort ganó impulso rápidamente. Con casi 4 millones de descargas hasta la fecha, Snort se ha convertido en la tecnología de detección de intrusos más utilizada del mundo.

El principal trabajo de Snort es escuchar el tráfico de red y buscar firmas en el flujo de datos que puedan indicar un incidente de seguridad en la infraestructura a monitorizar. Las reglas están configuradas para realizar una determinada acción. Esta acción puede ser pasiva, alertando del incidente, o activa, aplicando contramedidas en tiempo real.

Las organizaciones pueden aprovechar la aplicación de conjuntos de reglas existentes proporcionadas por la comunidad de Snort, así como escribir o modificar sus propias reglas de acuerdo con requisitos específicos de la red. Resulta posible escribir reglas complejas para identificar casi cualquier tipo de tráfico que atraviesa la red.

Gracias a la comunidad, las reglas de IDS se encuentran bajo una continua revisión y mejora con el fin de detectar las últimas amenazas de seguridad conocidas.

2.7.2. Suricata

Suricata es un sistema de detección de intrusos (al igual que Snort) basado en código abierto con el fin de construir la próxima generación. El objetivo de OISF es aportar nuevas ideas de seguridad e innovaciones tecnológicas a la industria de detección de intrusiones de IDS de código abierto.

Con la ayuda financiera del Departamento de Seguridad Interna de los Estados Unidos, se creó una alternativa multiproceso a Snort para ayudar a proteger las redes contra intrusiones de seguridad avanzadas.

La arquitectura de múltiples hilos de Suricata es única, ya que puede soportar sistemas multi-core y multiprocesador de alto rendimiento. Los principales beneficios de un diseño de múltiples hilos es que ofrece mayor velocidad y eficiencia en el análisis de tráfico de red y también puede ayudar a dividir la carga de trabajo de IDS / IPS en función de las necesidades de procesamiento. Además de la aceleración de hardware (con limitaciones de hardware y de tarjeta de red), el

¹⁴ <https://www.snort.org/>

¹⁵ <https://es.wikipedia.org/wiki/Snort>

motor está diseñado para utilizar la mayor potencia de procesamiento ofrecida por los últimos chips de CPU multi-núcleo.

Suricata se ha desarrollado con la idea de una fácil implementación, acompañado de documentación de inicio paso-a-paso y un potente manual de usuario. El motor también ha sido desarrollado en C, pensado desde los inicios para escalar. Adicionalmente, para facilitar la migración a este producto, Suricata emplea las mismas reglas y formatos de salida que Snort. Aunque Suricata sigue siendo un producto joven y menos extendido que su competencia, esta tecnología está ganando impulso entre los usuarios y empresas. El aumento del rendimiento, la compatibilidad con IPv6 nativa, modelos estadísticos de detección de anomalías y aceleración GPU son, entre otras, los principales puntos a favor de este motor.¹⁶

2.7.3. Elección

Tras un análisis de los motores de búsqueda, a pesar de encontrarse a la par en tecnología, Suricata parece situarse ligeramente adelantado respecto a Snort. En lo que respecta al proyecto, se decide emplear Suricata como motor de detección dado que su capacidad multi-hilo y escalabilidad aprovechan mejor las características hardware del dispositivo Raspberry Pi 3 Modelo B del que disponemos. Se recuerda que este dispone de un procesador ARM de cuatro núcleos que podrán ser utilizados de manera concurrente por este motor.

snort vs suricata

Parameter	Snort	Suricata
Developer	Sourcefire, Inc.	Open Information Security Foundation (OISF)
Availability	Since 1998	Since 2009
Coded Language	C	C
Operating System	Cross-platform	Cross-platform
Stable Release	2.9.5.5 (16 September 2013)	1.4.5 (26 July 2013)
Threads	Single-threaded	Multi-threaded
IPv6 Support	Yes	Yes
Snort (VRT) Rules Support	Yes	Yes
Emerging Threats Rules Support	Yes	Yes
Logging Format	Unified2	Unified2
Aanval Compatible	Yes	Yes

Figura 17: Tabla comparativa Snort Suricata.

2.8. Envío de datos:

2.8.1. Logstash

Logstash es un motor de recolección de datos de código abierto desarrollado por Elastic, creadores de Elasticsearch. Este puede unificar dinámicamente datos de fuentes dispares y normalizar los datos en destinos de su elección.

¹⁶ <https://suricata-ids.org/>

Si bien Logstash originalmente impulsó la innovación en la recopilación de registros, sus capacidades se extienden mucho más allá de ese caso de uso. Cualquier tipo de evento puede ser enriquecido y transformado con una amplia gama de entradas, filtros y plugins de salida, con muchos códec nativos simplificando aún más el proceso de la ingesta.

Esto permite modificar los registros para almacenar toda la información necesaria, en el formato que más nos interese y de la forma más óptima.

La aplicación se encuentra basada en jRuby y requiere de una maquina “Java virtual Machine” para funcionar. Gracias a esto la herramienta es multiplataforma, pudiendo ser ejecutada en cualquier sistema operativo moderno como Linux, Mac OS X o Windows.¹⁷

Otra ventaja de Logstash es que ha sido creada por el mismo desarrollador que la base de datos. Esto asegura que no habrá incompatibilidad entre las diferentes piezas de la implementación.

El punto negativo de este cliente, es que no se encuentra disponible oficialmente en arquitecturas ARM (No lo podemos instalar en nuestra Raspberry), y las versiones beta disponibles no se encuentran suficientemente pulidas en términos de estabilidad por su elevado uso de cómputo.

2.8.2. Beats

Beats, una serie de agentes ligeros de reenvío, de código abierto, desarrollados también por Elastic como una alternativa más ligera a Logstash. Originalmente, para la ingesta de datos era necesaria la inclusión de Logstash como nodo puente en la arquitectura. Desde la versión 5.0 en adelante, Elasticsearch admite la entrada directamente desde Beats, simplificando el diseño de esta.

Packetbeat, Filebeat, Metricbeat y Winlogbeat son algunos ejemplos de Beats. Packetbeat es un analizador de paquetes de red que envía información sobre las transacciones intercambiadas entre sus servidores de aplicaciones. Filebeat envía archivos de registro desde sus servidores. Metricbeat es un agente de monitoreo de servidores que periódicamente recopila métricas de los sistemas operativos y servicios que se ejecutan en sus servidores. Y Winlogbeat envía registros de eventos de Windows.

Para el caso que atañe al proyecto, el cliente correcto sería Filebeat. Este, a diferencia de su hermano mayor, se encuentra implementado en versiones estables para arquitecturas con procesador ARM. En contrapartida, no ofrece la potencia de procesado que ofrece Logstash.

2.8.3. Elección

Tras evaluar los pros y contras de los dos productos, se decide emplear Filebeat. Este producto, en comparación con Logstash, ofrece una versión más estable en arquitecturas con procesador ARM como la que se ha seleccionado para el dispositivo sonda. Así mismo, este cliente ligero ofrece una capacidad de interpretación menor, pero suficiente para los campos de los mensajes de alerta de Suricata.

¹⁷ <https://www.elastic.co/es/>

Esta última razón también deriva en un uso de recursos bastante menor, lo cual también beneficia al dispositivo sonda, que recordamos tiene unas prestaciones contenidas.

2.9. Elección de Base de datos

2.9.1. Elasticsearch

ElasticSearch es una solución de base de datos y servidor de búsqueda basado en Lucene. Este producto provee un motor de búsqueda distribuido y con capacidad multi-tenencia.

El término multi-tenencia se refiere a una arquitectura de software en la que una única instancia de software se ejecuta en un servidor y sirve a varios inquilinos. Los inquilinos son un grupo de usuarios que comparten un acceso común con privilegios específicos a la instancia de software. Con una arquitectura multi-tenencia, una aplicación de software está diseñada para proporcionar a cada inquilino una parte dedicada de la instancia, incluyendo sus datos, configuración, gestión de usuarios, funcionalidad individual y propiedades no funcionales. multi-tenencia contrasta con arquitecturas multi-instancia, donde las instancias de software por separado operan en nombre de los diferentes inquilinos.

Por otra parte, Leucene es una interfaz de programación de aplicaciones, o API, de código abierto pensada para la recuperación de información. Esta está orientada a cualquier aplicación que requiera indexado y búsqueda a texto completo.

El centro de la arquitectura lógica de Lucene se encuentra el concepto de Documento (Document) que contiene Campos (Fields) de texto. Esta flexibilidad permite a Lucene ser independiente del formato del fichero.

Esta solución emplea una interfaz RESTful. Esto es un estilo de arquitectura software para sistemas hipermedia distribuido y describe una interfaz entre sistemas que emplea HTTP para obtener datos o ejecutar operaciones sobre estos sin abstracciones adicionales.

Los sistemas REST, y por tanto nuestra elección, cumplen con una serie de fundamentos clave:

- Un protocolo Cliente-Servidor sin estado, es decir, cada mensaje contiene toda la información necesaria para comprender la petición. Por consiguiente, ninguna de las dos partes requiere recordar ningún estado.
- Un conjunto de operaciones bien definidas que se aplican a todos los recursos de la información.
- Una sintaxis universal para identificar los recursos. En los sistemas REST cada recurso es direccionarle únicamente a través de su URI.

Por último, los ficheros de datos emplean el formato JSON. Acrónimo de JavaScript Object Notation, es un formato de texto ligero para el intercambio de datos. Una de las principales ventajas de este formato es la simplicidad de implementar un analizador sintáctico.

Pero no todo acaba aquí. La velocidad de proceso de ElasticSearch radica en su escalabilidad horizontal.

2.9.2. Elastic Cloud

Es el servicio manejado de Elastic que ofrece Elasticsearch, App Search y Site Search en modo SaaS. Elasticsearch Service es el servicio de propósito general que nos permite desplegar todo tipo de soluciones, desde casos de búsqueda, centralización de logs y APM entre otros.

Elastic Cloud es nuestra creciente familia de ofertas de SaaS que facilitan el despliegue, la operación y el escalado de productos y soluciones Elastic en la nube. Desde una experiencia de Elasticsearch hospedado y administrado fácil de usar hasta soluciones de búsqueda potentes y listas para usar, Elastic Cloud es tu trampolín para poner a Elastic a trabajar para ti sin problemas.

2.9.3. Elección

En este caso, existiendo únicamente un producto, la elección reside en el modo de configuración, entre una única instancia física o en la nube. Esta elección depende de la cantidad de información que se desee almacenar y el presupuesto del que se disponga.

2.10. Interfaz gráfica

La elección de esta influirá en gran medida en la agilidad y capacidad de interpretar los eventos de seguridad que se han detectado en fases anteriores. Una mayor claridad en la exposición de los datos y posibilidad a la hora de aplicar filtros jugarán a favor de la eficiencia a la hora de investigar incidentes de seguridad.

A continuación, se comentan las dos herramientas más populares en este ámbito:

2.10.1. Graylog

Graylog es una solución para visualizar registros almacenados en una base de datos Elasticsearch. Graylog permite realizar consultas avanzadas sobre los datos almacenados, crear tableros con los resultados de las mismas o incluso generar alarmas ante determinados datos o ausencia de ellos.

El acceso se realiza vía navegador y dispone autenticación de usuarios para poder gestionar el acceso a la aplicación. La parte servidor solo tiene versiones RPM y DEB, por lo que únicamente funcionará sobre plataformas Red Hat, Debían y similares.

A pesar de emplear la base de datos Elasticsearch, Graylog necesita de una base de datos adicional MongoDB o MariaDB para almacenar su configuración, usuarios, etc.

Una de las principales desventajas es que Graylog no es compatible con la última versión de Elasticsearch 5.x, perdiendo el gran potencial que ofrece esta base de datos actualmente.

En las siguientes imágenes se observa la interfaz gráfica de Graylog:¹⁸

¹⁸ <https://www.graylog.org/>

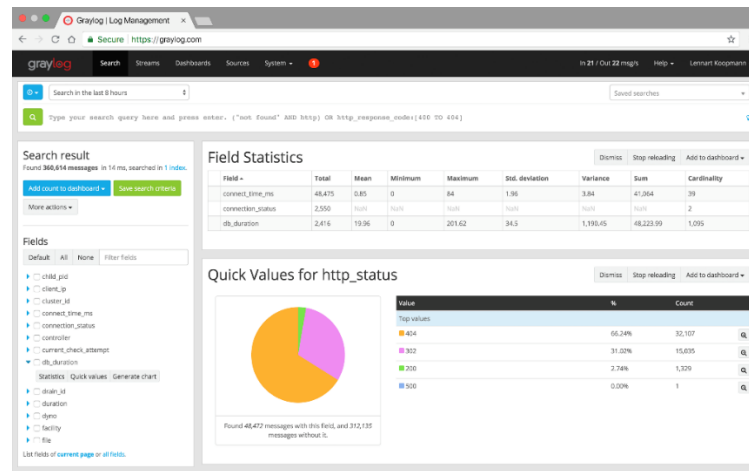


Figura 18: Interfaz Gráfica Graylog.

2.10.2. Kibana

Kibana es la alternativa a Graylog propuesta por Elastic. Esta solución es una potente herramienta pensada para el análisis masivo de datos almacenados en una base de datos Elasticsearch. Gracias a esta concepción, enfocada al Big Data, Kibana ofrece una infinidad de nuevas posibles representaciones gráficas para los eventos, como mapas de calor, localizaciones, etc.

Como su alternativa, Kibana ofrece un servicio accesible vía navegador. Si bien la opción de acceso mediante usuarios no está disponible en la versión básica, se puede implementar añadiendo el modulo X-Pack o un proxy Nginx para tal fin.

El software servidor no tiene dependencias del sistema operativo en el que se encuentra dado que, al igual que el resto de software de Elastic, se monta sobre la Máquina Virtual Java (JVM). Otra de las principales ventajas de Kibana es su completa integración con el resto de productos elegidos. Al ser un stack pensado y recomendado por el propio fabricante, no existirán incompatibilidades entre versiones al actualizar el software.

A continuación, se presentan capturas de múltiples posibles interfaces diseñadas en Kibana:



Figura 19: Interfaz Gráfica Kibana.

2.10.3. Elección

Las dos herramientas resultan muy efectivas para este cometido. Las posibilidades de personalización juegan a favor de Kibana, pues es mucho más personalizable que Graylog.

A nivel de seguridad Graylog ofrece de manera nativa la autenticación por usuarios, pero no resulta una ventaja diferenciadora dado que existe la posibilidad de añadirlo mediante módulos adicionales.

Pero el último factor determinante es la compatibilidad con la base de datos. En estos momentos, solo Kibana permite trabajar con la versión 5.x de Elasticsearch, lo cual decanta definitivamente la balanza hacia este producto.

3. Fase de desarrollo

Una vez definida la arquitectura del sistema de detección de intrusos y análisis de datos basado en red en el apartado anterior, se realizará un despliegue de la arquitectura mínima de la plataforma.

Con este despliegue se desea obtener un laboratorio del cual extraer datos valiosos del funcionamiento del sistema más allá del permisivo papel, donde todo funciona correctamente.

De este entorno se obtendrá un manual de despliegue probado, con puntos a tener en consideración tras instalaciones fallidas, deficientes o mejorables.

A lo largo de este apartado se describen los diferentes puntos de la instalación llevada a cabo.

3.1. Sistema operativo dispositivo sonda

3.1.1. Preparar la tarjeta microSD y descargando NOOBS

Lo primero que tenemos que hacer para instalar Raspbian en nuestra Raspberry Pi es preparar la tarjeta microSD para copiar los archivos necesarios. Para ello tenemos que formatearla con el sistema de archivos FAT32.

Ahora que ya tenemos preparada la tarjeta microSD, lo que tenemos que hacer para instalar Raspbian en nuestra Raspberry Pi es preparar la tarjeta microSD para copiar los archivos necesarios. Para ello tenemos que crear una partición con el sistema de archivos FAT32 en la que cojan todos los archivos que nos hemos descargado.

Todo este proceso lo vamos a realizar con el Administrador de discos de Windows. Para ello, pulsaremos la tecla de Windows y la R para que se abra la ventana y ahí escribiremos *diskmgmt.msc*. Una vez se nos abra el administrador de discos podremos borrar todas las particiones de la tarjeta microSD y crear una nueva partición FAT32.

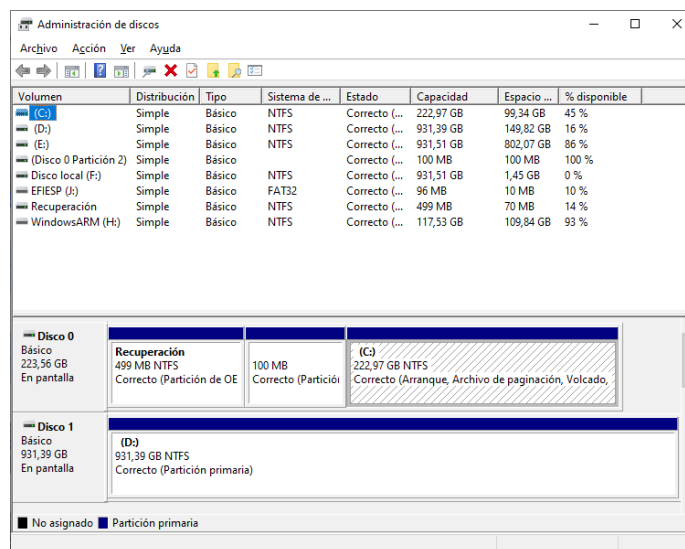


Figura 20: Administrador de discos Windows.

Ahora que tenemos todos los dispositivos de almacenamiento disponibles, buscamos la tarjeta microSD donde vamos a instalar Raspbian y eliminamos todas las particiones. Para eliminar todas las particiones vamos pulsando con el botón derecho en cada partición que tenga la tarjeta microSD y haciendo clic donde pone Eliminar volumen. Para ello tenemos que fijarnos en el contenido del punto de montaje o letra de la unidad antes de borrarla, ya que, si nos equivocamos, es posible que no podamos recuperar los datos de esa partición.

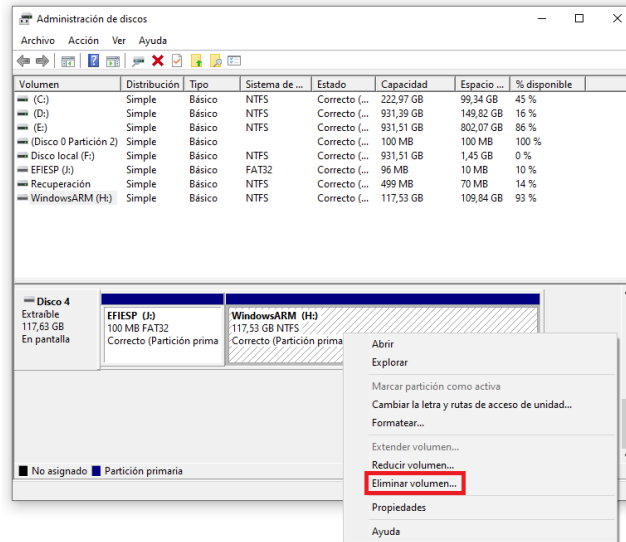


Figura 21: Administrador de discos Windows.

Ahora que ya tenemos la tarjeta microSD vacía, tenemos que crear una partición para poder copiar NOOBS. Esto se realiza de forma sencilla, pulsando con el botón derecho en el espacio no asignado de nuestra tarjeta microSD y haciendo clic en Nuevo volumen simple en el menú contextual. Ahí nos aparecerá un asistente que nos permitirá crear la partición para NOOBS.

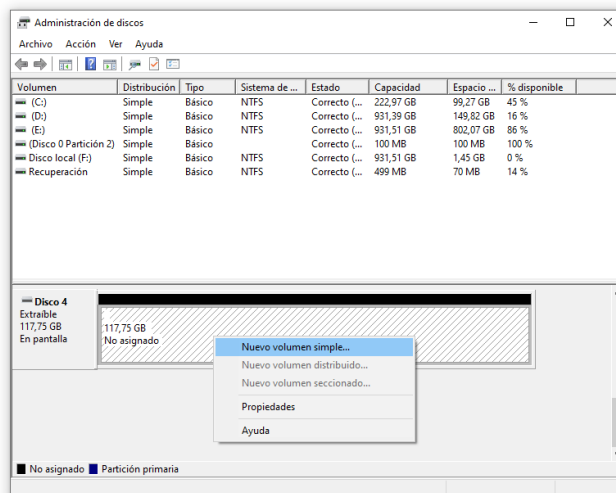


Figura 22: Nuevo volumen simple.

En dicho asistente, pulsamos primero en Siguiente para pasar a la pantalla donde asignaremos primero el tamaño de la partición. Si vamos a usar la imagen completa de NOOBS, recomendaría

usar un mínimo de 2560 MB, el equivalente a 5GB para almacenar tanto NOOBS como la imagen de Raspbian. Si vamos a usar NOOBS Lite, con solo 512 MB nos sobrará para copiar los archivos de NOOBS en la partición.

En la siguiente pantalla del asistente nos preguntará que letra le queremos asignar a la partición. En este caso, como nos es indiferente la letra, ya que lo único que queremos es tener la partición disponible para poder copiar los archivos de NOOBS, le daremos a Siguiente para pasar a la siguiente parte del asistente.

Ahora nos tocará formatear la partición y configurar el sistema de archivos de esta. Como bien he indicado al principio de esta parte del tutorial, necesitamos que esta partición sea FAT32 para que la Raspberry Pi pueda leerla. Así que en el asistente elegimos Formatear este volumen con la configuración siguiente y donde pone Sistema de archivos tenemos que elegir FAT32. Ahora pulsamos en Siguiente y luego en Finalizar y ya tenemos creada nuestra partición. Por si tenéis dudas, aquí os dejo una captura de cómo tiene que quedar la última pantalla antes de crear la partición.

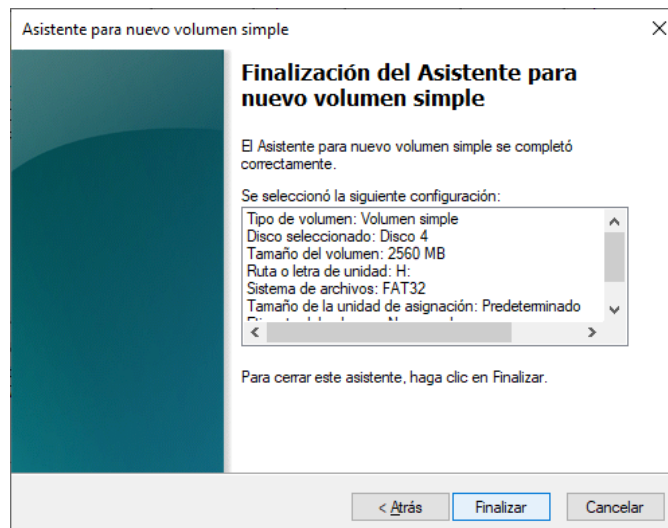


Figura 23: Finalización asistente.

Una vez que tenemos la tarjeta formateada y limpia, vamos a descargar la imagen de NOOBS con Raspbian. Esta la podemos encontrar en la sección de descargas de la web oficial de Raspberry Pi. Si disponemos de conexión a internet en la Raspberry Pi, podemos descargar NOOBS Lite para que luego sea el propio NOOBS el que se encargue de descargar la imagen de Raspbian para grabarla en la tarjeta microSD.

Ahora que tenemos el archivo descargado, extraemos el contenido de este en la raíz de la microSD. Con esto ya podemos olvidarnos de nuestro ordenador y comenzar a instalar Raspbian en nuestra Raspberry Pi.

3.1.2. Instalando Raspbian en la Raspberry Pi

Seguramente tienes muchas ganas de terminar este tutorial lo más rápido posible y empezar a usar tu Raspberry Pi. Aun así, si quieres seguir hasta el final asegúrate de tener un teclado y un ratón USB porque todo lo que vamos a hacer a continuación lo haremos desde la Raspberry Pi.

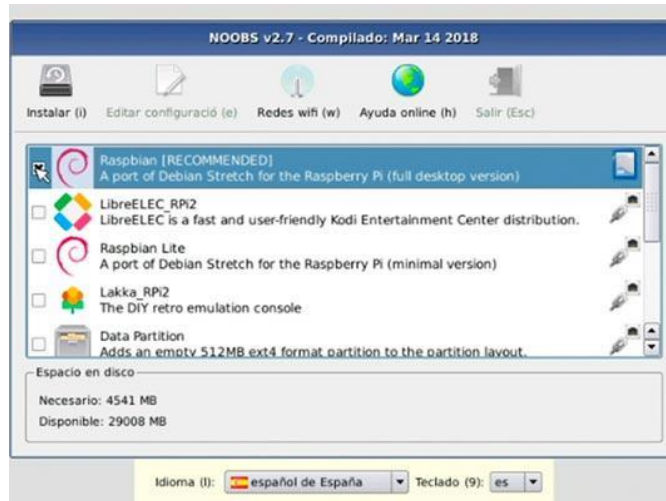


Figura 24: Instalador Raspbian.

Una vez introducimos la tarjeta microSD en la Raspberry Pi y la enchufamos a la corriente, lo primero que nos aparece es un menú donde tenemos que elegir qué sistema operativo vamos a instalar. En este caso elegiremos instalar Raspbian, que aparece con la etiqueta [RECOMMENDED]. La marcamos y pulsamos en install. Aquí no importa mucho si cambiamos el idioma a español, ya que el sistema operativo seguirá instalándose en inglés.

Después de aproximadamente 10 minutos, un mensaje nos dirá que el sistema operativo está instalado y al pulsar en OK la Raspberry Pi se reiniciará. Ahora ya nos podemos sentir orgullosos por instalar Raspbian en nuestra Raspberry Pi

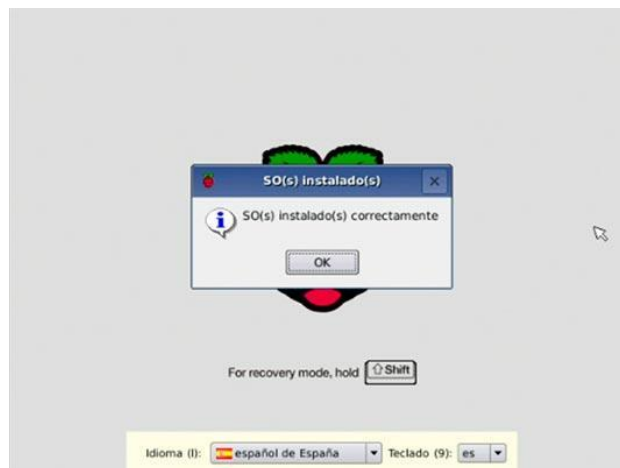


Figura 25: Raspbian instalado correctamente.

3.2. Crear un proxy MITM para la captura de tráfico.

3.2.1. Descripción

En este TFM vamos a realizar la configuración de un Raspberry Pi 3 que actúa como un punto de acceso Wi-Fi, ejecutando un proxy transparente man-in-the-middle (MitmProxy), que se puede usar para detectar el tráfico HTTP y HTTPS en los dispositivos conectados.

Un proxy MITM es una pieza de software que se ejecuta en un dispositivo (por ejemplo, un punto de acceso Wi-Fi o un enrutador de red) entre un cliente (su teléfono, su computadora portátil) y el servidor con el que desea comunicarse. El proxy puede interceptar y analizar la información que se envía entre el cliente y el servidor. Incluso puede manipular la solicitud que se envía o modificar la información que se devuelve.

Un proxy MITM no necesita ser "malicioso", aunque supongo que esto depende de su visión de la privacidad de la información y la implementación de los controles de seguridad de TI. La mayoría de las grandes organizaciones corporativas generalmente emplean un proxy MITM para escanear y filtrar el tráfico digital que se mueve dentro de su red interna y una red externa (como Internet). De esta forma, podrían detectar a alguien moviendo información confidencial fuera del entorno controlado de la compañía, y también intentar evitar que se instale malware en las máquinas del personal.

Un ejemplo de un proxy MITM malicioso sería un punto de acceso Wi-Fi al que puede conectarse para pensar que es confiable. Quizás esté en una cafetería y vea en su teléfono que hay un punto de acceso llamado "Cafetería FREE Wi-Fi". Incluso puede tener un portal "falso" con la misma contraseña "correcta" que le dio un proxy (legítimo). El problema es que este punto de acceso no tiene nada que ver con la cafetería, en realidad se está ejecutando en un dispositivo en el bolsillo de un hacker cercano, y ahora cualquier tráfico no HTTPS que se envía entre su computadora portátil y los sitios web que visita son visibles para el hacker, y puede ser registrado para su posterior inspección. Con un poco de esfuerzo, también es posible que el pirata informático pueda espiar su tráfico HTTPS. En una variación de este escenario, el hacker puede haber comprometido previamente a "Cafetería FREE Wi-Fi" verdadero punto de acceso Wi-Fi y podría reenviar el tráfico desde el punto de acceso a su máquina. En cualquier caso, el hacker puede inspeccionar el tráfico entre su dispositivo y el destino previsto.

3.2.2. Estructura

MitmProxy suelen centrarse en el filtrado de contenidos o de optimización de la velocidad a través de la memoria caché, el objetivo de MitmProxy es permitir que un atacante monitorear, capturar y alterar estas conexiones en tiempo real.

Atacando las conexiones HTTP

Para las conexiones HTTP sin cifrar, esto es bastante simple: MitmProxy acepta una conexión desde el cliente HTTP, por ejemplo un navegador móvil, muestra la solicitud (y sus parámetros de solicitud) al atacante en la pantalla, y envía la solicitud al servidor web de destino como pronto como el atacante confirma - tal vez después de ajustar la solicitud de carga útil un poco. MitmProxy simplemente actúa como un intermediario:

Para el cliente, que parece como si el servidor MitmProxy estaba simplemente transmitiendo su conexión (como el router o servidores de su ISP hacer). Y al servidor, parece que el servidor MitmProxy es el cliente.

Atacar a las conexiones HTTPS

Durante el ataque a cifrar el tráfico HTTP se puede hacer sin tener que lidiar con los certificados X.509 y las autoridades de certificación (CA), conexiones HTTPS con cifrado SSL encripta cada petición y respuesta entre el cliente y el servidor de extremo a extremo.

Y debido a que los datos transferidos se cifran con un secreto compartido, un hombre medio (o un equivalente) no pueden descifrar los paquetes de datos intercambiados.

Cuando el cliente abre una conexión SSL / TLS para el servidor web seguro, verifica la identidad del servidor mediante la comprobación de dos condiciones:

En primer lugar, se comprueba si el certificado fue firmado por una CA conocida al cliente. Y en segundo lugar, se asegura de que el nombre común (CN, también: el nombre de host) del servidor coincide con el que se conecta.

Si se cumplen ambas condiciones, el cliente asume la conexión es segura.

Con el fin de ser capaz de olfatear en la conexión, MitmProxy actúa como una autoridad de certificación, sin embargo, no es un muy digno de confianza uno:

En lugar de emitir certificados a personas u organizaciones reales, MitmProxy genera dinámicamente certificados a cualquier nombre de host que se necesita para una conexión.

Si, por ejemplo, un cliente desea conectarse a `https://www.facebook.com`, MitmProxy genera un certificado para "www.facebook.com" y lo firma con su propia CA.

Siempre que confía el cliente esta CA, ambos de los anteriores mencionados son ciertas condiciones (CA de confianza, misma CN) - lo que significa que el cliente cree que el servidor MitmProxy es, de hecho, "www.facebook.com".

La siguiente figura muestra el flujo de petición / respuesta para este escenario. Este mecanismo se denomina proxy HTTPS transparente.

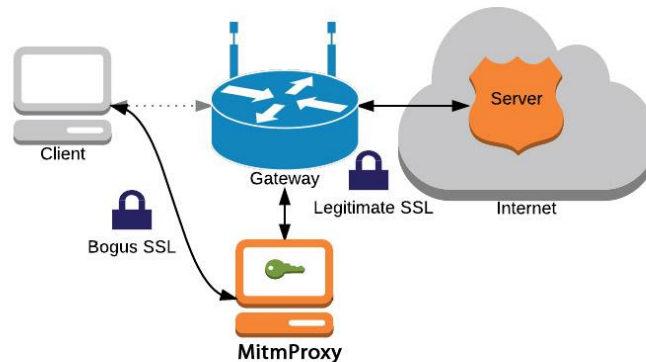


Figura 26: MitmProxy con certificado Https.

Para este ataque funcione, hay algunas condiciones que se deben cumplir:

- MitmProxy como pasarela estándar (HTTP y HTTPS): Para HTTP y HTTPS proxy, el servidor que ejecuta MitmProxy debe, por supuesto, ser capaz de interceptar los paquetes IP - lo que significa que debe estar en algún lugar en el camino de la trayectoria de paquetes. La forma más

sencilla de lograr esto es cambiar la puerta de enlace predeterminada en el dispositivo cliente a la dirección del servidor MitmProxy.

- CA de confianza MitmProxy (HTTPS): (y confiar en) Para el proxy HTTPS funcione, el cliente debe conocer la CA MitmProxy, es decir, el archivo de claves de CA se debe agregar al almacén de confianza del cliente.

3.2.3. Requisitos técnicos

Raspberry Pi 3:

Raspberry es una placa computadora de bajo coste desarrollada en el Reino Unido por la Fundación Raspberry pi, con el objetivo de estimular la enseñanza de la informática en las escuelas.

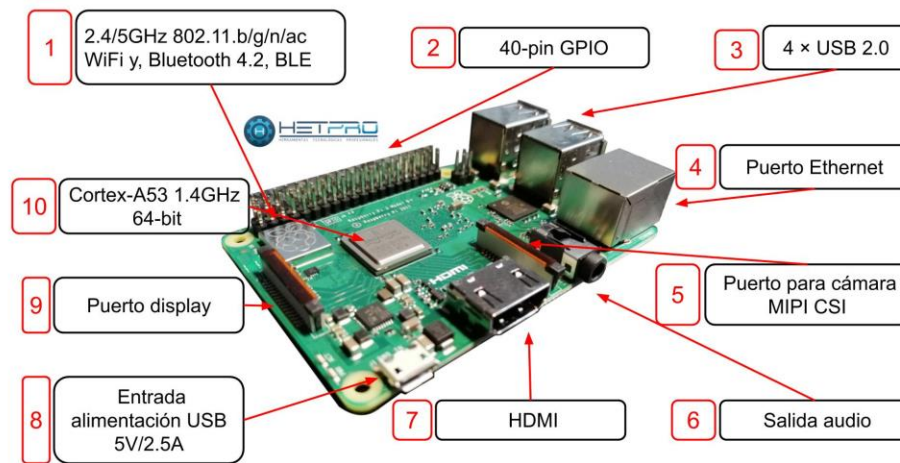


Figura 27: Raspberry Pi Especificaciones.

ESPECIFICACIONES TECNICAS:

- CPU Quad Core 1.2GHz Broadcom BCM2837 de 64 bits
- 1 GB de RAM
- BCM43438 Wireless LAN y Bluetooth Low Energy (BLE) a bordo
- GPIO extendido de 40 pines
- 4 puertos USB 2
- Salida estéreo de 4 polos y puerto de vídeo compuesto
- HDMI de tamaño completo
- Puerto de cámara CSI para conectar una cámara Raspberry Pi
- Puerto de pantalla DSI para conectar una pantalla táctil Raspberry Pi
- Puerto Micro SD para cargar su sistema operativo y almacenar datos
- Fuente de alimentación Micro USB conmutada mejorada hasta 2.5^a

Raspbian Buster Sistemas Operativo:

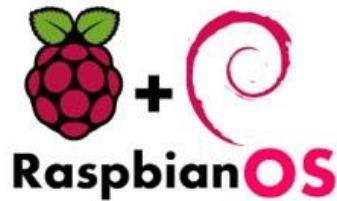


Figura 28: RaspbianOS.

Como siempre el nombre se corresponde con un personaje de las películas de Toy Story y en este caso le ha tocado al perro de Andy: Buster.¹⁹

Desde su lanzamiento ya ha habido varias revisiones para incluir correcciones y funcionalidades. En la web oficial si entráis en las descargas, en la parte solo para Raspbian, podéis encontrar un enlace a las notas de publicación: Raspbian Release notes.

Esta versión de Raspbian internamente es más compleja que las anteriores. Además de soportar el arranque con la partición /boot/ de todos los modelos anteriores, tiene que incluir el arranque especial para Raspberry Pi 4 con soporte de la EEPROM (una especie de BIOS muy básica, aunque hay placas como las La Frite que tienen mucho mejor todo esto y ya hablaremos de ellas). Esta EEPROM es también una de las nuevas fuentes de problemas de arranque de la Raspberry Pi 4.

La primera versión (2019-06-20) tenía bastantes fallos y a los 20 días (2019-07-10) ya había una actualización general en la que resolvían los peores errores. Luego en septiembre (2019-09-26) si sacaron una actualización completa que resolvía más problemas y añadía muchas funcionalidades sobre todo relacionadas con la salida para dos pantallas de la Raspberry Pi 4.

```
pi@raspberrypi:~ $ lsb_release -a
No LSB modules are available.
Distributor ID: Raspbian
Description:   Raspbian GNU/Linux 10 (buster)
Release:       10
Codename:      buster
```

Figura 29: Versión Raspberry.

3.2.4. Configuración

Configuración de red de Raspberry Pi:²⁰

Para convertir el Pi en un punto de acceso Wi-Fi, utilizaremos tanto la interfaz de red cableada como la interfaz de red inalámbrica integrada. En un Raspberry Pi 3 Modelo B con Raspbian Stretch, estos se nombrarán de la siguiente manera:

- eth0 para la interfaz de red cableada.
- wlan0 para la interfaz de red inalámbrica.

¹⁹ <https://www.raspberrypi.org/downloads/raspbian/>

²⁰ <https://www.dinofizzotti.com/blog/2019-01-09-running-a-man-in-the-middle-proxy-on-a-raspberry-pi-3/>

Configurar dhcpcd:

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Modificará la configuración del cliente DHCP existente de Pi para asignar una dirección IP estática a la interfaz `wlan0`, ya que esta interfaz de red representará la dirección del punto de acceso para todos los demás dispositivos que se conectarán a la red Wi-Fi personalizada.

El software del servidor DHCP es responsable de distribuir las direcciones de red a los clientes que desean unirse a la red.

Debemos instalar el software DHCP en la Pi.

Para modificar la `dhcpcd.conf` configuración actual del cliente DHCP () de Pi, lo abrimos `/etc/dhcpcd.conf` como root:

```
$ sudo nano /etc/dhcpcd.conf
```

Agregue las siguientes líneas al final del archivo:

```
interface wlan0
static ip_address=192.168.42.1/24
nohook wpa_supplicant
```

Figura 30: Archivo dhcpcd.conf

Esto le indica al cliente DHCP que use una dirección IP estática para la interfaz de red inalámbrica, así como también evita que el enlace de suplicante WPA se inicie en esta interfaz.

Instalar isc-dhcp-server y hostapd:

Para instalar este software, abra una terminal en el Pi y escribimos el siguiente comando:

```
$ sudo apt install hostapd isc-dhcp-server
```

Configurar isc-dhcp-server:

Abrimos el archivo: `/etc/dhcp/dhcpd.conf`

```
$ sudo nano /etc/dhcp/dhcpd.conf
```

Eliminamos el comentario en la línea que dice `authoritative` y añadimos:

```

subnet 192.168.42.0 netmask 255.255.255.0 {
    range 192.168.42.10 192.168.42.250;
    option broadcast-address 192.168.42.255;
    option routers 192.168.42.1;
    option domain-name "local";
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}

```

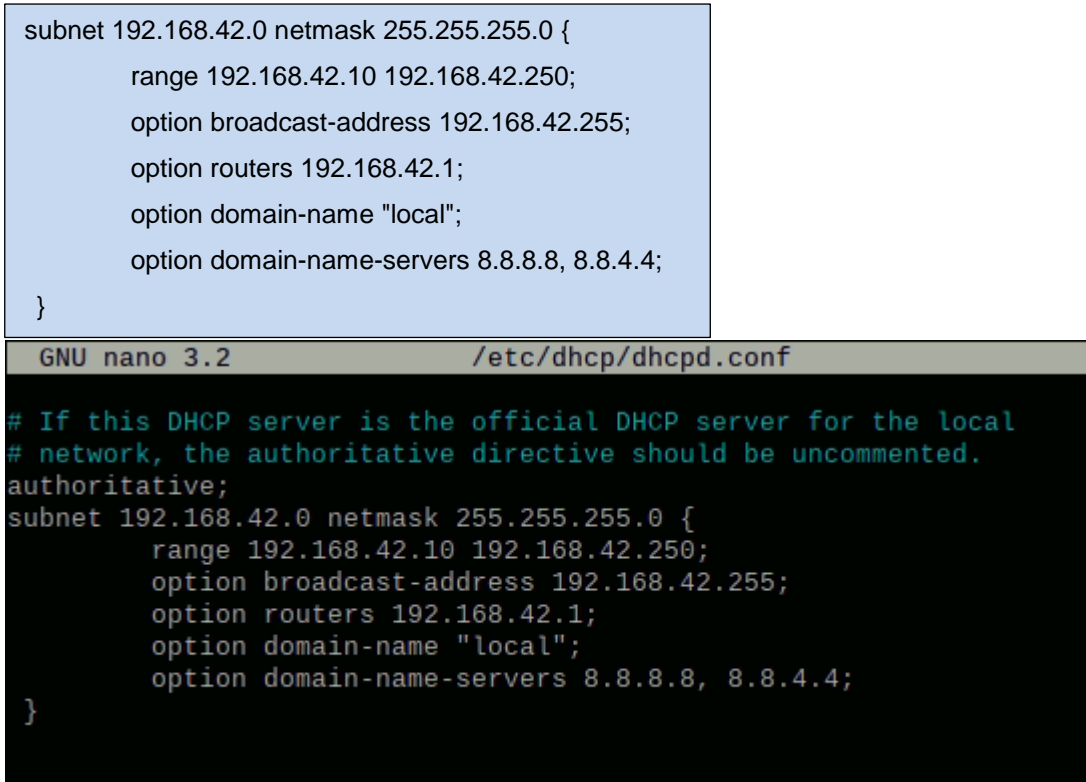


Figura 31: Archivo dhcpd.conf

Estas líneas configuran el servidor DHCP que funciona en la interfaz inalámbrica para distribuir direcciones IP desde, 192.168.42.10 hasta 192.168.42.250, con una dirección de transmisión de 192.168.42.255, así como especificar la dirección del enrutador 192.168.42.1.

A continuación, abrimos el `/etc/default/isc-dhcp-server`:

```
$ sudo nano /etc/default/isc-dhcp-server
```

Cambiamos la línea "INTERFACESv4" para contener wlan0 y comentar la "INTERFACESv6":

```

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="wlan0"
#INTERFACESv6=""

```

Figura 32: Archivo isc-dhcp-server.

Configurar la entrada systemd de isc-dhcp-server:

Después de la instalación `isc-dhcp-server`, se ejecutará automáticamente después del arranque; sin embargo, si intenta iniciarse antes de que la interfaz de red esté lista, fallará y no intentará comenzar de nuevo. Para resolver el problema hicimos lo siguiente:

1. `sudo cp /run/systemd/generator.late/isc-dhcp-server.service /etc/systemd/system`
2. `sudo nano /etc/systemd/system/isc-dhcp-server.service`
3. Edite la [Service]sección:

- set Restart=on-failure,
 - Agregar RestartSec=5 para indicarle al systemd que espere 5 segundos antes de reiniciar el servicio.
4. Agregue en la sección [Install] la siguiente línea:
 - WantedBy=multi-user.target
 5. sudo systemctl daemon-reload
 6. sudo systemctl disable isc-dhcp-server
 7. sudo systemctl enable isc-dhcp-server

Esto indica systemd que reinicie automáticamente el servidor ISC DHCPv4 si falla, pero que espere 5 segundos antes de intentar reiniciarlo.

Configurar hostapd:

Editamos el archivo hostapd de configuración, pero primero debemos copiar y extraer un archivo de configuración de ejemplo dentro del cual haremos nuestros cambios:

```
$ cd /etc/hostapd/
$ sudo cp /usr/share/doc/hostapd/examples/hostapd.conf .
```

```
$ sudo nano /etc/hostapd/hostapd.conf
```

Debemos encontrar las líneas en el archivo que establecen las variables de configuración a continuación. En algunos casos, deberá modificar el valor y en otros debemos descomentar y modificar el valor:

```
interface=wlan0
driver=nl80211
ssid=RaspberryMIM
macaddr_acl=0
auth_algs=1
wmm_enabled=0
wpa=2
wpa_passphrase=Abcd1234567890
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Figura 33: Archivo hostapd.

A continuación, debe abrir el archivo /etc/default/hostapd:

```
$ sudo nano /etc/default/hostapd
```

Y descomentar la línea que especifica DAEMON_CONF y edítela de modo que se lea así:

```

Defaults for hostapd initscript
#
# WARNING: The DAEMON_CONF setting has been deprecated and will be removed
#         in future package releases.
#
# See /usr/share/doc/hostapd/README.Debian for information about alternative
# methods of managing hostapd.
#
# Uncomment and set DAEMON_CONF to the absolute path of a hostapd configuration
# file and hostapd will be started during system boot. An example configuration
# file can be found at /usr/share/doc/hostapd/examples/hostapd.conf.gz
#
DAEMON_CONF="/etc/hostapd/hostapd.conf"

```

Figura 34: Archivo hostapd.conf

Ejecutamos los siguientes comandos para asegurarse de que el servicio esté desenmascarado y habilitado:

```

$ sudo systemctl unmask hostapd.service
$ sudo systemctl enable hostapd.service

```

Instalación y configuración de MitmProxy:

Instalamos la última versión de MitmProxy.

```

$ sudo pip3 install mitmproxy

```

Una vez que esto se haya completado, debería poder verificar que MitmProxy esté instalado correctamente con el siguiente comando:

```

Archivo  Editar  Pestañas  Ayuda
pi@raspberrypi:~ $ mitmproxy --version
Mitmproxy: 5.0.1
Python:    3.7.3
OpenSSL:   OpenSSL 1.1.1d  10 Sep 2019
Platform:  Linux-4.19.97-v7+-armv7l-with-debian-10.3

```

Figura 35: Versión MitmProxy.

Configure MitmProxy para que se ejecute al inicio:

Para iniciar, mitmweb abrimos un editor de texto y guardamos los siguientes contenidos en un archivo en la ubicación /home/pi/start_mitmweb.sh:

```

GNU nano 3.2 start_mitmweb.sh
#!/bin/bash
mitmweb --mode transparent --web-port 9090 --web-iface 0.0.0.0 &>> /var/log/mitmweb.log

```

Figura 36: Archivo start_mitmweb.sh

Explicación de los argumentos de la línea de comando:

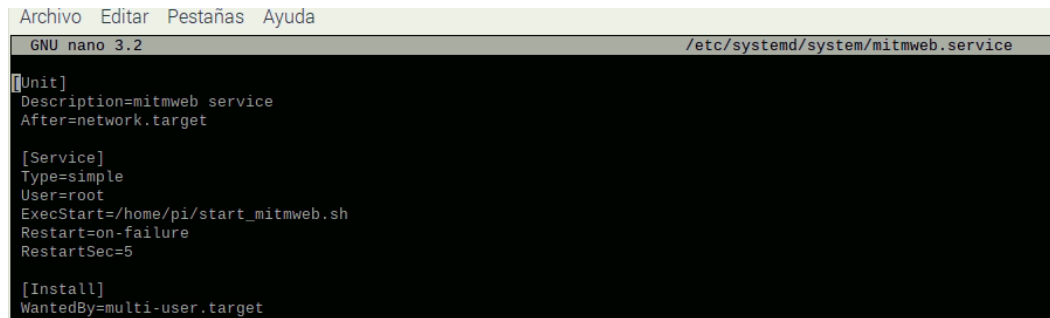
- Mode transparent: ejecuta MitmProxy en modo proxy transparente, que reenvía las solicitudes y respuestas a sus destinos previstos después de ser inspeccionadas.
- web-port 9090: esto le dice a la aplicación mitmweb en qué puerto exponer la interfaz web.
- web-iface 0.0.0.0: esto le dice a la aplicación mitmweb que la interfaz web debe ser visible y accesible en la dirección IP LAN de Pi.

Tendremos que hacer que este script sea ejecutable ejecutando `$ chmod a+x /home/pi/start_mitmweb.sh`.

A continuación, necesitamos crear un archivo de servicio systemd.

```
$ sudo nano /etc/systemd/system/mitmweb.service
```

Y con el siguiente contenido:



```

Archivo Editar Pestañas Ayuda
GNU nano 3.2 /etc/systemd/system/mitmweb.service
[[Unit]]
Description=mitmweb service
After=network.target

[Service]
Type=simple
User=root
ExecStart=/home/pi/start_mitmweb.sh
Restart=on-failure
RestartSec=5

[Install]
WantedBy=multi-user.target

```

Figura 37: Archivo mitmweb.service

Habilitamos el servicio para que se ejecute automáticamente al inicio ejecutando los siguientes comandos:

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable mitmweb.service
```

Configuración del tráfico de red:

Modificar las reglas de iptables.

Para interceptar y reenviar correctamente el tráfico entre la interfaz inalámbrica y la interfaz con cable, deberá emitir los siguientes comandos para configurar las reglas de firewall "iptables":

A continuación, guardamos la configuración de iptables en un archivo:

```
$ sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT
$ sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT
$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
$ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
$ sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8080
```

Ahora modificaremos una secuencia de comandos para emitir un comando para restaurará las reglas al inicio. Abra el archivo "rc.local":

```
$ sudo nano /etc/rc.local
```

Ingresa la siguiente declaración antes de la línea de "salida 0" al final del archivo:

```
iptables-restore < /etc/iptables.up.rules
```

Habilitar el reenvío de tráfico:

Por defecto, el sistema operativo no permitirá que el tráfico IP se reenvíe de una red a otra. Para cambiar este comportamiento, ejecute el siguiente comando:

```
$ sudo sysctl -w net.ipv4.ip_forward=1
```

Y luego, para garantizar que esta configuración persista entre los ciclos de arranque, abra el archivo /etc/sysctl.conf:

```
$ sudo nano /etc/sysctl.conf
```

Encontrar la línea comentada que dice "# net.ipv4.ip_forward = 1" y descomentarla:

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Reiniciar, la próxima vez que se inicie, aparecerá un punto de acceso inalámbrico y ejecutará el proxy MITM transparente.

3.2.5. Ejecución

Abrimos una pestaña del navegador en su computadora portátil y vaya a

<http://http://192.168.1.116: 9090/>

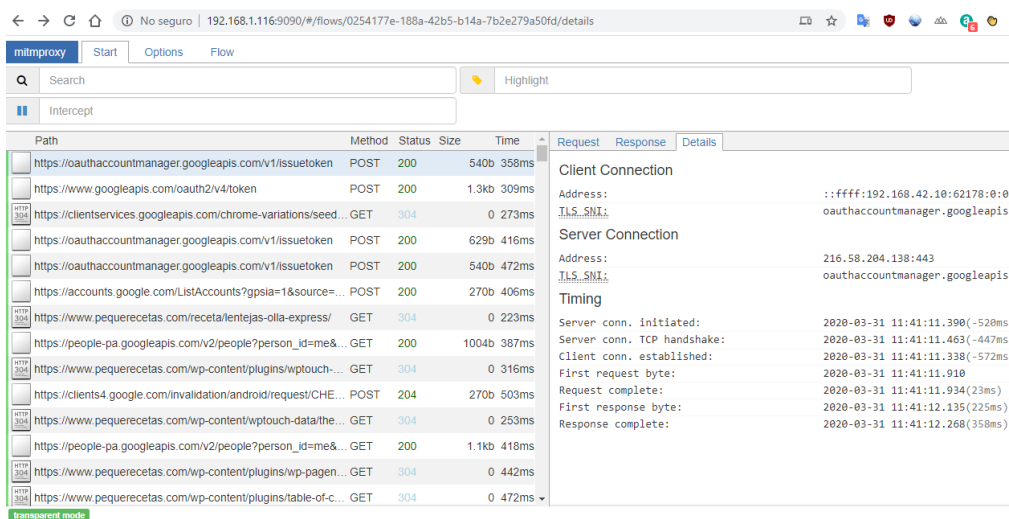


Figura 38: Interface Gráfica MitmProxy.

Esperamos unos segundos y luego use su teléfono para buscar un nuevo punto de acceso Wi-Fi.

Debería ver uno llamado "RaspberryMIM".

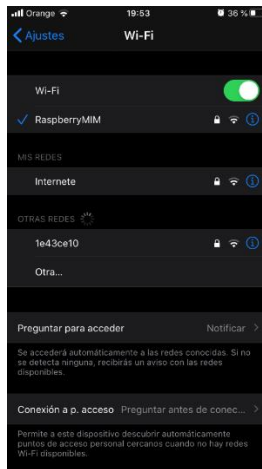


Figura 39: WiFi emitida Raspberry.

Nos conectamos al punto de acceso " RaspberryMIM " y use la contraseña "Abcd12345678" para unirse a la red.

Una vez conectado, abra un navegador web y navegue a <http://www.example.com> (asegúrese de que sea http y no https).

Observamos el tráfico en la aplicación mitmweb que se ejecuta en la pestaña del navegador de la computadora portátil.

Si intenta ver el sitio web de un http, puede recibir una advertencia en su navegador.

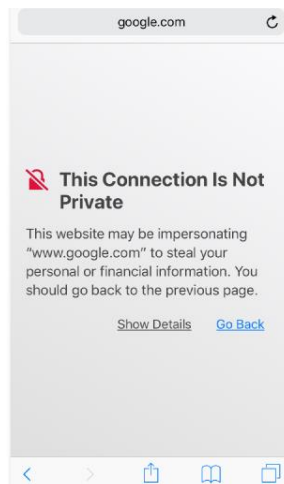


Figura 40: Navegación sin certificado.

Mientras estamos conectado al punto de acceso " RaspberryMIM ", navegue en el navegador de su teléfono a <http://mitm.it>

Observará un sitio web que le dará la opción de enlaces que descargarán el certificado raíz para la plataforma correspondiente.



Figura 41: Instalación tipo de certificado por SO.

Toque el icono de la plataforma que estamos utilizando actualmente, se descargará un certificado que debe instalarse en la tienda de confianza de su dispositivo, cuyas instrucciones varían de una plataforma a otra. Vea a continuación algunas capturas de pantalla de la experiencia iOS.

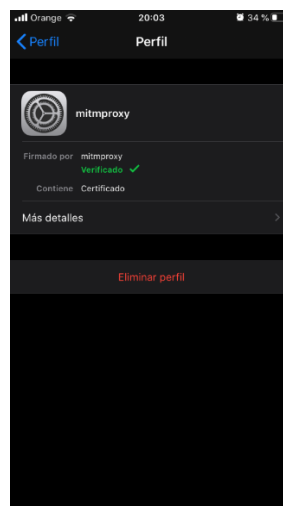


Figura 42: Certificado Instalado en IOS.

Nota para iOS: después de instalar el certificado, deberá activarlo manualmente yendo a Configuración -> Acerca de -> Configuración de confianza de certificado y activando el certificado para "RaspberryMIM".

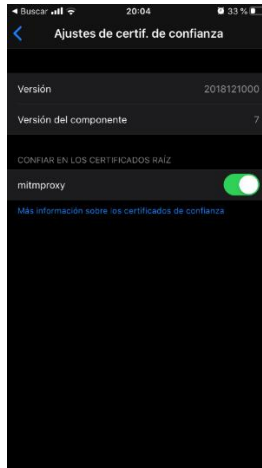


Figura 43: Certificado.

Una vez que haya instalado y confiado en el certificado, debería poder visitar los sitios web de http y https y ver las solicitudes y respuestas sin ninguna advertencia en su dispositivo.



Figura 44: Web con certificado instalado.

El tráfico en tiempo real y posterior análisis lo sacaremos de la interfaz web del MitmProxy.

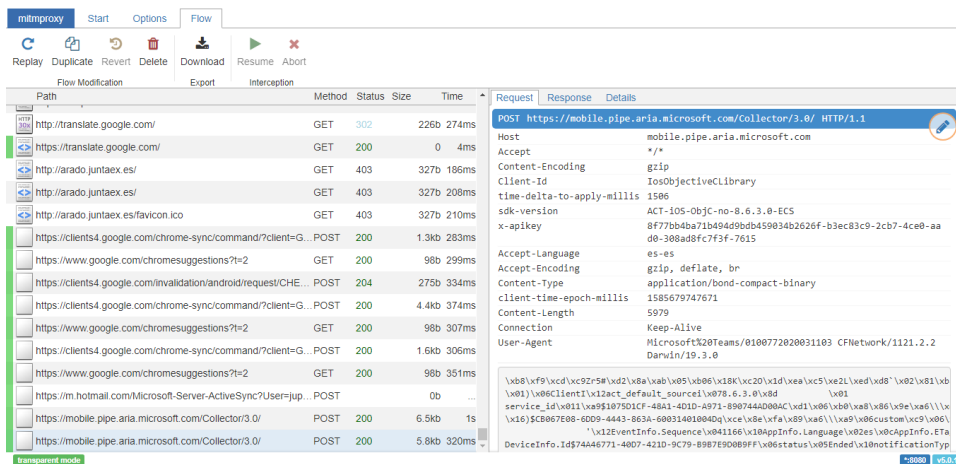


Figura 45: Captura de paquetes MitmProxy.

3.3. Implementar IDS para análisis de datos.

3.3.1. Instalación Suricata.

Se procede a la instalación del motor de análisis de tráfico de red, Suricata. Para esto, los sistemas Linux basados en Debían tienen un paquete en sus repositorios, por lo que es tan sencillo como ejecutar:²¹

```
sudo apt install suricata
```

```
root@raspberrypi:/home/pi# sudo apt install suricata
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
suricata ya está en su versión más reciente (1:4.1.2-2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
```

Figura 46: Instalación de Suricata IDS en Raspbian.

Podemos comprobar que tenemos el servicio corriendo, y por tanto todo ha ido bien, mediante el comando:

```
systemctl status suricata
```

```
root@raspberrypi:/home/pi# systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-04-23 10:43:29 CEST; 4 days ago
     Docs: man:suricata(8)
           man:suricataase(8)
           https://suricata-ids.org/docs/
   Process: 421 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid (code=exited, status=0/SUCCESS)
  Main PID: 643 (Suricata-Main)
    Tasks: 10 (limit: 2191)
   Memory: 322.7M
   CGroup: /system.slice/suricata.service
           └─643 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
```

Figura 47: Comprobación del estado del servicio Suricata.

Ahora deberemos realizar un par de configuraciones para que todo funcione correctamente. De forma predeterminada, Suricata utiliza el modo de trabajo AF-PACKET (lectura de sockets en raw) sobre la interfaz eth0. Tendremos que configurar la interfaz donde vamos a inspeccionar el tráfico.

3.3.2. Configuración

Dentro del fichero de configuración localizado en /etc/suricata/suricata.yaml, debemos buscar el apartado de configuración del modo af-packet y cambiar la interfaz de la siguiente forma:

²¹ <https://fwhibbit.es/suricata-ids-instalacion-puesta-en-marcha-y-primera-prueba>

```
# Linux high speed capture support
af-packet:
- interface: wlan0
  # Number of receive threads. "auto" uses the number of cores
  #threads: auto
  # Default clusterid. AF_PACKET will load balance packets based on flow.
  cluster-id: 99
```

Figura 48: Edición de suricata.yaml para establecer la interfaz de escucha.

Ya tenemos nuestro servicio configurado y corriendo, pero esto de poco nos va a servir si no sabes qué es lo que tiene que buscar, el set de reglas que trae por defecto es muy pobre. Para completar estas reglas vamos a utilizar las reglas de emergingthreats. Estas son actualizadas casi a diario así que hay que mantenerlas lo más actualizadas posibles. Para ello, hemos realizado un pequeño script en mi repositorio, que ejecutándolo mediante una tarea programada mantendrá estas reglas actualizadas. El primer paso es descargar el script y ejecutarlo por primera vez.

```
root@raspberrypi:/etc/suricata# wget https://raw.githubusercontent.com/jupinjin/suricata/master/rulesupdate.py
--2020-04-27 19:41:00-- https://raw.githubusercontent.com/jupinjin/suricata/master/rulesupdate.py
Resolviendo raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.132.133
Conectando con raw.githubusercontent.com (raw.githubusercontent.com)[151.101.132.133]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 1024 (1,0K) [text/plain]
Grabando a: "rulesupdate.py"

rulesupdate.py          100%[=====>]  1,00K  --.-KB/s  en 0s
2020-04-27 19:41:01 (5,97 MB/s) - "rulesupdate.py" guardado [1024/1024]
root@raspberrypi:/etc/suricata# python /etc/suricata/rulesupdate.py
```

Figura 49: Descarga de repositorio de script para actualizar reglas.

3.3.3. Ejecución

Una vez ejecutado dispondremos de todas las reglas de emerginthreats en el directorio "/etc/suricata/rules/" para que estas se mantengan actualizadas se recarguen todas las noches vamos a añadir dos tareas a nuestro crontab.

```
crontab -e
```

```
0 2 * * * python /etc/suricata/rulesupdate.py
15 2 * * * suricatasc -c reload-rules
```

Figura 50: Tarea programada.

Por ultimo comprobamos las tareas programadas de nuestro sistema.

```
crontab -l
```

3.4. Instalación de Filebeat en Raspberry

Esta es la última pieza en nuestra sonda, a diferencia del resto, esta pieza no tiene disponibilidad en repositorios para plataformas ARM. Por tanto, se deberá de descargar e instalar esta utilidad manualmente.²²²³

3.4.1. Prerrequisitos

Instalar Go

También llamado golang, es un lenguaje de programación de código abierto desarrollado por un equipo (Robert Griesemer, Rob Pike y Ken Thompson) en Google y muchos colaboradores de la comunidad de código abierto.

Go es expresivo, simple, confiable, conciso, limpio y eficiente, lo que hace que los programadores escriban/desarrollen aplicaciones de manera fácil y más productiva, que en máquinas multicore y en red. El lenguaje Go fue diseñado para resolver críticas comunes de otros lenguajes, manteniendo sus características positivas.

```
sudo apt update
sudo apt install -t buster golang
```

Instalar Python

En Raspbian ya viene preinstalado la versión 2.7.16, además nosotros cuando hemos instalado el proxy también hemos instalados una versión superior.

```
root@raspberrypi:/home/pi# python --version
Python 2.7.16
```

Figura 51: Versión Python.

Ampliación de memoria Swapfile

Para poder compilar con Go necesitamos ampliar la memoria swapfile a 1024MB de nuestra Raspberry, la memoria que trae por defecto es de 100MB, para poder hacer esa ampliación hacemos lo siguiente.

```
sudo dphys-swapfile swapoff
CONF_SWAPSIZE=1024
sudo dphys-swapfile swapon
```

```
Tasks: 144 total,
%Cpu(s): 1,2 us,
MiB Mem : 922,1
MiB Swap: 1024,0
```

Figura 52: Swap.

²² <https://gist.github.com/andig/650915e02b18cfe38de6516686977bca>

²³ <https://github.com/josh-thurston/easyBEATS>

3.4.2. Instalación de Filebeat

Establecemos la raíz para el administrador de paquetes Go.

```
export GOPATH=~/.go
```

Obtenemos los fuentes de la pagina github.com.

```
cd ~/.go/src/github.com/elastic/beats/filebeat/
```

Seleccionamos la versión

```
git checkout 6.8
```

Ahora construimos el binario con el administrador de paquetes Go.

```
GOPATH=~/.go make
```

3.4.3. Configuración

Esto genera el ejecutable Filebeat, una vez que tenemos ya el ejecutable ya podemos lanzar el mismo, no sin antes configurar el archivo filebeat.yml. Nosotros en el solo hemos configurado el tipo de evento que se va a monitorizar y el lugar donde está ubicado dentro de la máquina. Después tenemos que indicarle la conexión con la base de datos Elastic para ellos tenemos una sección específica de cloud, en el cual le vamos a indicar el cloud.id y el cloud.auth que posteriormente vamos a configurar en la sección de Elastic Cloud.

```
filebeat.inputs:
# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.
- type: log

# Change to true to enable this input configuration.
enabled: true

# Paths that should be crawled and fetched. Glob based paths.
paths:
- /var/log/eve.json
#- c:\programdata\elasticsearch\logs\*
```

Figura 53: Filebeat.yml.

```

#===== Elastic Cloud =====
# These settings simplify using filebeat with the Elastic Cloud (https://cloud.elastic.co/).
# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
cloud.id: "TFM:dXMTZWfZdC0xLmF3cy5mb3VuZC5pbyQ2MTRkN2I4NzIxZDY0NTBkYmUzMjF1YmEzODAzMTUxYSRjYjRiNGMzMGVhM2Y0MDh1YjM5NmY5MmMxNGI1OTNiYg=="
# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `:<pass>`.
cloud.auth: "elastic:VqDob4HxwhpSU4UbWu1BRbhf"

```

Figura 54: Sección Elastic Cloud archivo filebeat.yml.

3.4.4. Ejecución

Para ejecutarlo lanzamos. `/Filebeat -v -e`.

Con `-v` podemos ver en consola los errores en lugar de syslog.

```

2020-04-28T13:28:58.531+0200 INFO instance/beat.go:280 Setup Beat: filebeat; Version: 6.8.9
2020-04-28T13:28:58.544+0200 INFO elasticsearch/client.go:164 Elasticsearch url: https://614d7b8721d6450dbe321eba3807151a.us-east-1.aws.found.io:443
2020-04-28T13:28:58.560+0200 INFO [publisher] pipeline/module.go:110 Beat name: raspberrypi
2020-04-28T13:28:58.566+0200 INFO instance/beat.go:492 filebeat start running.
2020-04-28T13:28:58.567+0200 INFO registrar/registrar.go:134 Loading registrar data from /root/go/src/github.com/elastic/beats/filebeat/data/regis
ry
2020-04-28T13:28:58.576+0200 INFO [monitoring] log/log.go:117 Starting metrics logging every 30s
2020-04-28T13:28:58.593+0200 INFO registrar/registrar.go:141 States Loaded from registrar: 24
2020-04-28T13:28:58.596+0200 INFO crawler/crawler.go:72 Loading Inputs: 1
2020-04-28T13:28:58.603+0200 INFO log/input.go:148 Configured paths: [/var/log/eve.json]
2020-04-28T13:28:58.603+0200 INFO input/input.go:114 Starting input of type: log; ID: 1911162521133576251
2020-04-28T13:28:58.604+0200 INFO crawler/crawler.go:106 Loading and starting Inputs completed. Enabled inputs: 1
2020-04-28T13:28:58.605+0200 INFO cfgfile/reload.go:150 Config reloader started
2020-04-28T13:28:58.606+0200 INFO cfgfile/reload.go:205 Loading of config files completed.
2020-04-28T13:28:58.613+0200 INFO log/harvester.go:255 Harvester started for file: /var/log/eve.json
2020-04-28T13:29:01.538+0200 INFO add_cloud_metadata/add_cloud_metadata.go:340 add_cloud_metadata: hosting provider type not detected.
2020-04-28T13:29:01.906+0200 INFO pipeline/output.go:95 Connecting to backoff(elasticsearch(https://614d7b8721d6450dbe321eba3807151a.us-east-1.aws.fou
nd.io:443))
2020-04-28T13:29:03.121+0200 INFO elasticsearch/client.go:739 Attempting to connect to Elasticsearch version 7.6.2
2020-04-28T13:29:03.349+0200 INFO template/load.go:128 Template already exists and will not be overwritten.
2020-04-28T13:29:03.352+0200 INFO instance/beat.go:889 Template successfully loaded.
2020-04-28T13:29:03.354+0200 INFO pipeline/output.go:105 Connection to backoff(elasticsearch(https://614d7b8721d6450dbe321eba3807151a.us-east-1.aws.fou
nd.io:443)) established

```

Figura 55: Ejecución Filebeat.

3.5. Elastic Cloud

3.5.1. Registro

Comenzar a analizar y visualizar datos no podría ser más fácil que con la plataforma SaaS, Elastic Cloud. Con unos pocos clics, podemos activar Elasticsearch y Kibana, y escalar para satisfacer sus necesidades de datos.

Lo primero que tenemos que hacer es registrarnos en la página de Elastic.

<https://cloud.elastic.co>

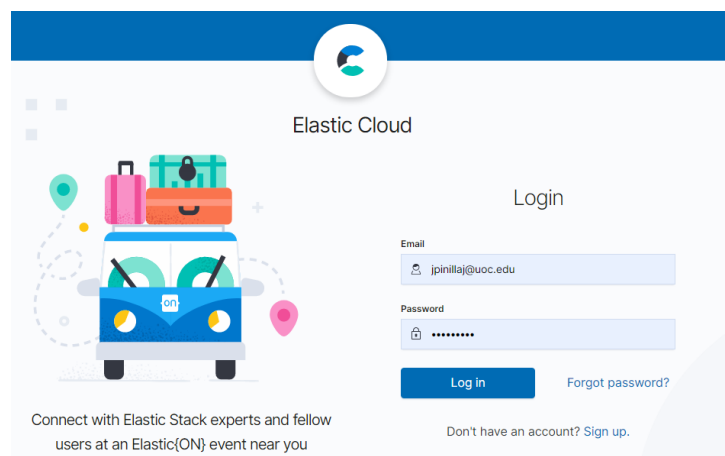


Figura 56: Acceso a Elastic Cloud.

Una vez registrado disponemos de 14 días para probar la aplicación y después pasado estos días tendremos que contratar el plan que mejor nos convenga, en nuestro caso con el plan estándar tendría un coste de 16\$/mes.

3.5.2. Instalación

Lo primero que nos pide es el nombre del despliegue, la plataforma donde lo queremos alojar en la nube, el país y las demás opciones por defecto, creamos el despliegue.

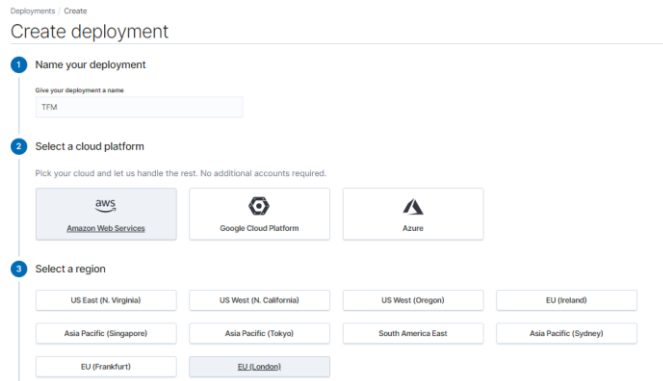


Figura 57: Instalación Elastic cloud.

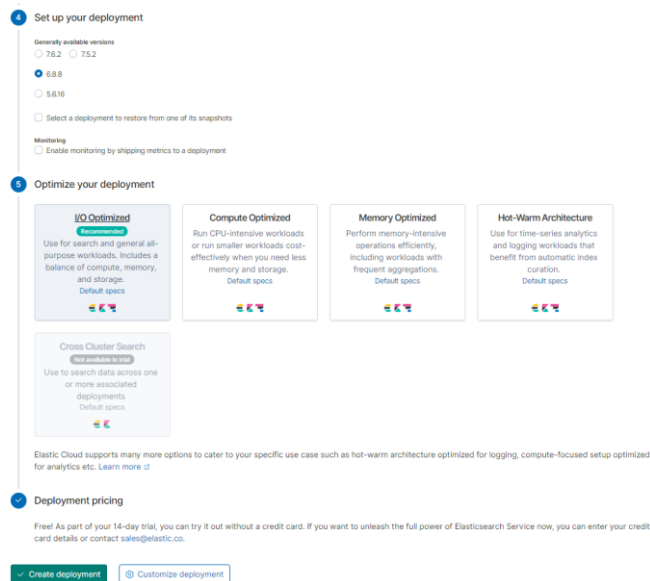


Figura 58: Instalación Elastic cloud.

Un dato a tener en cuenta elegiremos la misma versión que el Filebeat instalado en la Raspberry Pi para no tener problemas.

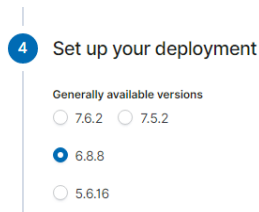


Figura 59: Versiones disponibles ElasticSearch.

Le damos a crear y en tan solo unos minutos ya tendremos nuestra infraestructura.

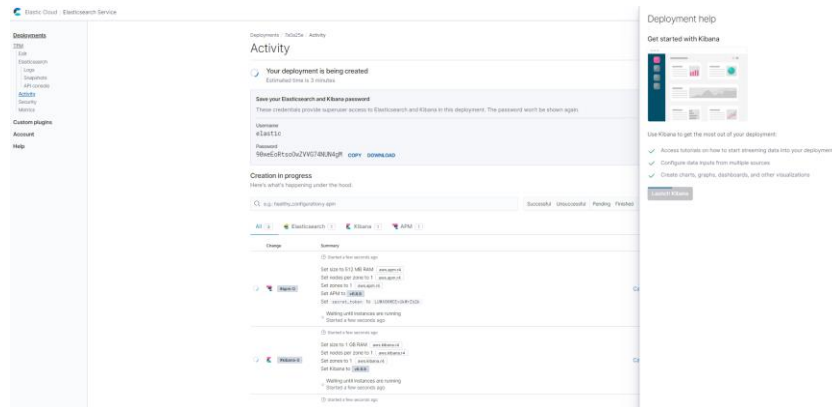


Figura 60: Despliegue Cloud disponible.

Ya tengo mi despliegue disponible:

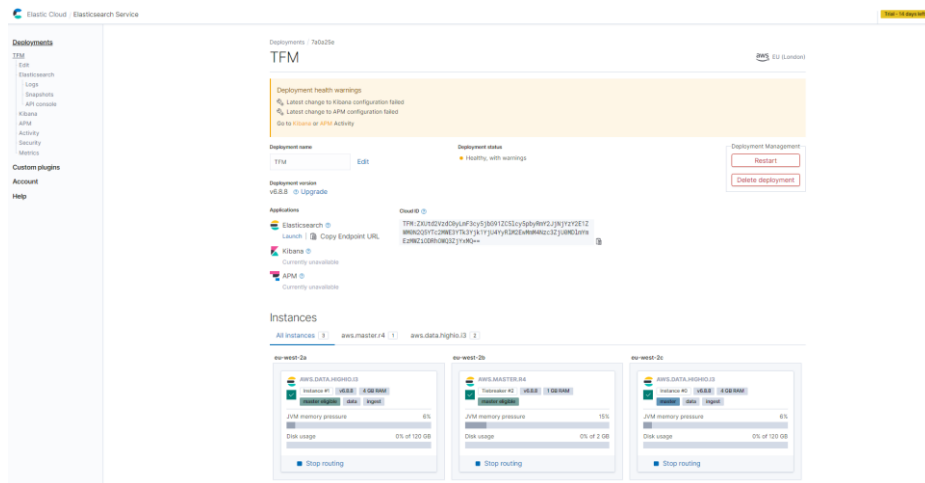


Figura 61: Despliegue Cloud disponible.

Nuestro Cloud id ya está disponible para poder enviar los datos, esa configuración la tenemos que poner en el fichero de configuración de Filebeat

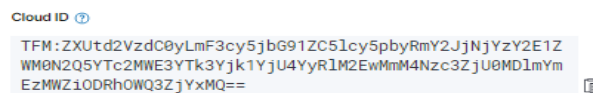


Figura 62: Cloud ID.

3.5.3. Configuración de Kibana.

Lo primero que tenemos que definir es un index patterns, Se deben configurar en Kibana los índices de clasificación de datos establecidos con anterioridad para que Kibana sea capaz de

realizar búsquedas con dichos datos. La configuración de los índices se realiza en Management > Kibana > Index Patterns.

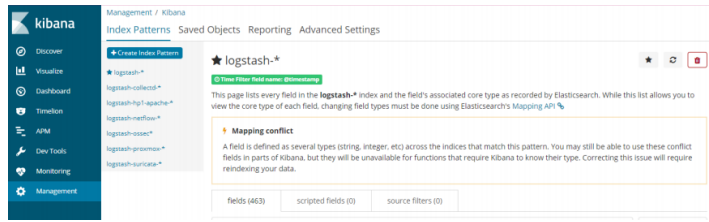


Figura 63: Creación Index Patterns.

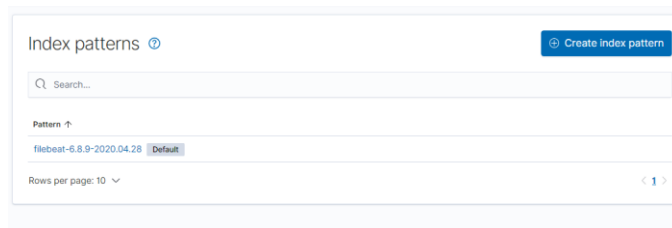


Figura 64: Creación Index Patterns.

Una vez configurados los índices, en la sección Discover, Kibana muestra todos los datos pertenecientes a los índices configurados que está recogiendo ElasticSearch, y veremos todo el tráfico que generamos con el teléfono móvil, se envían todos los logs del Suricata.



Figura 65: Pantalla de Discover.

Ya detectamos que hay tráfico que nos puede resultar peligroso con lo cual el siguiente paso a seguir es el análisis de esos datos.

```
> Apr 28, 2020 @ 20:50:54.950 @timestamp: Apr 28, 2020 @ 20:50:54.950 message: {"timestamp": "2020-04-28T20:50:54.865246+0200", "flow_id": "626375800027991", "in_iface": "wlan0", "event_type": "alert", "src_ip": "31.3.245.133", "src_port": 80, "dest_ip": "192.168.42.10", "dest_port": 56347, "proto": "TCP", "alert": {"action": "allowed", "gid": 1, "signature_id": 2100498, "rev": 7, "signature": "GPL ATTACK_RESPONSE id check returned root", "category": "Potentially Bad Traffic", "severity": 2, "metadata": {"updated_at": ["2010_09_23"], "created_at":
```

Figura 66: Mensaje Kibana.

3.6. Análisis de datos

En la parte anterior se ha analizado lo que son los sistemas IDS y cómo se pueden utilizar para capturar todo tipo de información del tráfico de red. Pero estos datos capturados se almacenan en ficheros tipo Log/json difíciles de leer y analizar incluso para el personal técnico. Es necesario un sistema que permita transformar estos datos en información útil.

Para un análisis más exhaustivo la información necesitamos filtrar esos datos para que tengan sentido, para ellos vamos a realizar filtros de Logstash.

3.6.1. Filtro Logstash

Mediante el sistema de transferencia de ficheros un fichero eve.json se recogerá de la Sonda IDS hasta el equipo donde se está ejecutando un proceso de Logstash.

Este proceso para poder cargar el fichero, debe estar configurado con un fichero, en este caso llamado eve.conf, que le indicará cómo hacerlo.

El fichero de configuración de Logstash, está organizado en tres bloques.²⁴

- Input: Para definir la entrada de los datos.
- Filter: En este bloque se puede tratar los datos para filtrarlos o realizar mapeos.
- Output: Define la salida o envío de datos tratados.

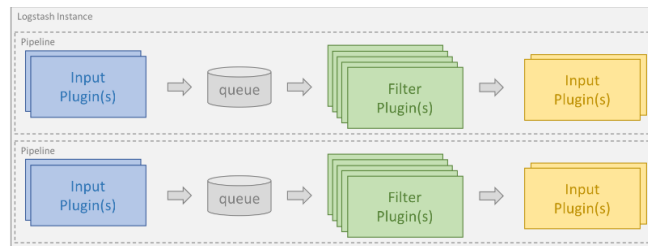


Figura 67: Estructura Logstash

Los Ficheros de configuración utilizados para la carga de datos eve.json es el siguiente:

Filtro translate:

```
filter {
  translate {
    field => "[src_ip]"
    destination => "[aaDispositivo]"
    dictionary => {
      "192.168.42.10" => "Iphone"
      "192.168.42.11" => "Sony"
      "192.168.42.12" => "Xiaomi"
    }
    fallback => "Otros"
  }
}
```

²⁴ <https://www.elastic.co/es/blog/a-practical-introduction-to-logstash>

Este primer filtro traduce las direcciones ip de nuestro dispositivos en nombres, para poder hacer una análisis más exhaustivo de los datos. En Kibana se mostraría así:

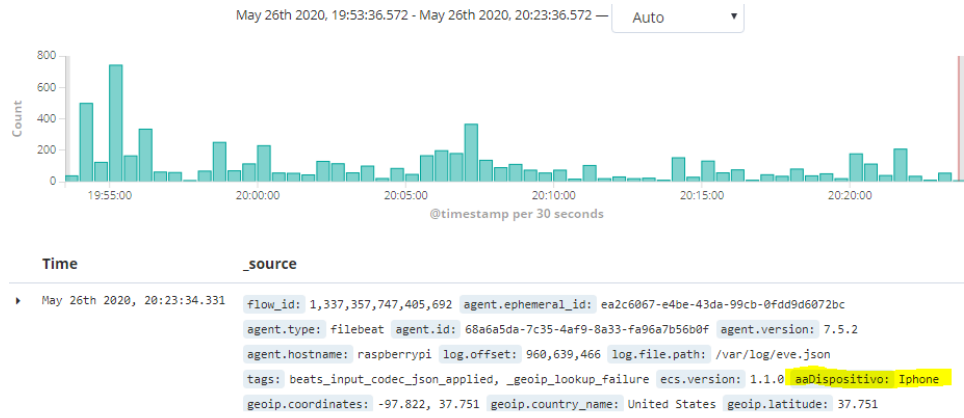


Figura 68: Datos Kibana después de filtro.

Filtro Suricata:

```

filter {
  if [application] == "suricata" {
    date {
      match => [ "timestamp", "ISO8601" ]
    }
    ruby {
      code => "if event['event_type'] == 'fileinfo'; event['fileinfo']['type']=event['fileinfo']['magic'].to_s.split('.')[0];
end;"
    }
  }

  if [src_ip] {
    geoip {
      source => "src_ip"
      target => "geoip"
      add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
      add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
    }
    mutate {
      convert => [ "[geoip][coordinates]", "float" ]
    }
    if ![geoip.ip] {
      if [dest_ip] {
        geoip {
          source => "dest_ip"
          target => "geoip"
          add_field => [ "[geoip][coordinates]", "%{[geoip][longitude]}" ]
          add_field => [ "[geoip][coordinates]", "%{[geoip][latitude]}" ]
        }
        mutate {
          convert => [ "[geoip][coordinates]", "float" ]
        }
      }
    }
  }
}

```

En el fichero de configuración podemos destacar lo siguiente:

Filter: De momento se han utilizado dos plugin:

- Geoip: Para asignar Geolocalización a las direcciones IPs.
- Translate: Para realizar un mapeo mediante diccionario entre IPs de dispositivos de la red local y su nombre.
- Drop: Es utilizado para detectar registros de estadísticas y borrarlos.
- Mutate: Permite renombrar, mover o reemplazar campos de un evento. En este caso se usa para convertir los tipos de registro a otro formato.

3.6.2. Monitorización de datos en Kibana

Cada uno de estos campos de datos de cada uno de los registros de datos de todos los índices configurados en Kibana son los que posteriormente se utilizan para la realización de búsquedas y la generación de gráficas de datos.

La visualización de datos en Kibana se realiza a través de gráficas y cuadros de resultados de búsquedas, por lo que se deben configurar todas las gráficas y búsquedas que se deseen en el apartado Visualize. Por el momento, se configuran las siguientes gráficas para los siguientes tipos de datos:

Suricata-Event type:

Histórico de los diferentes eventos que Suricata detecta en el tráfico del móvil a lo largo del tiempo.

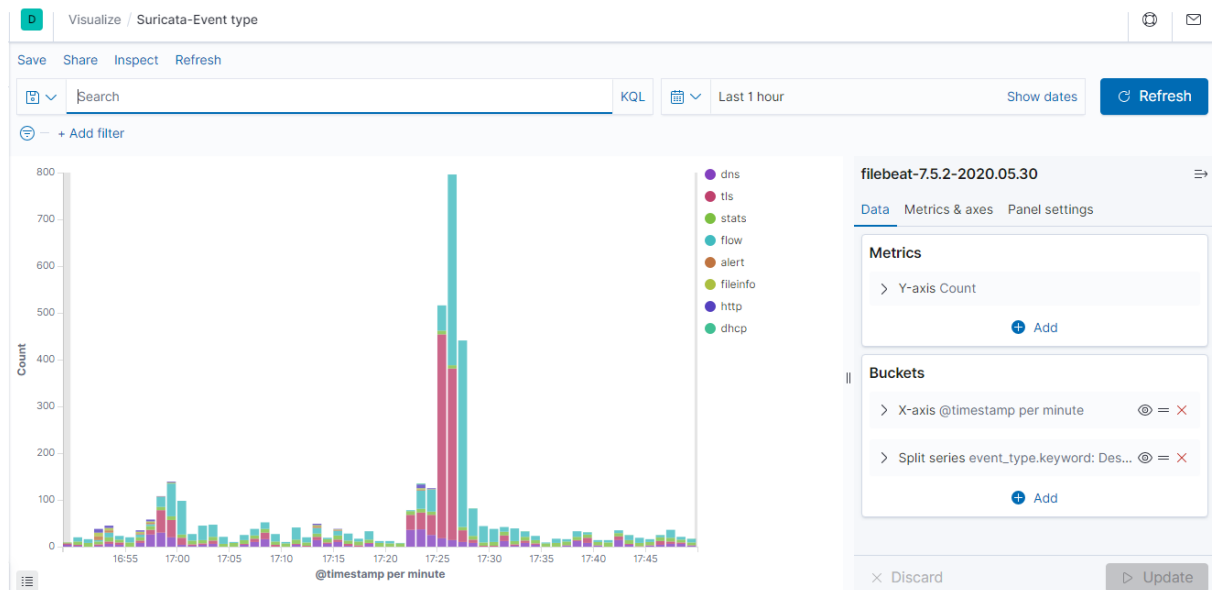


Figura 69: Suricata-Event type

Suricata Alert Signature.

En el gráfico de barras a continuación, estamos monitoreando las diferentes categorías de alertas que Suricata está registrando con el tiempo:

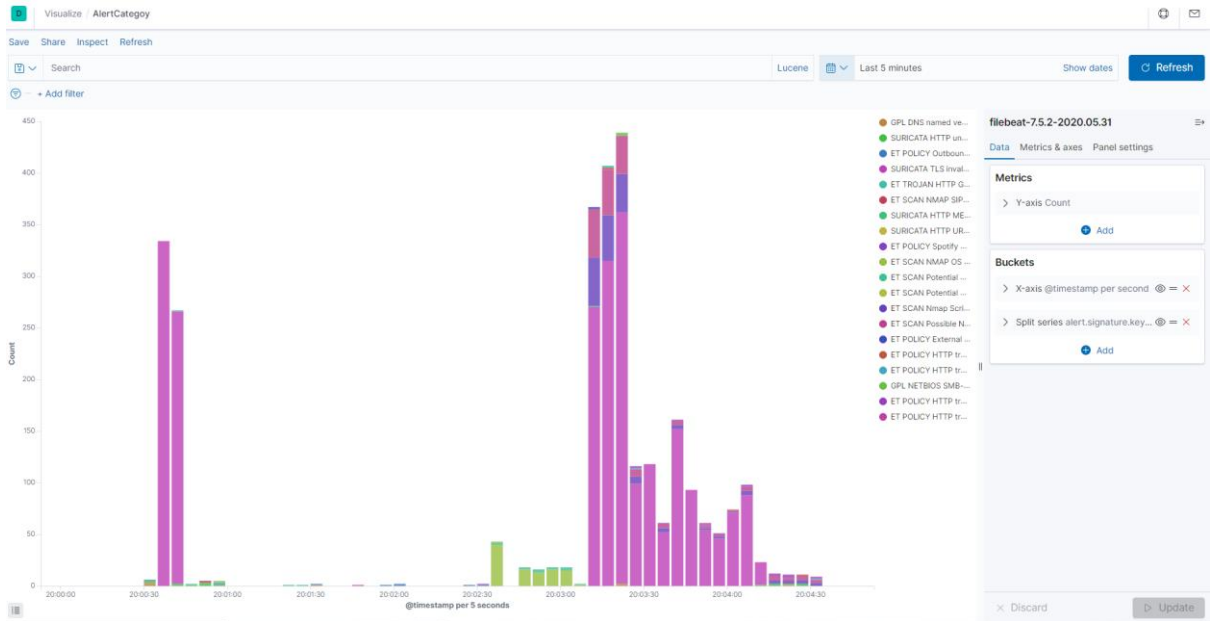


Figura 70: Suricata Alert Signature.

Para monitorear las firmas de alertas, podríamos construir una visualización de tabla de datos:

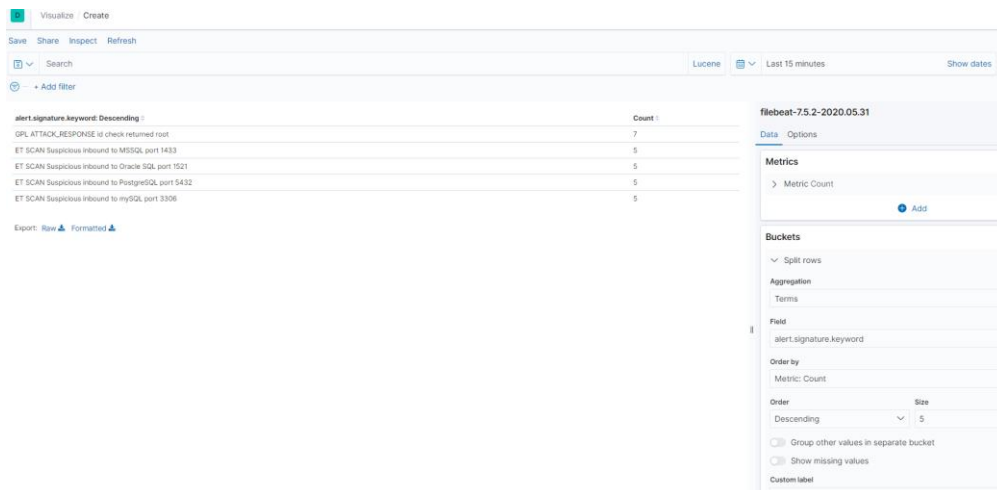


Figura 71: Suricata Alert Signature.

Suricata Geopip Country.

Podemos monitorear la distribución geográfica del tráfico que ingresa a nuestro sistema utilizando la visualización del Mapa de coordenadas de Kibana. Para hacer esto, haremos uso de la mejora geográfica aplicada al campo src_ip en los registros de Suricata.

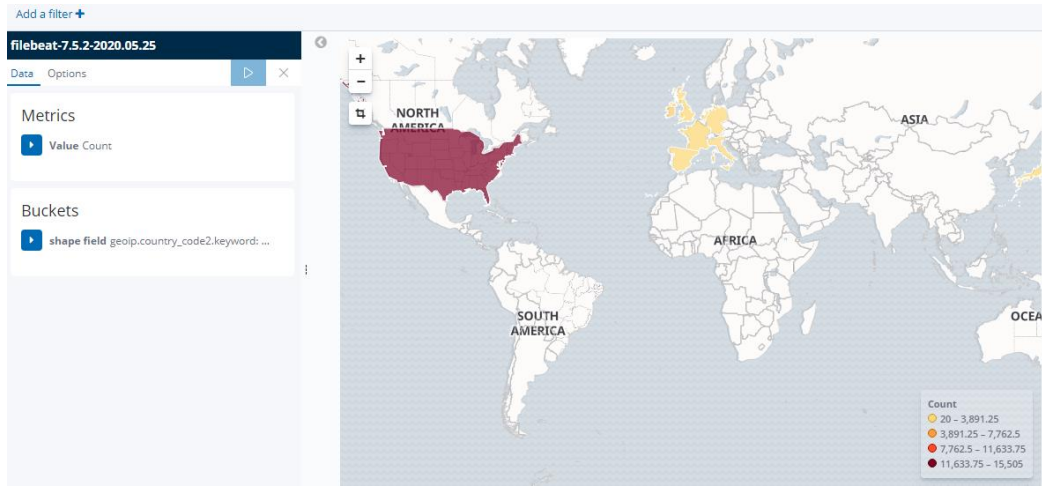


Figura 72: Suricata Geop Country.

Suricata

Las visualizaciones de gráficos de líneas son excelentes para monitorear tendencias a lo largo del tiempo. En la visualización a continuación, observamos los principales tipos de registro de

Suricata AADispositivo.

Trafico de red por dispositivos y tiempo.



Figura 73: Suricata AADispositivo.

Suricata Dns.

Mostramos los sitios más visitados de nuestros dispositivos.

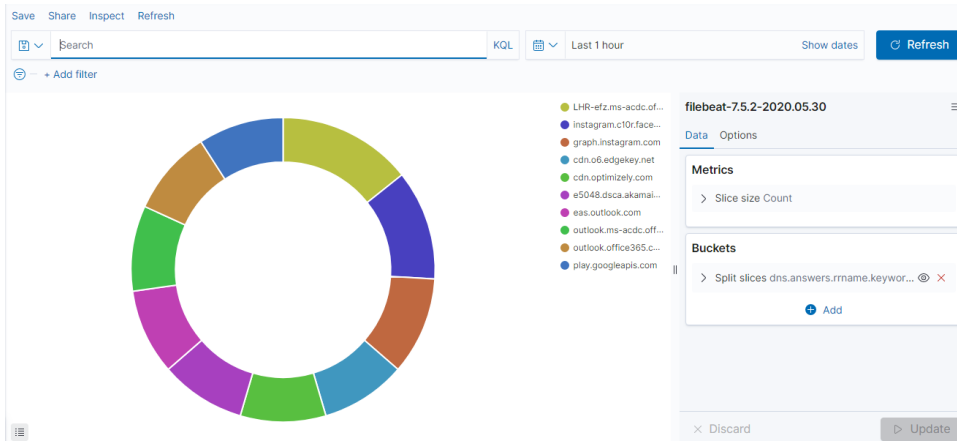


Figura 74: Suricata Dns.

Suricata top Ip destino.

Se muestra el top 10 de Ip de destino de nuestros dispositivos.

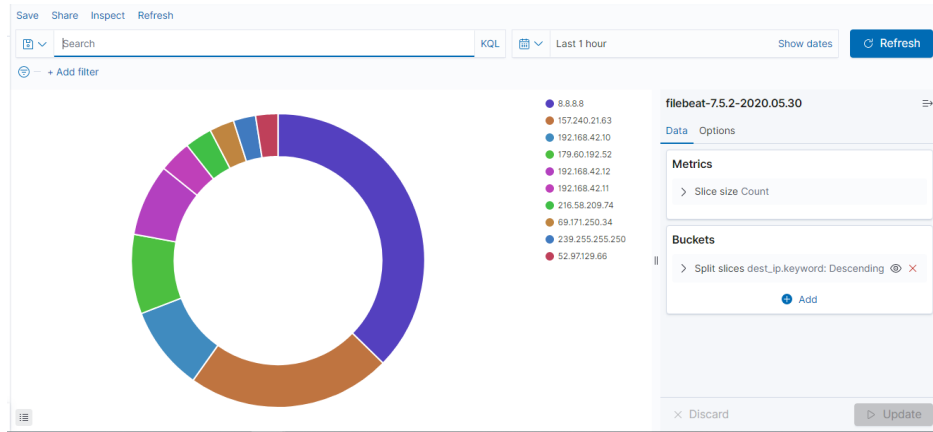


Figura 75: Suricata top Ip destino.

Suricata top Puerto Destino

Se muestra el top 10 de los puertos de destino que acceden nuestros dispositivos.

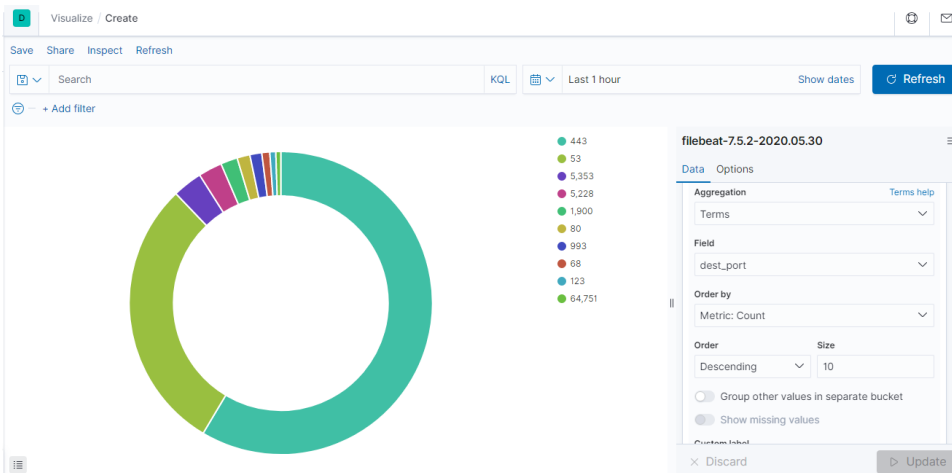


Figura 76: Suricata top Puerto Destino.

Dashboard:

Finalmente, nos detendremos brevemente el Dashboard de Kibana. Para ello será necesario crear un primer panel de control de prueba utilizando la búsqueda y la visualización que se guardaron en los pasos anteriores 4 y 5. Selecciona en primer lugar el panel de control en la navegación de la página y clics en “Create new dashboard” (Crear nuevo panel de control) y, a continuación, en “Add” (Añadir). Kibana listará entonces automáticamente todas las visualizaciones o búsquedas guardadas:

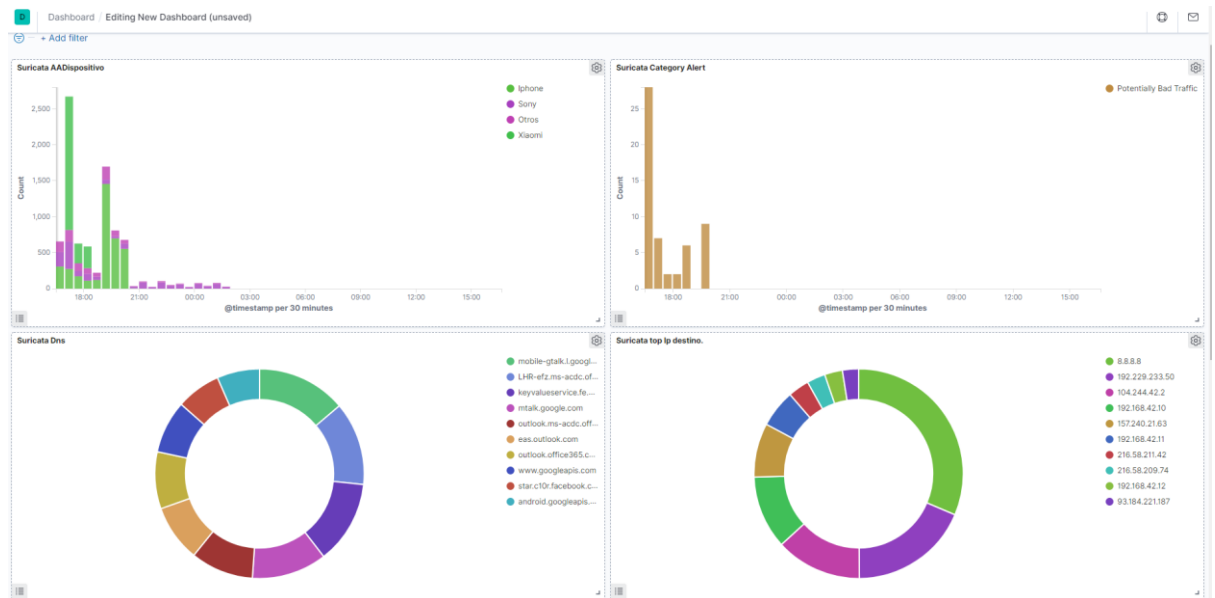


Figura 77: Dashboard 1/2.

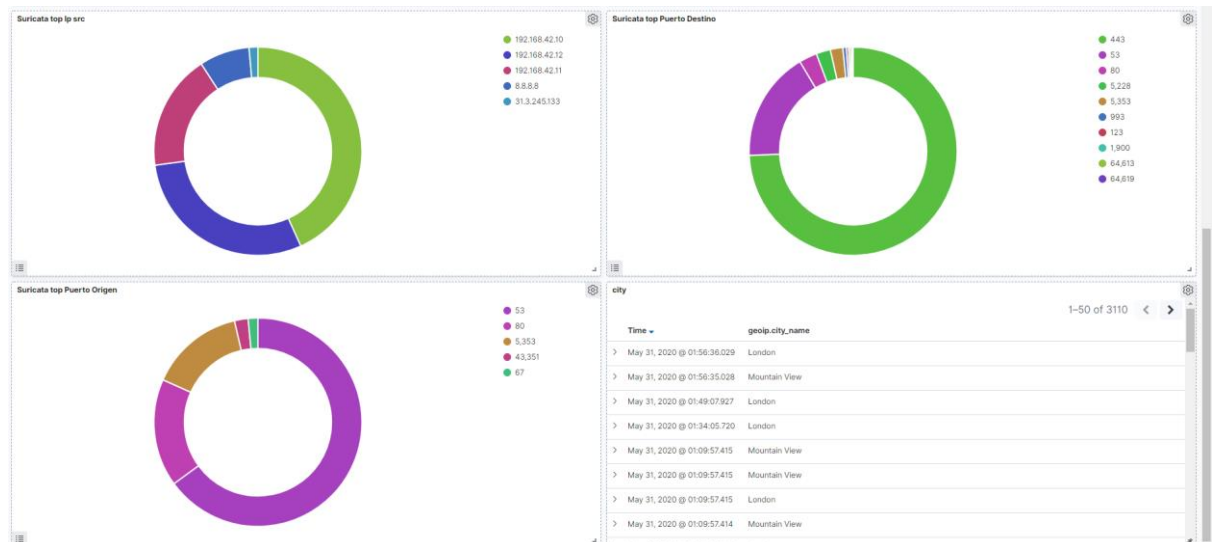


Figura 78: Dashboard 2/2.

3.7. Envío de alertas con Kibana

Las alertas le permiten detectar condiciones complejas dentro de diferentes aplicaciones de Kibana y activar acciones cuando se cumplen esas condiciones. Las alertas funcionan ejecutando verificaciones en un tiempo para detectar condiciones concretas. Cuando se cumple

una condición, la alerta la rastrea como una instancia de alerta y responde activando una o más acciones. Las acciones generalmente implican interacción con los servicios de Kibana o integraciones de terceros.²⁵

Cómo funciona la alerta:

Una alerta consta de condiciones, acciones y un cronograma. Cuando se cumplen las condiciones, se crean instancias de alerta que representan acciones y las invocan. Para facilitar la configuración y actualización de acciones, las acciones se refieren a conectores que centralizan la información utilizada para conectarse con los servicios de Kibana y las integraciones de terceros.

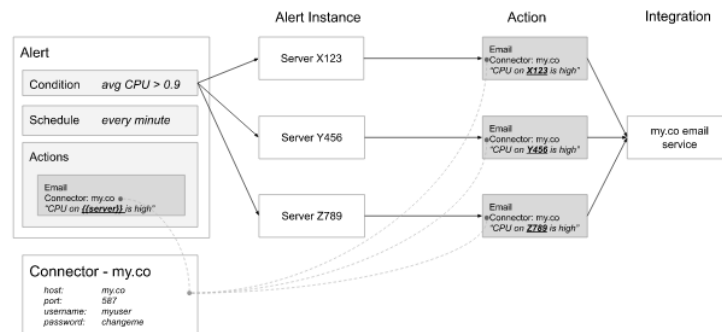


Figura 79: Funcionamiento alerta.

Alerta: especificación de las condiciones a detectar, el cronograma de detección y la respuesta cuando se produce la detección.

Acción: la respuesta a una condición detectada definida en la alerta. Por lo general, las acciones especifican un servicio o integración de terceros junto con detalles de alertas que se le enviarán.

Instancia de alerta: estado rastreado por Kibana para cada aparición de una condición detectada. Las acciones, así como los controles como el silenciamiento y la nueva notificación, se controlan a nivel de instancia.

Conector: configuraciones centralizadas para servicios e integración de terceros a las que hacen referencia las acciones.

Configuración de alerta.

Antes de configurar nuestra alerta nos disponemos a crear un conector, en nuestro caso las alertas serán enviadas por correo, con lo cual hemos configurado un conector tipo correo electrónico.

²⁵ <https://www.elastic.co/guide/en/kibana/7.x/alerting-getting-started.html#alerting-concepts-conditions>

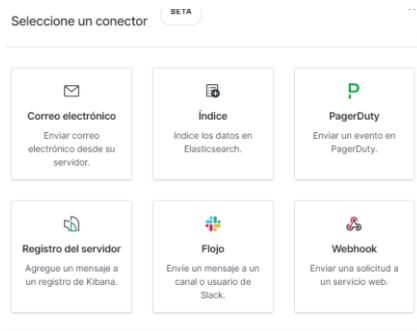


Figura 80: Tipo de conector.

Después configuramos nuestro servidor de correo electrónico:

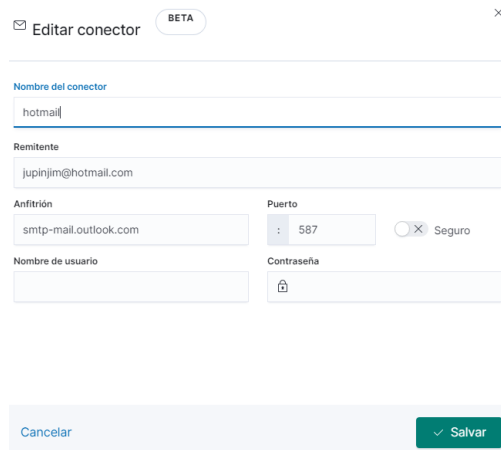


Figura 81: Configuración servidor correo.

A continuación tenemos que configurar nuestra alerta, cada cuanto se verifica y el tiempo de notificación.

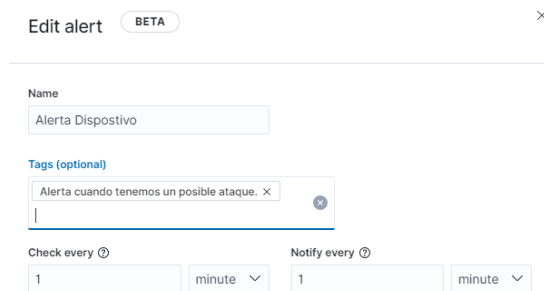


Figura 82: Alerta.

Luego seleccionamos un índice, en nuestro caso hemos escogido *filebeat** y el campo que vamos a examinar que es *alert.signature.keyword*,

Index threshold

1 Select an index.

```
INDEX filebeat*
WHEN count()
GROUPED OVER top 1 'alert.signature.keyword'
```

Figura 83: Índice alerta.

Por último definimos la condición, en nuestro caso que esté por encima de 0, una vez que se cumpla esa condición se generaría una alerta y recibiríamos en nuestro correo electrónico un posible ataque.

2 Define the condition.

```
IS ABOVE 0 FOR THE LAST 1 minute
```

Figura 84: Condición alerta.

En nuestro correo recibiríamos esto:

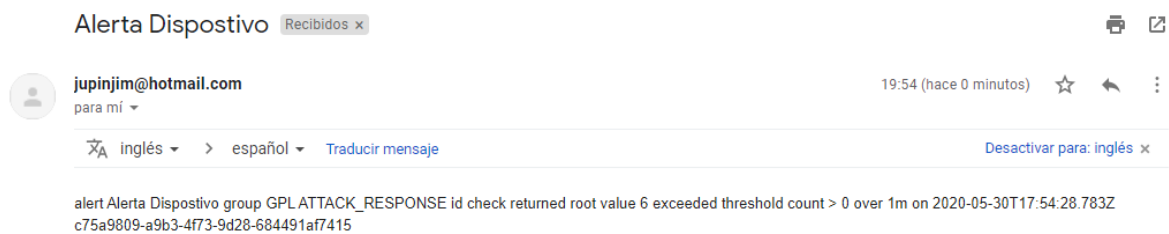


Figura 85: Correo Alerta.

4. Conclusiones y trabajo futuro

A continuación se describen las conclusiones finales del trabajo así como algunas lecciones aprendidas:

- Con este proyecto, se ha demostrado que en la actualidad es posible implementar sistemas de seguridad caseros, con un coste asequible. Raspberry es una de las plataformas más extendidas para el desarrollo de este tipo de proyectos a nivel doméstico. Gracias a este tipo de proyectos se ve la viabilidad de usar estos dispositivos en entornos reducidos.
- Otro de los objetivos del proyecto ha sido analizar las mejores opciones que ofrece el mercado, en software libre, para llevar a implementar un sistema de detección de intrusos basado en red con logs centralizados. Mediante el estudio realizado, se ha llegado a la conclusión de que el mejor motor de análisis de tráfico basado en firmas en estos momentos es Suricata.
- Se ha podido comprobar que tanto Suricata IDS como la Pila Elastic son aplicativos muy potentes y con capacidad de configuración adaptable a las necesidades de cada entorno.
- También se determina que la pila Elastic formada por Filebeat, Elasticsearch, Logstash y Kibana son la mejor opción para abordar los apartados de persistencia de los datos y presentación de la información. Esto se debe a las prestaciones del sistema y la multitud de presentaciones de la información posibles. A esto se le añade la simplicidad de integración entre los componentes, dado que son trabajados por el mismo grupo de desarrolladores.
- Por otro lado la Pila ELK es demasiado pesada para funcionar en la propia Raspberry-pi. Se ha optado en este proyecto por instalarla en la nube.
- Hay amenazas en la red, que no pueden tratarse con nuestro sistema, ya que podemos controlar donde se conectan los dispositivos, pero no el contenido de las comunicaciones que suelen ir cifradas.
- Un sistema como este, no puede dar soluciones completas al análisis del tráfico móvil, sino que deben utilizarse como un complemento que ofrece información y ayuda.

4.1. Problemas encontrados en la implementación del proyecto.

A continuación se detallan algunos de los problemas encontrados en la implementación que han retrasado la planificación general del proyecto.

4.1.1. Configuración de Raspberry-pi como punto de acceso con MitmProxy.

Se prepararon varios prototipos, para comprobar si bajaba la calidad del servicio utilizando la Raspberry-pi como punto de acceso WiFi a través del proxy MITM. Se realizó una instalación completa con el software MitmProxy y finalmente se optó por esta solución, ya que de las dos

soluciones probadas era la más ventajosa para la calidad del servicio, aun así la velocidad de conexión ha resultado más baja que conectado directamente a la WiFi.

4.1.2. Estudio de diseño final del sistema ELK.

Se hicieron prueba de instalación de ElasticSearch y Logstash en la propia Raspberry, pero se descartó, principalmente para evitar cargar demasiado el dispositivo y por diversos problemas en la compilación e instalación de los productos de Elastic en la propia Raspberry-pi que estaban consumiendo mucho tiempo de investigación.

Gran parte de la instalación se realizó en la nube, pero los filtros de Logstash nos funcionaban, con lo cual hemos tenido que implementar una Pila interna con máquina virtual para poder hacer las pruebas y poder analizar los datos correctamente.

4.1.3. Tareas pendientes en la implementación.

Finalmente se ha conseguido la implementación de un sistema funcional que permite el análisis de los dispositivos móviles que se conectan a nuestra red WiFi, pero ha faltado tiempo para experimentar lo suficiente con las reglas de Suricata, para afinar más en la búsqueda de amenazas y realizar más pruebas de concepto.

4.2. Trabajo futuro.

Una vez conseguidos los objetivos didácticos establecidos en este trabajo, se enumeran a continuación varias líneas de trabajo futuro para mejorar el proyecto:

- Ha quedado pendiente probar el sistema de alertas notificando mediante otras herramientas que la pila ELK nos ofrece.
- Definir un paquete de reglas útiles en el IDS para detectar aplicaciones concretas.
- Mejorar el sistema SIEM. En el proyecto se ha utilizado la pila ELK, pero se ha tenido que instalar en la nube con las complicaciones de seguridad de los datos que esto conlleva. Sería interesante utilizar un sistema de monitorización en la propia Raspberry-pi más.
- ELK es un conjunto de herramientas con mucho potencial, el margen de mejora y optimización es amplio. En este trabajo solo se abarcado un conocimiento base, sería interesante un proyecto que abarcara todos los servicios que nos ofrece esta herramienta y profundizar hasta un punto experto.
- En este trabajo se ha definido un Dashboard en Kibana con finalidades didácticas para valorar la potencia de la herramienta en lo que respecta a los objetivos del proyecto. Por lo tanto quedaría pendiente como trabajo futuro definir un Dashboard con más gráficos de utilidad para el análisis de datos más concretos.

5. Bibliografía/Webgrafía.

- La revolución del Tráfico de Datos Móviles en los próximos cinco años
<https://cibersuite.com/la-revolucion-del-trafico-datos-moviles-los-proximos-cinco-anos/>
- Análítica móvil: la segmentación para orientar tus campañas
<http://blog.fmb.mx/analitica-movil-segmentacion>
- Top 5 de herramientas de analítica móvil para medir el éxito de tu app
<https://kingofapp.com/es/blog/top-herramientas-analitica-movil-medir-exito-app/>
- Aepd.es
<https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf>
- Análisis de la seguridad en dispositivos móviles durante el primer semestre de 2019 | WeLiveSecurity
<https://www.welivesecurity.com/la-es/2019/09/03/analisis-seguridad-dispositivos-moviles-primer-semester-2019/>
- Catálogo de medidas preventivas y herramientas para proteger la privacidad | AEPD
<https://www.aepd.es/es/areas-de-actuacion/recomendaciones/medidas>
- Latam.kaspersky.com
<https://latam.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store>
- Raspberry Pi
https://es.wikipedia.org/wiki/Raspberry_Pi
- Ubuntu
<https://es.wikipedia.org/wiki/Ubuntu>
- Servidor cloud o local, ¿cuál es la mejor opción para las pymes?
<https://blog.prodware.es/servidor-cloud-local-mejor-opcion-pymes/>
- Hyperfox es uno de los Proxy MITM para la captura de tráfico HTTP y HTTPS más completos
<https://www.redeszone.net/2016/10/02/hyperfox-uno-los-proxy-mitm-la-captura-trafico-http-https-mas-completos/>
- Mitmproxy: MitM de tráfico Web for fun and profit - Hacking Ético
<https://hacking-etico.com/2015/10/23/mitmproxy-mitm-de-trafico-web-for-fun-and-profit/>
- Introduction Mitmproxy
<https://docs.mitmproxy.org/stable/>
- Snort - Network Intrusion Detection & Prevention System
<https://www.snort.org/>
- Snort
<https://es.wikipedia.org/wiki/Snort>
- Suricata

- <https://suricata-ids.org/>
- Búsqueda y análisis de código abierto · Elasticsearch | Elastic
<https://www.elastic.co/es/>
- Industry Leading Log Management | Graylog
<https://www.graylog.org/>
- Download Raspberry Pi OS for Raspberry Pi
<https://www.raspberrypi.org/downloads/raspbian/>
- Running a man-in-the-middle proxy on a Raspberry Pi 3
<https://www.dinofizzotti.com/blog/2019-01-09-running-a-man-in-the-middle-proxy-on-a-raspberry-pi-3/>
- Suricata IDS – Instalación, puesta en marcha y primera prueba – Follow The White Rabbit
<https://fwhibbit.es/suricata-ids-instalacion-puesta-en-marcha-y-primer-prueba>
- elastic-pi.md
<https://gist.github.com/andig/650915e02b18cfe38de6516686977bca>
- josh-thurston/easyBEATS
<https://github.com/josh-thurston/easyBEATS>
- A Practical Introduction to Logstash
<https://www.elastic.co/es/blog/a-practical-introduction-to-logstash>
- Alerting and Actions | Kibana Guide [7.x] | Elastic
<https://www.elastic.co/guide/en/kibana/7.x/alerting-getting-started.html#alerting-concepts-conditions>