UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Sistemas de detección de intrusos en la red para usuarios no técnicos

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Simón Paniello, Miguel Ángel

Tutor/a: Andrés Martínez, David de

CURSO ACADÉMICO: 2022/2023

Resumen

Los sistemas NIDS (del inglés *Network Intrusion Detection System*) permiten monitorizar una red generando alertas cuando se dé una o varias conexiones que puedan señalar a un ataque o compromiso. Estos sistemas se usan por organizaciones para ayudar a defender sus entornos informáticos, entornos industriales, etcétera. De hecho, existen aplicaciones que facilitan gestionar más fácilmente un NIDS desde algún tipo de entorno en concreto, pudiendo modificar configuraciones para, por ejemplo, definir e ignorar ciertas conexiones que, siendo legítimas, estuvieran provocando alertas. Sin embargo, hay un ámbito para el que no parece haber soporte en este sentido, y es el de la red doméstica de los usuarios no técnicos, es decir, el público general que no posee especiales conocimientos o formación en seguridad de la información ni en sistemas informáticos. Estos usuarios son los que más dificultad pueden tener para entender y gestionar un sistema de detección de intrusos, pero también tienden a ser precisamente los usuarios más vulnerables y los que menos información tienen sobre el estado de su red, por lo que se podrían beneficiar enormemente de un sistema de este tipo que fuera accesible y orientado al público general. El objetivo de este trabajo es el desarrollo de una aplicación que permita la gestión de un sistema NIDS a los usuarios no técnicos, enfocando la aplicación a la recepción de alertas útiles, la asistencia para poder reaccionar a estas alertas, y la capacidad de definir excepciones a las reglas de forma precisa, para las conexiones que el usuario pueda confirmar como legítimas. Para ello, primero se buscará agrupar los distintos tipos de alerta bajo una serie de categorías generales. Esto permitirá diseñar una explicación clara y entendible para cada caso de uso, lo cual no sería factible para cada alerta distinta. También se añadirá una serie de consejos relacionados con el caso de uso, que sean factibles para usuarios con un bajo nivel de conocimiento técnico, así como enlaces de referencia y otros recursos complementarios. Por último, se ofrecerá la posibilidad de añadir una excepción a la regla para esa IP origen o destino, puerto origen o destino, cabeceras, etc. Para que esta opción sea manejable por un usuario sin conocimiento técnico, los consejos al respecto deberán ser claros e incluir los riesgos de ignorar alertas basándose en un criterio demasiado genérico.

Palabras clave: NIDS, IDS, monitorización, ciberseguridad, aplicación.

Abstract

Network Intrusion Detection Systems are a tool to monitor a network generating alerts when certain connections are made that could point to a compromise or attack. These systems are used by companies to help defend their IT environments, industrial environments, and such. Apps have been developed to better manage systems like NIDS, with such functionalities as defining and ignoring a type of connection that is legitimate but has been triggering alerts. However, these kinds of apps are usually developed to be used in a certain environment, and one such environment that has not been covered is the home network of non technical users, that is, users without significant knowledge or training in cybersecurity. These users are confronted with the most hardship when managing such a system as a NIDS, but are also usually the most vulnerable users and the ones with the least intel about the state of their network, so it would be greatly beneficial for them to have a similar app that was oriented to the broader public. The goal of this work is to develop an app that will allow managing a NIDS to the non technical users, focusing in receiving useful alerts, aiding the user in deciding how to react to those alerts, and giving the user a way to define exceptions to the rules in a precise manner, for the connections that the user can confirm are legitimate. In order to achieve this, currently existing rules will first be grouped in a series of general categories. This will allow the writing of clear and understandable explanations for each category, which isn't possible for each individual alert. Tips about the use case will also be included, tips intended for users with a low technical level. Also included will be other resources such as reference links. Lastly, there will also be a way to add exceptions to the rules for a specific source IP, destination IP, source or destination port, etc. For this option to be adequate for a non technical user, advice on it must be clear and include the risks of ignoring alerts based on too broad criteria.

Keywords : NIDS, IDS, monitoring, cybersecurity, app.

Tabla de contenidos

1. Introducción

1.1: Motivación

La seguridad de la información es un tema de gran importancia en la actualidad, ya que cada vez son más comunes los ataques cibernéticos [1] [2] [3] y la información confidencial almacenada en las redes es cada vez más valiosa [4] [5]. Una de las medidas de seguridad más utilizadas para proteger las redes es el uso de sistemas de detección de intrusos en red (en adelante NIDS, del inglés Network Intrusion Detection System) [6].

Estos sistemas permiten predefinir varias reglas, cada una de las cuales consiste en una serie de características. Cuando se produzca en la red una conexión cuyas características coincidan con una de estas reglas, se generará una alerta para su envío a cualquier clase de sistema de gestión de alertas. Dicho sistema puede ser desde una solución Administración de Eventos e Información de Seguridad (SIEM, del inglés Security Information and Event Manager) centralizada que integre varias fuentes, hasta un sencillo programa que envíe un mensaje a un teléfono móvil [7].

Pero un factor común a las herramientas utilizadas para la gestión de estas alertas es que siempre están orientadas a usuarios con conocimiento técnico en materia de tecnologías de la información e incluso seguridad de la información.

El objetivo de este trabajo es el desarrollo de una aplicación que permita a usuarios sin este conocimiento gestionar y entender de manera clara y sencilla un NIDS, de forma que puedan extraer de las alertas información de valor y tomar las medidas reactivas apropiadas.

Para ello, será necesario encontrar o diseñar reglas cuyas alertas sean útiles para entornos domésticos, además de poner especial empeño en diseñar una interfaz de usuario intuitiva y unas descripciones claras e informativas.

1.2: Objetivos del trabajo

El objetivo de este trabajo es explorar la aplicabilidad de una herramienta NIDS en un entorno doméstico y la utilidad de las reglas prediseñadas más comunes en estas herramientas para usuarios sin conocimiento o entrenamiento técnico.

El medio para llevar a cabo este objetivo será la creación de una aplicación para la gestión de un sistema NIDS. En esta, un NIDS estará a la escucha de las reglas que se han determinado útiles y, cuando dispare una alerta, esta quedará disponible para ser visualizada por los dispositivos locales que realicen una petición.

Por tanto, por una parte, el NIDS deberá estar preconfigurado descartando las reglas que no sean aplicables a un entorno doméstico. Por otra parte, el servidor deberá ofrecer las alertas a los dispositivos que las consulten junto con unas explicaciones y consejos que se adapten a un nivel técnico bajo.

Finalmente, el servidor también deberá ofrecer la posibilidad de añadir cambios en la configuración, principalmente excepciones a reglas concretas para los dispositivos, puertos y/o paquetes concretos que no precisen alertas. Es importante destacar que esta función está pensada para los casos que el usuario pueda asegurar con certeza y de antemano que serán legítimos.

1.3. Breve descripción de los demás capítulos

En este apartado se resume la estructura de los demás capítulos.

- Estado del arte: en este capítulo se comentan las herramientas existentes que cumplan una función similar a la planteada. Además, se examinan distintos NIDS así como fuentes abiertas de reglas para alimentarlos y potenciarlos.
- Diseño: en esta sección se verán las distintas decisiones tomadas así como el diseño de la aplicación y el de unas explicaciones claras para las alertas.
- Implementación: En esta parte se presentará la aplicación desarrollada, tanto la configuración del servidor como su programación y la del cliente.
- Pruebas: en este punto se replica el uso esperable de la aplicación para comentar las distintas fases de los casos de uso.
- Conclusiones: En este apartado se revisan los objetivos iniciales y el resultado final para determinar el cumplimiento de los primeros por parte del segundo.
- Trabajos futuros: Finalmente, se recogen ciertas mejoras posibles para la aplicación, que no se han implementado por salir del alcance determinado para la misma, pero pueden aumentar su utilidad o calidad.

2. Estado del arte

Actualmente no existen productos similares en el mercado, ya que los sistemas NIDS se utilizan habitualmente para su gestión por parte de usuarios técnicos dentro de entornos comerciales, industriales, gubernamentales… [8] donde se monitoriza la red desde distintas fuentes, se encuentran servicios expuestos a Internet, y hay un volumen mucho mayor de elementos en la red, lo cual lleva a una mayor *superficie de ataque* (número de posibles vulnerabilidades tanto informáticas como humanas).

2.1. Sistemas SIEM: gestión de información y eventos de seguridad

Los productos más similares, o que mejor cubren necesidades similares, están pensados para centralizar alertas provenientes de distintas fuentes, y gestionarlas desde un equipo de varias personas. Son los llamados sistemas SIEM [9] (del inglés *Security Information and Event Management*, es decir, Gestión de Información y Eventos de Seguridad).

Existen múltiples sistemas SIEM. Los hay de código abierto como OSSIM [10] o Wazuh [11], y los hay de licencia comercial como SolarWinds SEM [12], FortiSIEM [13] o GLORIA [14].

Estas plataformas de seguridad recopilan, correlacionan y analizan información de múltiples fuentes para brindar una visión integral de la postura de seguridad de una organización. No sólo están diseñados para ayudar a detectar y responder a amenazas de seguridad, sino también para cumplir con requisitos de cumplimiento normativo.

Por tanto, los sistemas SIEM no sólo recopilan datos de un sistema NIDS, sino de diferentes fuentes como registros de eventos de sistemas, registros de firewall, registros de servidores, registros de aplicaciones…

Estos sistemas no sólo incluyen muchas funcionalidades que no son necesarias para este proyecto, sino que además suelen añadir una capa más de complejidad al ofrecer una funcionalidad propia de adición de excepciones, no relacionada con la funcionalidad similar integrada en muchos NIDS.

.

2.2. NIDS: Sistemas de detección de intrusos en red

Un NIDS es un sistema que supervisa y analiza el tráfico de red en busca de actividad sospechosa o maliciosa, con el objetivo de identificar y responder a intentos de intrusiones o ataques cibernéticos en tiempo real.

Existen distintos NIDS, y algunos de los más populares [15] son:

- Snort [16]: Es uno de los sistemas NIDS de código abierto más conocidos. Utiliza una combinación de análisis de firmas y detección basada en reglas para identificar actividades sospechosas en el tráfico de red.
- Suricata [17]: También es un sistema NIDS de código abierto y se considera una alternativa a Snort. Ofrece capacidades de detección de amenazas en tiempo real y es altamente escalable.
- Bro/Zeek [18]: Es un sistema NIDS que se enfoca en el análisis de protocolo y en la generación de registros detallados. Proporciona una visión profunda del tráfico de red y es ampliamente utilizado en investigaciones de incidentes.

Estos sistemas son capaces de mantenerse a la escucha del tráfico de red y seleccionar de entre éste las conexiones que puedan ser relevantes para la seguridad de la red.

2.2.1 Elección de NIDS

De entre los NIDS mencionados, cada uno de ellos difiere en ciertas características [19], de las cuales las más relevantes para este trabajo se recopilan y comparan en la *Tabla* 1.

Tabla 1. Comparación de características entre distintos NIDS.

	SNORT	SURICATA	ZEEK
Soporte de la comunidad	Muy positivo	Positivo	Positivo
Configuración inicial	Configuración simple, scriptable	Configuración simple	Complicado de configurar
Adaptable a las necesidades	Modular, con más de 200 plugins	Modular	Arquitectura muy extensible
Valor añadido	Auto-genera documentación de referencias	Captura y extracción de malware	Registro y análisis extensivo del tráfico, extracción de archivos
Adaptable al hardware (al hardware poco potente)	Perfil de memoria escalable, multi-thread para procesado de paquetes	Multi-thread para todo el funcionamiento	Soporte de clustering para entornos a gran escala
Protocolos extra	Número muy limitado de protocolos	Certificados TLS/SSL, peticiones HTTP, peticiones DNS…	Soporte para DNS, FTP, HTTP, IRC, SMTP, SSH, SSL y otros
Scripting	Sin motor de scripting	Motor de scripting con info de los paquetes para correlar reglas	Lenguaje de scripting (Bro scripts) orientado a automatización y a generar eventos en un SIEM o similar

El soporte de la comunidad y la adaptabilidad son buenos en los tres NIDS, pero el soporte brilla especialmente en el caso de Snort por el mero hecho de llevar considerablemente más tiempo en el mercado.

Por esta misma razón, sin embargo, está más limitado en cuanto a análisis de protocolos de red (más allá de paquetes TCP o UDP). Aunque genera documentación de referencia sobre las alertas, esta documentación está orientada a usuarios técnicos y será de poca utilidad para este proyecto.

Snort tampoco presenta posibilidades integradas de scripting o de correlación entre reglas. Por último, es la opción con posibilidades menos potentes en cuanto a aprovechamiento del hardware.En este sentido, el NIDS que más llama la atención es Zeek. Sin embargo, la opción que presenta (clustering) no se corresponde con el hardware que habrá disponible para el servidor en un entorno doméstico. Esto denota una orientación a entornos grandes que se confirma por su elevada dificultad de configuración.

Por tanto, el NIDS elegido para este trabajo es Suricata, por su configuración simple (frente a Zeek) y su capacidad de analizar diversos protocolos (frente a Snort), pero sobre todo por su rendimiento en un hardware más limitado.

2.2.2 Reglas NIDS

Un NIDS funciona bajo la premisa de que no es factible revisar todo el tráfico de una red, de forma que es necesario definir de antemano una serie de características que puedan suponer una amenaza a la seguridad. Estos conjuntos de características que, si se dan todas juntas, deberán generar una alerta, se conocen como reglas NIDS.

Los NIDS permiten diseñar reglas que se adapten a las necesidades de cada red en la que se utilicen, y cada uno de ellos tiene una sintaxis propia para definir estas reglas. Por ejemplo, la sintaxis de las reglas en Snort y Suricata es bastante similar, lo que significa que las reglas de Snort a menudo se pueden adaptar y utilizar en Suricata con modificaciones mínimas. Sin embargo, algunas características y opciones específicas de Snort pueden no ser compatibles con Suricata y viceversa. Por su parte, Zeek utiliza su propio lenguaje de scripting (Bro script [20]) para definir reglas y políticas de detección. La sintaxis y la estructura de las reglas de Zeek son diferentes de las de Snort y Suricata, por lo que sus reglas nunca serán compatibles sin realizar cambios.

La estructura básica de una regla en Snort o Suricata es la siguiente:

```
action protocol src_ip src_port -> dst_ip dst_port (msg:"Title"; option:value, value).
```

Donde *action* es qué acción se debe tomar cuando se cumple la regla (suele estar en *alert* cuando se trata de una alerta), *protocol* es el protocolo IP (Suricata también soporta algunos protocolos de aplicación), *src_ip* y *src_port* son la IP y puerto desde

los que se origina la conexión a detectar, *dst_ip* y *dst_port* la IP y puerto hacia los que deberá ir la conexión para activar la regla, *msg* es el título que se le dará a las alertas y *option:value, value;* son uno o varios parámetros separadas por punto y coma, algunas de las cuales tendrán uno o varios argumentos separados por comas.

Además de la posibilidad de definir reglas, existen ciertos repositorios de reglas prediseñadas que abarcan un amplio espectro de posibles amenazas. Algunas de las fuentes populares de reglas NIDS abiertas incluyen:

- Snort Community Rules [21]: La comunidad de Snort mantiene un conjunto de reglas de detección gratuitas y de código abierto que cubren amenazas conocidas. Estas reglas se actualizan regularmente y están disponibles para su descarga desde el sitio web oficial de Snort.
- Talos Rules [21]: Talos Intelligence, parte de Cisco, proporciona un conjunto de reglas de detección gratuitas para Snort y Suricata. Estas reglas se basan en la inteligencia de amenazas y la investigación realizada por el equipo de Talos.
- Emerging Threats [22]: Emerging Threats Intelligence es una división de Proofpoint que se dedica a la investigación y análisis de amenazas de seguridad. El nombre Emerging Threats viene de la antigua empresa de mismo nombre que fue adquirida por Proofpoint en 2015. Se dedica a la investigación y análisis de amenazas de seguridad, y proporciona reglas de detección de intrusiones para sistemas NIDS, especialmente Snort y Suricata. Ofrece diferentes conjuntos de reglas que cubren una amplia gama de amenazas y es ampliamente utilizado en la comunidad de seguridad

En este proyecto se utilizarán las reglas de Emerging Threats que, si bien no vienen por defecto en la instalación de Suricata, sí se descargan por defecto al ejecutar el comando `suricata-update`. De entre las múltiples reglas que ofrece Emerging Threats, no todas las categorías de regla son útiles para un entorno doméstico.

Los títulos (*msg*:) de las reglas Emerging Threats tienen siempre [1] la siguiente estructura:

```
ET TYPE Explained title
```

Donde *TYPE* es una de entre (a fecha de redacción) 53 opciones [23] en las que Proofpoint clasifica estas reglas.

[1] Las reglas de la licencia de pago empiezan por ETPRO en lugar de ET

3. Diseño

En este capítulo se presenta la solución a nivel lógico, las posibilidades para la arquitectura física de red, y las reglas que se han contemplado, tanto las que se han quitado por defecto como aquellas para las que se han redactado consejos..

3.1 Estructura lógica de la solución

El proyecto constará de un NIDS a la escucha, un script en el mismo servidor que el NIDS, y una aplicación descargable o accesible por navegador desde los dispositivos locales que deseen disponer de las alertas.

En la Ilustración 1 se puede ver el esquema lógico de la solución. El servidor deberá tener un NIDS correctamente configurado y tener además un servicio abierto que le permita comunicarse con los clientes.

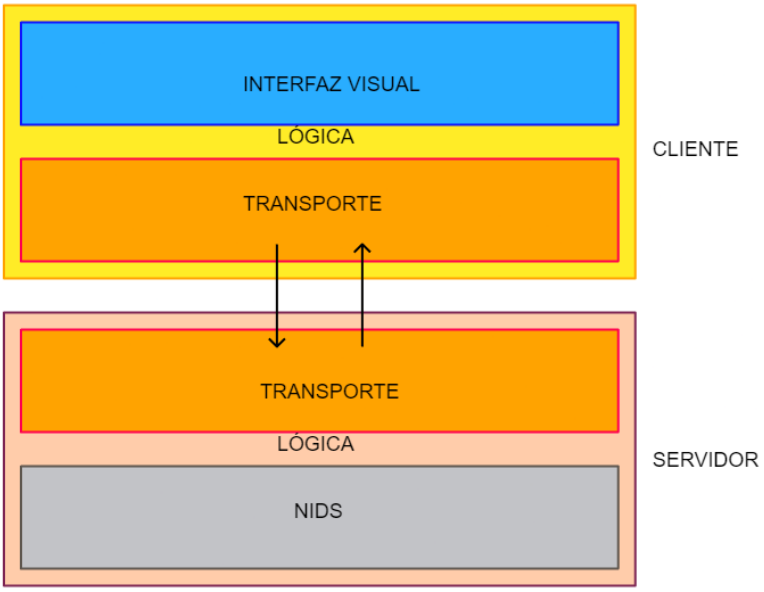


Ilustración 1. Esquema Lógico del Proyecto

Las comunicaciones se iniciarán por los clientes, ya que todas las funcionalidades a considerar (actualizar el listado de alertas o añadir una excepción) empezarán con una petición por parte del cliente. El servidor simplemente se mantendrá a la escucha de las peticiones[2] gracias a una API que permitirá el acceso (con contraseña) a clientes web o de aplicación. Actualmente, se ha diseñado un único tipo de cliente que accederá a los servicios desde una aplicación Android.

[2] El servidor únicamente se mantendrá a la escucha *en la versión actual*, ya que se ha planteado como trabajo futuro (capítulo 7) la notificación activa de las alertas más críticas.

3.2 Estructura física de la red

Para utilizar un NIDS en una red, el dispositivo en el que está instalado debe ser capaz de mantenerse a la escucha (*sniffing*) de todas las conexiones en dicha red. Para ello, el dispositivo (en adelante *servidor NIDS*) debe estar conectado a un dispositivo configurado para replicar todas las conexiones de una interfaz de red y enviarlas al servidor.

Para ello, existen distintas opciones, de las cuales se considerarán las siguientes:

- Port mirroring: algunos routers y switches permiten duplicar todo el tráfico de uno o varios puertos del router o switch y enviarlo a otro puerto en concreto. Si se duplican todos los puertos a los que se pueda conectar un dispositivo y se envían al puerto correspondiente al servidor, este recibirá todo el tráfico de red.
- Hub: al contrario que los routers o switches, los Hubs distribuyen todo el tráfico a la vez a todos sus puertos. Esto significa que si todo el tráfico de red pasa por un Hub conectado al servidor NIDS, este último tendrá por defecto acceso al tráfico.

Durante el resto de esta sección, cuando se hable de un servidor NIDS directamente conectado a un router, se entiende que se trata de un router con port mirroring.

3.2.1 Hub y servidor NIDS antes que el router

Para esta estructura, en teoría sólo sería necesario el uso de un Hub por el que pase toda la información que va hacia el router (ver Ilustración 2). El Hub lo redireccionará automáticamente al servidor NIDS.

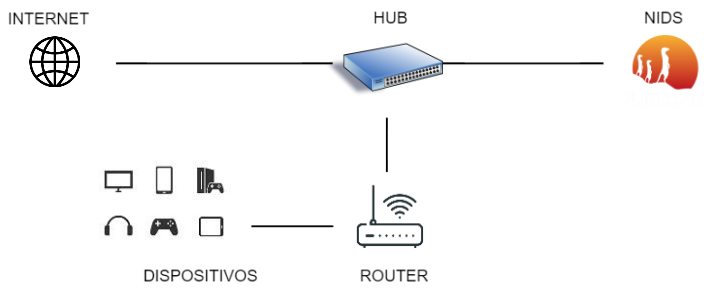


Ilustración 2: Estructura teórica con Hub y servidor antes que el router

La realidad de este caso es que el servidor NIDS necesitaría una IP diferente de cara a Internet, por lo que este esquema no es viable ni estaría permitido por la mayoría de los proveedores de servicio. Además, en caso de estar permitido, el servidor NIDS estaría expuesto a Internet, de forma que podría ser atacado de forma mucho más directa que estando detrás del NAT de la red.

Por eso, la estructura a considerar es más bien la de la Ilustración 3:

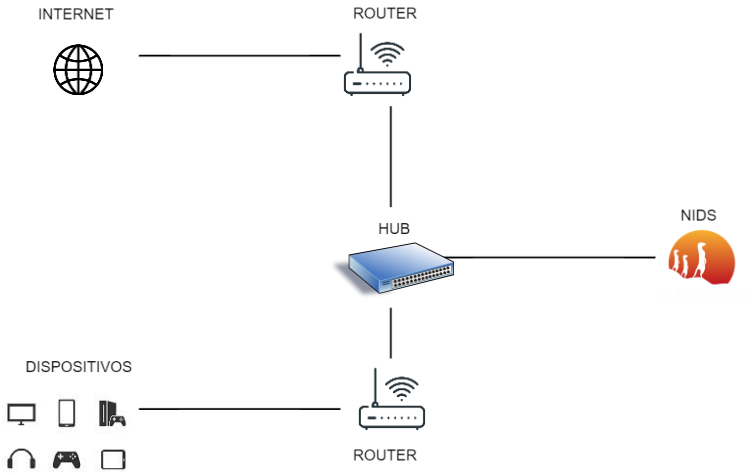


Ilustración 3: Estructura con Hub y servidor antes que el segundo router

La estructura final consistiría en un router como pudiera ser el instalado por el proveedor de servicios, que sólo haría la función de separar la red interna de Internet, y después la estructura antes mencionada.

El principal problema principal de esta estructura es que el (segundo) router no mostrará por defecto las Ips internas de los dispositivos sino la suya propia. Aunque se pueda configurar un port mapping para relacionar cada IP interna al router con un puerto del mismo en la interfaz externa, esto sólo se puede hacer para un número limitado de puertos en cada dispositivo. Cada uno de los dispositivos tiene tantos puertos (65,535) como el router, por lo que este se quedaría sin puertos que asignar en algún momento.

Es decir, que esta opción sólo es útil para monitorizar determinados puertos de los dispositivos o para monitorizar sin saber bien a qué dispositivo corresponden las alertas.

3.2.2 Hub y servidor NIDS después que el router

Como se puede ver en la Ilustración 4, se puede prescindir del segundo router y enviar las conexiones al servidor NIDS con las Ips adecuadas, si se conectan los dispositivos directamente al HUB.

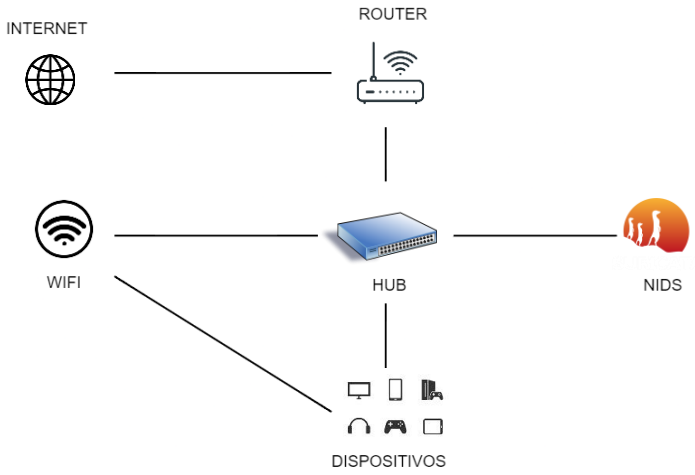


Ilustración 4: Estructura con Hub y servidor después que el router

Esta estructura sí que permitiría la correcta monitorización de los distintos dispositivos, aunque requeriría de un elemento extra en caso de querer monitorizar los dispositivos conectados por WiFi (de lo contrario, se podrían conectar directamente al router y no serían monitorizados).

Por supuesto, todas estas dificultades se pueden circunvalar si se utiliza un router con capacidad de port mirroring.

3.2.3 Router con port mirroring al servidor NIDS

El uso de port mirroring en el router permite simplificar la estructura, tal y como se aprecia en la Ilustración 5. Por supuesto, el router que realiza el port mirroring puede estar detrás de otro router comercial si esto simplifica la instalación.

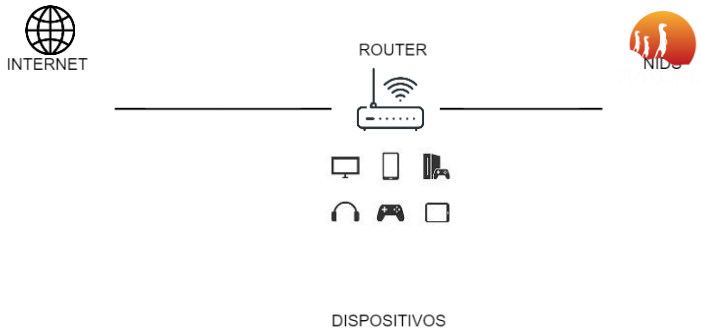


Ilustración 5: Estructura con router haciendo port mirror al servidor

El problema principal de tomar este camino es que el tráfico de red duplicado puede llegar a sobrecargar un router que no esté preparado para estos niveles de tráfico. Además, es necesario configurar el port mirroring, un paso extra que puede ser intimidante para un usuario no técnico.

3.2.4 Hardware dedicado

La última posibilidad es diseñar un dispositivo físico que las veces tanto de router (con port mirroring preconfigurado para la salida del servidor NIDS) como de servidor NIDS. Mientras que Ilustración 6 muestra la versión más sencilla de esto, en Ilustración 7 se puede ver una versión que alteraría menos la configuración original de la red. Más al respecto en el apartado de Trabajo Futuro.

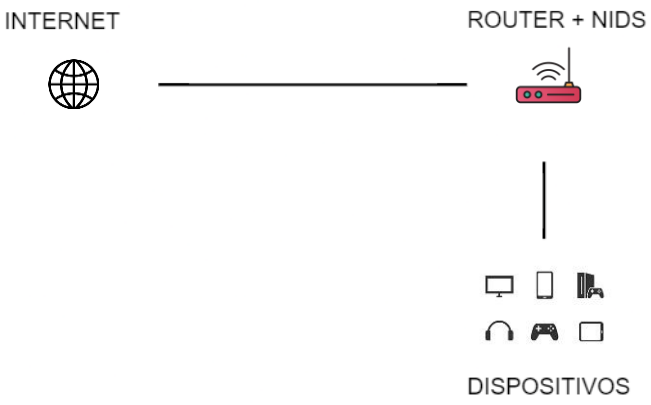


Ilustración 6: Router con servidor NIDS integrado

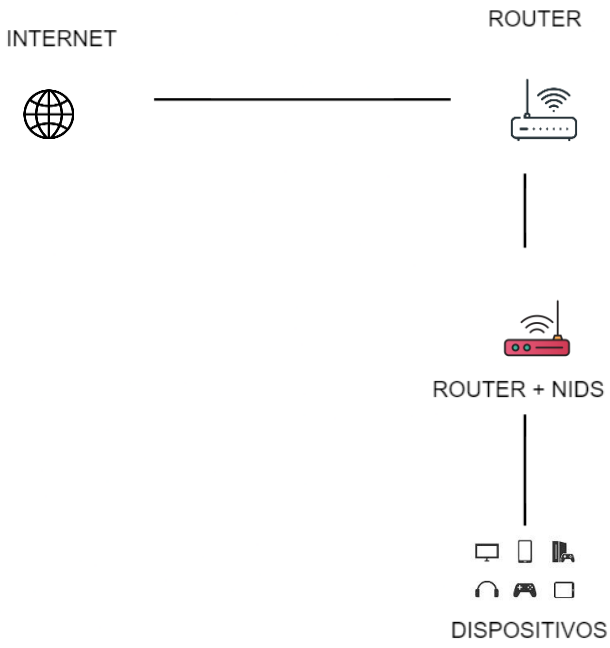


Ilustración 7: Router con servidor NIDS integrado, tras router comercial

3.3 Cliente para móvil

Se ha diseñado una aplicación cliente orientada a móviles para realizar y visualizar las acciones explicadas (obtención de alertas y adición de excepciones). Se ha elegido un cliente de móvil por la familiaridad del usuario promedio con el concepto de descargar una aplicación en el mismo.

El nombre pensado para la aplicación es INTU, por el inglés IDS for Non Technical Users.

Habrá tres pestañas disponibles en todo momento. Las alertas llegarán a la pestaña "ALERTAS" cuando se abra esta pestaña, y de nuevo cuando se utilice la función de cargar nuevas, como se puede ver en la Ilustración 8. Cada una de estas alertas podrá ser pulsada para ampliar la información y habilitar la opción de excepcionarla:

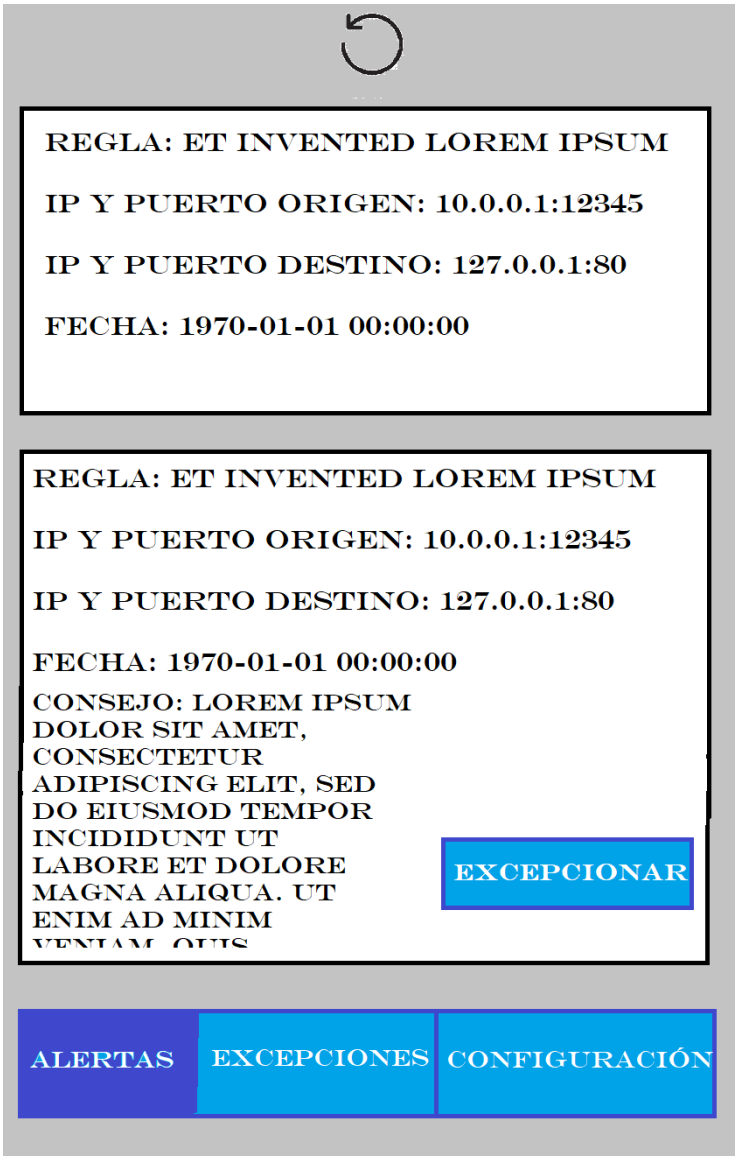


Ilustración 8: Pestaña Alertas

El botón “EXCEPCIONAR” visible en una alerta de la Ilustración 8 abrirá un diálogo en el que rellenar los datos de la excepción. Por defecto, vendrán los datos de la alerta desde la que se ha accedido a la pestaña de excepciones, en este caso los datos visibles en la Ilustración 9:

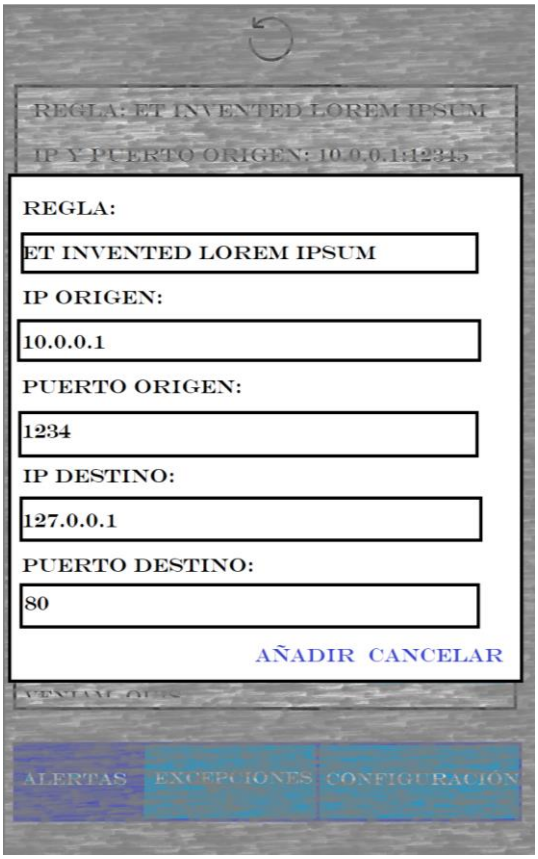


Ilustración 9: Diálogo con datos editables para añadir excepción

Desde aquí se podrán eliminar campos para hacer que la excepción abarque más alertas similares, o sustituir el valor de algún campo por otro valor que se sepa legítimo. Si hacemos click en Añadir se enviará la excepción al servidor con los datos que hayamos establecido.

Otra manera de acceder al mismo diálogo será desde la pestaña EXCEPCIONES, donde, tal y como se ve en la Ilustración 10, se podrán visualizar todas las excepciones establecidas en el fichero de excepciones del servidor.

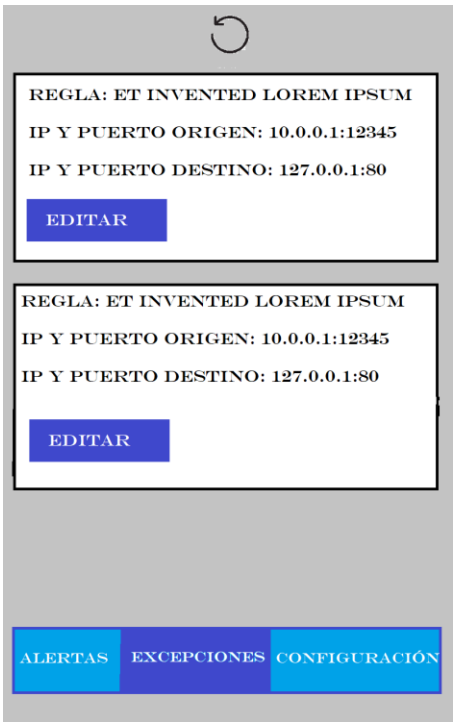


Ilustración 10: Pestaña Excepciones

Por último, la pestaña CONFIGURACIÓN permitirá configurar la IP y puerto del servidor al que se quiere acceder, así como la contraseña con la que autenticarse contra el servidor:

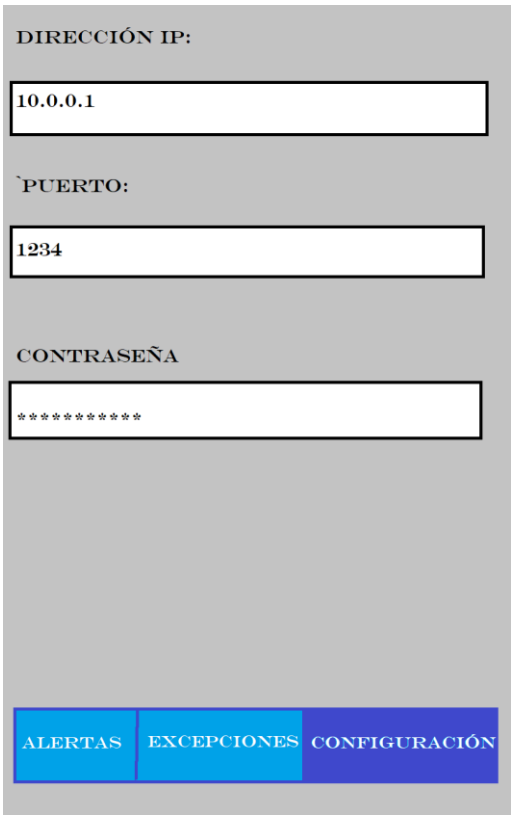


Ilustración 11: Pestaña Configuración

Como se puede ver en la Ilustración 11, la pestaña Configuración permitirá ver la IP y puerto actualmente introducidos, así como introducir una nueva IP, puerto o contraseña.

3.4 Reglas Emerging Threats

De entre las múltiples reglas que ofrece Emerging Threats, no todas las categorías de regla son útiles para un entorno doméstico. De entre estas categorías, se han redactado explicaciones para aquellas que se vayan a usar (subcapítulo 3.5), pero se han revisado o descartado las siguientes categorías:

- ET CHAT: La intención de esta categoría es detectar posibles contactos de agentes maliciosos, pero en una red doméstica no tiene sentido revisar el acceso a chats tan comunes como el de Facebook.
- ET FTP: Esta categoría está pensada en general para detectar ataques desde el exterior hacia objetivos con servicios expuestos a Internet. La utilidad de estas reglas se ve ampliamente reducida por el hecho de que una red doméstica no suele tener ningún servicio expuesto directamente a Internet (ni debería, ni puede por defecto). Por tanto, se excepcionan las reglas de conexiones entrantes.
- ET GAMES: Esta categoría está pensada para facilitar la prohibición de juegos online en empresas que los consideren inadecuados para la seguridad o la productividad. En el caso de una red doméstica, esta categoría no es necesaria en principio.
- ET HUNTING: Esta categoría es para reglas que darán falsos positivos a menudo, pero que están destinadas a ser correlacionadas con otras reglas para proporcionar inteligencia. Esta correlación la haría un sistema como puede ser un SIEM, pero no entra en el alcance de este trabajo.
- ET ICMP: Se trata de ataques contra vulnerabilidades relacionadas con el protocolo ICMP (protocolo de mensajes de control de Internet, en inglés: Internet Control Message Protocol). En la red doméstica de un usuario no técnico no es esperable encontrar un servidor de correo, por ejemplo.
- ET ICMP_INFO: Similar a la categoría anterior, pero no se trata siquiera de ataques sino de actividad cuyas alertas se utilizarían para llevar un registro.
- ET IMAP: Mismo caso que en las dos categorías anteriores, ya que no sólo se trata de actividad relacionada con el correo, sino que también incluye actividad no sospechosa.
- ET INAPPROPIATE: Igual que en el caso de ET GAMES, estas reglas están pensadas para un ambiente de trabajo y no para redes domésticas.
- ET INFO: Se trata de reglas que proporcionan información a nivel de auditoría.
- ET P2P: El uso de tráfico P2P en sitios como edonkey, Bittorrent, Gnutella y Limewire [24] es muy común para la piratería. Se estima [25] que al menos el 50% del contenido pirata contiene malware, por lo que estas reglas permanecerán por defecto para informar de los riesgos (al menos una o dos veces hasta que sean excepcionadas por los usuarios que asuman los riesgos).

- ET POLICY: Esta categoría se encuentra en una situación que ya se ha mencionado: sus reglas están destinadas a mantener informados a los administradores de red (o los responsables de equipo) de actividad inapropiada en entornos de trabajo, pero no tienen ninguna utilidad en entornos domésticos.
- ET POP3: Una nueva categoría dedicada a defender servidores de correo e informar de actividad no maliciosa.
- ET RPC: Igual que en el caso de FTP, estas reglas detectan ataques hacia un protocolo que no estará abierto por defecto. Por tanto, se excepcionarán las reglas de conexiones entrantes.
- ET SCADA: Estas reglas están relacionadas con el entorno industrial.
- ET SCAN: Debido a que los hosts internos no se pueden detectar, se excepcionarán las reglas para conexiones entrantes. Este tipo de actividad también puede ser detectada desde un equipo infectado que intenta infectar otros equipos, por lo que las conexiones internas sospechosas seguirán generando alertas.
- ET SMTP: Otra categoría relacionada con servidores de correo y actividad no maliciosa.
- ET SQL: De nuevo, se trata de un tipo de servicio que no se ofrecerá desde la red doméstica de un usuario no técnico.
- ET TFTP: Igual que para ET FTP, sólo el tráfico interno será revisado.
- ET WEB_SERVER: Esta categoría está definitivamente diseñada para servicios no encontrados en una red doméstica: servicios web.
- ET WEB_SPECIFIC_APPS: Mismo caso que ET WEB_SERVER.

Las demás categorías quedarán explicadas en la sección siguiente, ya que se ha redactado una explicación sencilla (que no simple) para cada una de ellas.

3.5 Descripciones de las alertas por categoría

Se diseñan explicaciones[3] a nivel de usuario no técnico para las categorías de reglas que seguirán presentes tras deshabilitar las mencionadas en el apartado anterior. Es importante tener en cuenta que estas explicaciones tratan de ajustarse al nivel técnico de un usuario sin conocimientos previos:

[3] Los recursos mencionados son los sitios web de VirusTotal [29], AbuseIPDB [30], unas guías para bloquear IPs [31] o dominios [32] en Firewall de Windows, y tutoriales para mantener ActiveX actualizado [36], minimizar el daño de un ataque DOS [33], o bloquear NetBIOS [34] o Telnet [35]. En el programa final, cada consejo tiene un apartado final con los recursos que le corresponden.

Categoría de reglas: ET 3CORESec

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET ActiveX

Descripción: Alguien podría estar intentando atacar tu sistema mediante una vulnerabilidad en ActiveX. Los controles ActiveX son pequeñas aplicaciones de Internet Explorer, que sirven para mostrar contenido en algunos sitios web.

Instrucciones: Asegúrate de mantener ActiveX actualizado mediante la guía del enlace de Microsoft.

Consejo: Comprueba también la IP desde la que se ha hecho la conexión, introduciéndola en uno de los buscadores de los enlaces (VirusTotal, AbuseIPDB) o en otro buscador similar. Si está considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus. Aunque la mayoría de antivirus comprueban las posibles fuentes de malware en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Adware-PUP

Descripción: Se ha detectado actividad que puede señalar a la presencia de software no deseable como puede ser el adware. No suelen ser programas que pongan en peligro tu seguridad, pero pueden estar ralentizando tu equipo o haciendo que veas más anuncios de lo habitual o anuncios engañosos.

Instrucciones: Si no reconoces el nombre de la regla como un programa que deseas legítimamente en tu equipo, localiza el programa (puede que el antivirus te ayude) o infórmate sobre el método de borrado del mismo.

Consejo: Si se trata de un programa que utilizas activamente, puedes añadir una excepción a la regla;

Categoría de reglas: ET Attack Response

Descripción: Se ha detectado actividad similar a la que se ve cuando un equipo infectado se comunica con este atacante. Esta regla detecta cuándo el equipo

responde a una conexión con las mismas características que en ciertos ataques conocidos.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Botcc

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o

de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Botcc Portgrouped

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban

los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET CIArmy

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Coinmining

Descripción: Se ha detectado actividad similar a la que se ve cuando un equipo infectado está siendo utilizado para minar criptomonedas. Esto suele provocar la ralentización del equipo, y además significa que un atacante tiene una vía de entrada al equipo que en el futuro podría utilizar para actividad más intrusiva.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Compromised

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad

maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Current Events

Descripción: Para este caso, tendrás que fiarte del nombre de la alerta, ya que esta categoría abarca varios tipos de amenaza (direcciones IP o dominios que se saben maliciosos, explotación de vulnerabilidades…).

Consejo: Ten en cuenta que estas alertas se basan en indicadores que cambian cada poco tiempo, así que puedes buscar la regla para ver la fecha en la que se creó (created_at) o actualizó (updated_at) por última vez. Si se trata de una alerta con más de 6 meses de antigüedad, puedes descartarla directamente.

Categoría de reglas: ET DNS

Descripción: Se han detectado accesos o intentoa de acceso a sitios web sospechosos o con características sospechosas.

Instrucciones: Si has accedido voluntariamente a un sitio web con las características mencionadas por la regla, busca información y contrasta que sea legítimo con los recursos de VirusTotal, AbuseIPDB u otros repositorios similares. Si no has accedido por tu cuenta, comprueba el estado de tu equipo con un escaneo del antivirus ya que podría ser una petición hecha por malware dentro de tu equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET DOS

Descripción: Parece que alguien podría estar intentando sobrecargar tu router para evitar que pueda funcionar correctamente.

Instrucciones: Sigue las instrucciones del primer enlace para mejorar tus posibilidades contra un ataque DoS.

Consejo: Si el ataque viene de una IP origen considerada como maliciosa en las fuentes de los enlaces (VirusTotal, AbuseIPDB), puedes aprovechar para bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Categoría de reglas: ET Drop

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una

web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Dshield

Descripción: Se ha producido una conexión a una IP catalogada como posiblemente maliciosa. Esto puede significar que has intentado acceder a un sitio web malicioso sin saberlo, o que hay un archivo de malware en tu equipo intentando conectarse con el atacante que lo creó.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Esta regla puede saltar por error cuando una IP fue catalogada como maliciosa en el pasado pero ha sido reutilizada desde entonces para cosas más normales. Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Exploit

Descripción: Parece que alguien podría estar intentando aprovechar una vulnerabilidad en tu sistema. Esta regla se da cuando una conexión tiene las mismas características que las conexiones maliciosas que atacan cierto programa concreto

Instrucciones: Si tienes el programa mencionado en la alerta, comprueba que tienes la última versión (ya que muchas de las actualizaciones de los programas son actualizaciones de seguridad). En caso de tratarse de una IP origen considerada como maliciosa en las fuentes referidas (VirusTotal, AbuseIPDB), puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus por si el equipo que realiza el escaneo estuviese infectado de malware.

Consejo: Aunque la mayoría de antivirus comprueban los archivos las posibles fuentes de malware llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Exploit-Kit

Descripción: Parece que alguien podría estar intentando atacar tu sistema. Esta alerta se da cuando hay conexiones muy similares a las que producen ciertos programas que buscan diversas vulnerabilidades.

Instrucciones: En caso de tratarse de una IP origen considerada como maliciosa en las fuentes referidas (VirusTotal, AbuseIPDB), puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus por si el equipo que realiza el escaneo estuviese infectado de malware. Aunque la mayoría de antivirus comprueban las posibles fuentes de malware en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET JA3

Descripción: Se ha detectado actividad igual a la que se ve cuando un equipo infectado se comunica con este atacante. Se ha accedido a un sitio que tiene unas características muy similares a las del atacante mencionado en el título de la alerta.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado.

Esta categoría concreta provoca falsos positivos a menudo, por lo que si tienes cierta certeza de que la alerta está causada por webs o programas legítimos, puedes excepcionar esta alerta para ellos. De lo contrario, comprueba que sean benignos escaneando el programa sospechoso con el antivirus o buscando información sobre la web sospechosa. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para URLs o incluso archivos.Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Malware

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un equipo infectado.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Misc

Descripción: Para este caso, tendrás que fiarte del nombre de la alerta, ya que esta categoría abarca varios tipos de amenaza (direcciones IP o dominios que se saben maliciosos, explotación de vulnerabilidades…).

Consejo: Si el mismo equipo ha producido otras alertas recientemente, puedes seguir los Instruccioness de estas. De lo contrario, tendrás que informarte lo mejor posible.

Categoría de reglas: ET Mobile Malware

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un móvil infectado.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba la legitimidad de las aplicaciones o sitios web que puedan haberla causado. Si has instalado recientemente aplicaciones desde fuera de la tienda oficial (App Store, Google Play…), considera desinstalar la aplicación en cuestión o busca en Internet quejas sobre la seguridad de la misma.

Categoría de reglas: ET NETBIOS

Descripción: Parece que alguien podría estar intentando atacar tu sistema mediante una vulnerabilidad en el protocolo NETBIOS. Este protocolo permite a ciertas aplicaciones la conexión con la red, pero a día de hoy está prácticamente obsoleto.

Instrucciones: Si crees que nunca has utilizado este protocolo, puedes deshabilitarlo mediante la guía del primer enlace, aunque se puede revertir si termina provocando problemas en alguna aplicación. Comprueba también la IP desde la que se ha hecho la conexión, introduciéndola en uno de los buscadores de los enlaces (VirusTotal, AbuseIPDB) o en otro buscador similar. Si está considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus por si uno estuviera infectado e intentando infectar al otro. Aunque la mayoría de antivirus comprueban las posibles fuentes de malware en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET P2P

Descripción: Se han detectado conexiones que indican el uso de una herramienta de compartición de datos P2P (enú ws, edonkey, etcétera). Aunque estas herramientas no son de por sí maliciosas, se utilizan a menudo para obtener contenido pirata. Debes tener en cuenta que la piratería es no sólo un delito, sino un riesgo grave a la seguridad. Recuerda que se ha calculado que más del 50% del contenido pirata que circula por Internet incluye alguna clase de malware o código malicioso. Piratear contenido supone una inversión de tiempo a quien lo hace, y es esperable que pretendan ganar algo a cambio (nada es realmente gratis).

Instrucciones: Evitar el uso de redes P2P para la obtención de contenido pirata.

Consejo: Si decides ignorar esta advertencia, puedes excepcionar esta alerta.

Categoría de reglas: ET Phishing

Descripción: Parece que podrías estar siendo víctima de phishing, es decir, de alguna clase de estafa por correo o similar.

Instrucciones: Comprueba las páginas a las que has accedido clickando en un enlace para asegurarte de que son los sitios que dicen ser, y en general que son fiables. Puedes introducir el enlace en VirusTotal para que sea analizado. Si has introducido tu cuenta de correo o de algún servicio en un sitio web que ahora te resulta sospechoso, cambia la contraseña de esa cuenta.

Categoría de reglas: ET SCAN

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un equipo infectado que intenta comprobar el estado de otros equipos de la red.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Shellcode

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un equipo infectado. Puede estar contactando con otro equipo para intentar infectarlo, o tal vez con una IP externa para intentar exfiltrar tu información o recibir órdenes.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por programas legítimos, pero has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus. En caso de encontrar una IP considerada como maliciosa en las fuentes referidas (VirusTotal o AbuseIPDB), puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo, o de los equipos en caso de ser internos tanto el origen como el destino. Aunque la mayoría de antivirus comprueban

los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET TELNET

Descripción: Parece que alguien podría estar intentando atacar tu sistema mediante una vulnerabilidad en el protocolo TELNET. Este protocolo permite a un equipo conectarse con otro de la misma red, pero a día de hoy está prácticamente obsoleto.

Instrucciones: Comprueba la IP desde la que se ha hecho la conexión, introduciéndola en uno de los buscadores de los enlaces (VirusTotal, AbuseIPDB) o en otro buscador similar. Si está considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus. Aunque la mayoría de antivirus comprueban las posibles fuentes de malware en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Consejo: Si crees que nunca has utilizado este protocolo, puedes deshabilitarlo en dispositivos Windows mediante la guía del primer enlace.

Categoría de reglas: ET TOR

Descripción: Se ha producido una conexión a una IP catalogada como nodo de la red TOR. Esta red P2P se utiliza a menudo en busca de anonimidad, y se conoce de múlcasiones en que los atacantes la utilizan. Forma parte de lo que se conoce como \” enú web\”.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado (aunque es difícil que un navegador corriente haya llegado a un nodo de la red TOR). Si no

tienes la certeza de que la alerta está causada por webs o programas legítimos, te recomendamos bloquear la IP en los dispositivos Windows siguiendo la guía del último enlace.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET Trojan

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un equipo infectado por un troyano. Esta clase de malware aparenta ser un programa legítimo pero, una vez ejecutado, habilita el control remoto del equipo por parte del atacante.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado (especialmente los programas). Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET User Agents

Descripción: Se ha detectado actividad desde un dispositivo o aplicación extraño. El User-Agent es un identificador del dispositivo o aplicación que realiza las conexiones, y el User-Agent de esta conexión no es el esperable en un navegador corriente. Es probable que esta conexión se haya hecho desde un programa distinto al navegador.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET VOIP

Descripción: Parece que alguien podría estar intentando atacar tu sistema mediante una vulnerabilidad en el protocolo VOIP, que permite realizar llamadas por Internet.

Instrucciones: Si no tienes la certeza de que la alerta está causada por webs o programas legítimos (Zoom, Teams, Meets…), pero has encontrado un archivo

sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para URLs, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya) caso de tratarse de una IP origen considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía del último enlace. Si ambas Ips son internas, comprueba el estado de los equipos con el antivirus. Aunque la mayoría de antivirus comprueban las posibles fuentes de malware en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

Categoría de reglas: ET WORM

Descripción: Se ha detectado actividad similar a las conexiones que se ven desde un equipo infectado.

Instrucciones: Intenta recordar la actividad que estabas haciendo en el momento de la alerta y comprueba los programas o sitios web que puedan haberla causado. Si no tienes la certeza de que la alerta está causada por webs o programas legítimos, sino que has encontrado un archivo sospechoso o has encontrado que accediste a una web sospechosa, comprueba el archivo con el antivirus o comprueba la web accedida buscando información sobre ella. Puedes usar los recursos VirusTotal y AbuseIPDB para consultar si una web ha sido detectada alguna vez cometiendo actividad maliciosa. VirusTotal también es útil para archivos, y si introduces la IP de la alerta te dirá si es sospechosa de malware (la alerta probablemente proviene de un archivo) o de phishing (proviene probablemente de navegación tuya). En caso de encontrar una web o una IP considerada como maliciosa en las fuentes referidas, puedes bloquearla en los dispositivos Windows siguiendo la guía de los dos últimos enlaces.

Consejo: Si no has localizado nada sospechoso, antes de excepcionar nada comprueba con el antivirus el estado del equipo por si la actividad proviniese de un malware oculto dentro del mismo equipo. Aunque la mayoría de antivirus comprueban los archivos en cuanto llegan al equipo, un escaneo pedido activamente por el usuario puede profundizar más y encontrar malware mejor escondido.

4. Implementación

Este apartado presenta la implementación final y configuración de la aplicación servidor y la aplicación cliente.

Se ha utilizado como servidor una Raspberry Pi 2, por disponibilidad. Como se ha mencionado, el NIDS elegido es Suricata por sus bajos requerimientos de hardware.

En cuanto a la arquitectura de red, finalmente no se ha podido implementar ninguna de las mencionadas, debido a que el router disponible presenta menos funcionalidades de las esperadas y no permite port mirroring.

En su lugar, las pruebas se llevarán a cabo utilizando un archivo .pcap, es decir, un archivo de captura de tráfico. El tráfico se capturará en el mismo equipo que lo genere, y se analizará mediante Suricata tras compartir el archivo .pcap con el servidor NIDS.

4.1 Suricata

Para excepcionar categorías enteras, se han añadido los archivos de `/etc/suricata/rules` relacionados con estas categorías en un nuevo fichero `/etc/suricata/disable.conf`.

Esto hace que, cada vez que se actualicen las reglas con el comando `suricata-update`, las reglas de estas categorías serán deshabilitadas.

Por su parte, para las categorías que no se deshabilitarán enteras, se han añadido al mismo fichero los identificadores de sus reglas entrantes.

El fichero disable.conf ha quedado como se muestra en la Ilustración 12:

```
group:emerging-games.rules
group:emerging-hunting.rules
group:emerging-icmp.rules
group:emerging-icmp_info.rules
group:emerging-imap.rules
group:emerging-inappropriate.rules
group:emerging-info.rules
group:emerging-p2p.rules
group:emerging-policy.rules
group:emerging-pop3.rules
group:emerging-scada.rules
group:emerging-scan.rules
group:emerging-shellcode.rules
group:emerging-smtp.rules
group:emerging-snmp.rules
group:emerging-sql.rules
group:emerging-web_server.rules
group:emerging-web_specific_apps.rules
2010732
2010733
2010734
2010735
2010736
2010737
2010738
2010739
2010740
2002851
2009981
2009982
2009983
2009984
2009985
2010081
2010731
2002850
2012051
```

Ilustración 12: Contenido de disable.conf

Con esto, la ejecución del actualizador `suricata-update` respetará la nueva configuración en la que todas estas reglas se deshabilitan. La ejecución de `suricata-update` dará un resultado parecido a la Ilustración 13:

```
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2045882] ET WEB_SPECIFIC_APPS WordPress - Attempted Check for Malicious posts-layout (post-layout Doppelgange
r) Plugin
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2045883] ET WEB_SPECIFIC_APPS Wordpress - Successful Check for Malicious posts-layout (post-layout Doppelgang
er) Plugin - Infected Web Server
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2045881] ET WEB_SPECIFIC_APPS Wordpress - posts-layout (post-layout Doppelganger) Plugin Activation
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046053] ET WEB_SPECIFIC_APPS MOVEit File Transfer - HTTP POST to /moveitaspi.dll (CVE-2023-34362)
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046054] ET WEB_SPECIFIC_APPS MOVEit File Transfer - HTTP POST to /guestaccess.aspx (CVE-2023-34362)
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046055] ET WEB_SPECIFIC_APPS MOVEit File Transfer - HTTP POST to /api/v1/folders (CVE-2023-34362)
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046188] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Set Session Variables - Guest Account Creation - CVE-202
3-34362 Stage 1a
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046189] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Set Session Variables - SQLi Payload Creation - CVE-2023
-34362 Stage 1b
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046190] ET WEB_SPECIFIC_APPS MOVEit File Transfer - CSRF Token Request on guestaccess.aspx - CVE-2023-34362
Stage 1b
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046191] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Successful CSRF Token Request on guestaccess.aspx - CVE-
2023-34362 Stage 1b
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046192] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Trigger SQL Injection via guestaccess.aspx - CVE-2023-34
362 Stage 2
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046193] ET WEB_SPECIFIC_APPS MOVEit File Transfer - API Token Request - CVE-2023-34362 Stage 3
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046195] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Folder Request - CVE-2023-34362 Stage 4
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046197] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Set Session Variables - SQLi Payload Creation - CVE-2023
-34362 Stage 5a
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046198] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Payload Trigger Request - CVE-2023-34362 Stage 5b
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046194] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Successful API Token Request - CVE-2023-34362 Stage 3
20/6/2023 -- 12:01:22 - <Debug> -- Disabling: [1:2046196] ET WEB_SPECIFIC_APPS MOVEit File Transfer - Successful Folder Request - CVE-2023-34362 Stage 4
20/6/2023 -- 12:01:28 - <Info> -- Disabled 13335 rules.
20/6/2023 -- 12:01:28 - <Info> -- Enabled 0 rules.
20/6/2023 -- 12:01:28 - <Info> -- Modified 0 rules.
20/6/2023 -- 12:01:28 - <Info> -- Dropped 0 rules.
```

Ilustración 13: Extracto del resultado de ejecutar suricata-update

Curiosamente, la ruta a `disable.conf` no necesita ser establecida en el fichero de configuración `suricata.yaml`, si el fichero `disable.conf` se ha creado en `/etc/suricata`. Lo que sí se ha de concretar en `suricata.yaml` es la ruta a los ficheros de reglas que se utilizarán, dejando los campos `default-rule-path` y `rule-files` como se muestra en la Ilustración 14. La ruta es la que contiene el fichero `suricata.rules` con las reglas de

Emerging Threats, tal y como las descarga el comando `suricata-update`. Esta ruta es distinta de la ruta por defecto, que hubiera sido `/etc/suricata/rules`:

```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - local.rules
```

Ilustración 14: Configuración en suricata.yaml

Adicionalmente, se incluye el fichero local.rules, que se utilizará como fichero de excepciones para las reglas que excepcione el usuario.

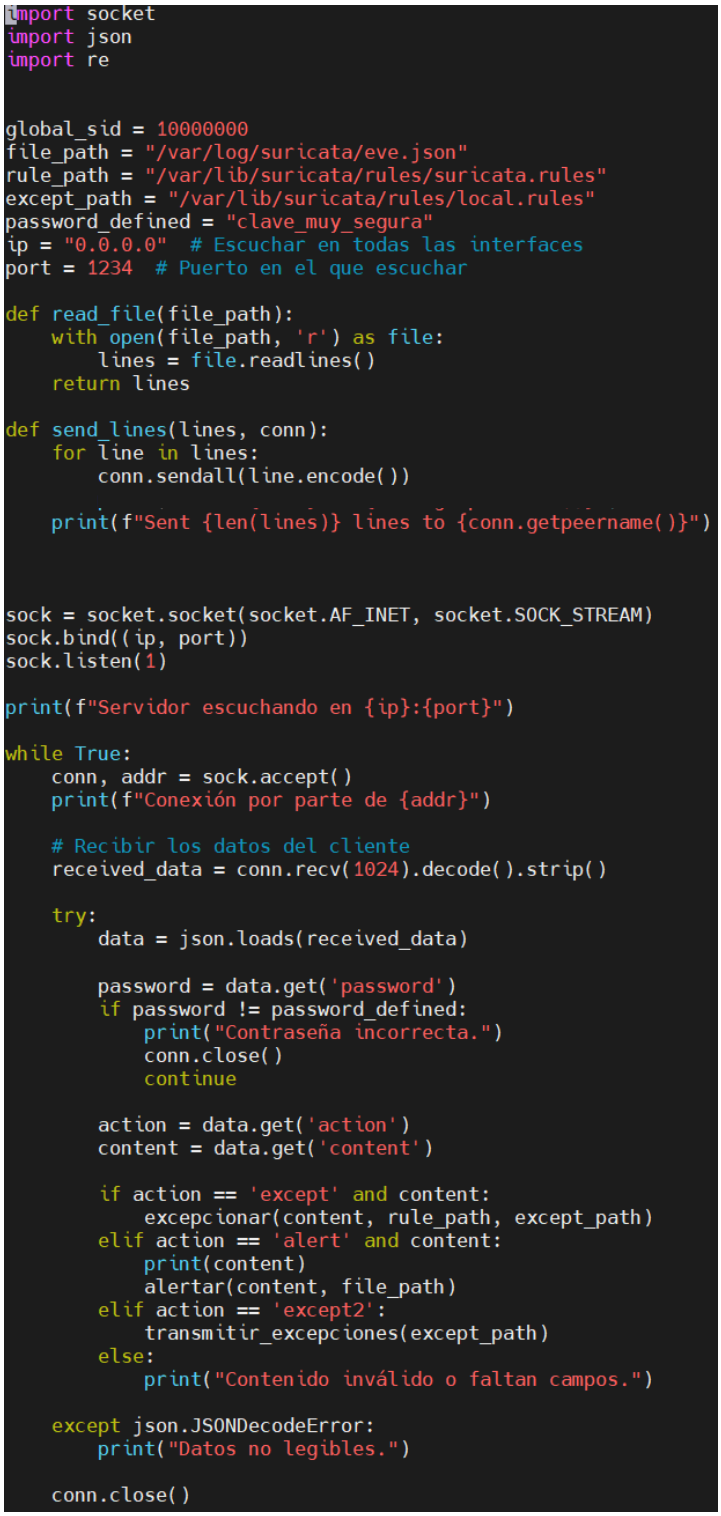
4.2 Capa de transporte en el servidor

El servidor está preparado para aceptar peticiones de cualquier cliente. Sin embargo, la petición debe incluir entre sus campos una contraseña concreta para verificar que el cliente tiene acceso.

El servidor utiliza un socket (Ilustración 15[4]) que se mantiene a la escucha de conexiones desde clientes de la red, y en cada conexión vendrán en formato JSON la contraseña, un tag con el caso de uso (`alert` para mostrar alertas, `except` para añadir excepciones y `except2` para mostrar excepciones) y la información necesaria para gestionar el caso de uso.

Se accede según sea necesario al fichero de reglas (`rule_path`), de excepciones (`exception_path`), y/o de alertas (`file_path`).

[4] La ilustración muestra una versión del código en la que las funciones `excepcionar`, `alertar` y `transmitir_excepcion` serán definidas más abajo. Por el funcionamiento de Python, en la versión final del código estas funciones están definidas antes que el bucle `while True:` pero se ha mantenido la imagen por claridad para separar correctamente los subapartados.



```python
import socket
import json
import re


global_sid = 10000000
file_path = "/var/log/suricata/eve.json"
rule_path = "/var/lib/suricata/rules/suricata.rules"
except_path = "/var/lib/suricata/rules/local.rules"
password_defined = "clave_muy_segura"
ip = "0.0.0.0"  # Escuchar en todas las interfaces
port = 1234  # Puerto en el que escuchar

def read_file(file_path):
    with open(file_path, 'r') as file:
        lines = file.readlines()
    return lines

def send_lines(lines, conn):
    for line in lines:
        conn.sendall(line.encode())

    print(f"Sent {len(lines)} lines to {conn.getpeername()}")



sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.bind((ip, port))
sock.listen(1)

print(f"Servidor escuchando en {ip}:{port}")

while True:
    conn, addr = sock.accept()
    print(f"Conexión por parte de {addr}")

    # Recibir los datos del cliente
    received_data = conn.recv(1024).decode().strip()

    try:
        data = json.loads(received_data)

        password = data.get('password')
        if password != password_defined:
            print("Contraseña incorrecta.")
            conn.close()
            continue

        action = data.get('action')
        content = data.get('content')

        if action == 'except' and content:
            excepcionar(content, rule_path, except_path)
        elif action == 'alert' and content:
            print(content)
            alertar(content, file_path)
        elif action == 'except2':
            transmitir_excepciones(except_path)
        else:
            print("Contenido inválido o faltan campos.")

    except json.JSONDecodeError:
        print("Datos no legibles.")

    conn.close()
```

Ilustración 15: Servidor – Valores por defecto y conectividad

En la Ilustración 15 se pueden ver las librerías importadas, seguidas de la definición de ciertas variables globales y dos funciones sencillas definidas por claridad del código posterior. Después, se inicia el socket de conexión y se reciben peticiones, comprobando el caso de uso al que corresponden.

4.2.1 Caso de uso: obtención de alertas recientes

El primer caso de uso es que el cliente pida obtener las alertas nuevas. Para este caso, el cliente proveerá como content la fecha y hora de la última alerta que ha recibido.

```
    try:
        data = json.loads(received_data)

        password = data.get('password')
        if password != password_defined:
            print("Contraseña incorrecta.")
            conn.close()
            continue

        type = data.get('type')
        content = data.get('content')

        if type == 'except' and content:
            excepcionar(content, rule_path, except_path)
        elif type == 'alert' and content:
            with open(file_path, 'r') as file:
                lines = file.readlines()
                for line in lines:
                    if content in line:
                        starting_line = line.strip()
                        break
                else:
                    starting_line = None

            if starting_line:
                index = lines.index(starting_line)
                new_lines = lines[index + 1:]
            else:
                new_lines = lines
            if new_lines:
                send_lines(new_lines, conn)
        else:
            print("Contenido inválido o faltan campos.")

    except json.JSONDecodeError:
        print("Datos no legibles.")

    conn.close()
```

Ilustración 16: Servidor – Caso de uso de enviar nuevas alertas

Como se ve en la Ilustración 16, en caso de encontrarse en el fichero leído una alerta de dicha hora, se enviarán todas las alertas posteriores. De lo contrario, se enviarán todas las alertas almacenadas en el fichero de logs. El fichero eve.log, concretamente,

almacena su contenido en backups para empezar de cero cada cierto tiempo, por lo que no llegará a exceder un tamaño razonable una vez configurado para sólo almacenar alertas.

4.2.2 Caso de uso: obtención de excepciones

Para este caso de uso, en lugar de enviar las excepciones más nuevas como en el caso de las alertas, se ha considerado más apropiado enviar todas las excepciones cada vez que el cliente las pida. Para este caso no hay contenido en la variable content, y las excepciones han de pasar por cierto formateo (Ilustración 17) para convertirse en campos separados por punto y coma que serán utilizados por el cliente para construir visualmente la excepción. Estos campos corresponden a la regla, IP origen, puerto origen, IP destino y puerto destino de la excepción.

```
def transmitir_excepciones(except_path):
        with open(except_path, 'r') as file:
            lines = file.readlines()
        exceptions = []
        for line in lines:
            values = re.findall(r'[\w.-]+', line)
            rule = re.search(r'msg:"(.*?)";', line).group(1)
            src_ip = values[2]
            src_port = values[3]
            dst_ip = values[5]
            dst_port = values[6]

            data = {
                    "signature": rule,
                    "src_ip": src_ip,
                    "src_port": src_port,
                    "dst_ip": dst_ip,
                    "dst_port": dst_port
                    }

            json_line = json.dumps(data)
            exceptions.append(json_line+"\n")
        if exceptions:
            send_lines(exceptions, conn)
```

Ilustración 17: Servidor – caso de uso de transmitir excepciones

4.2.3 Caso de uso: añadir excepciones

En caso de tratarse de una petición de añadir excepción, el contenido serán los campos (separados por punto y coma): identificador, IP origen, puerto origen, IP destino, puerto destino.

```python
def excepcionar(datos, fichero_reglas, fichero_excepciones):
    global global_sid
    # Extraer los campos
    fields = datos.split(';')
    print (fields)
    sid, src_ip, src_port, dst_ip, dst_port = fields

    # Leer el fichero de reglas en busca de la regla con el SID adecuado
    with open(fichero_reglas, "r") as file:
        lines = file.readlines()
    line_to_update = None
    for i in range(len(lines)):
        if sid in lines[i]:
            line_to_update = lines[i].strip()
            break

    if line_to_update is not None:
        # Gestiones varias del formato
        alert_index = line_to_update.index("alert ")
        line_parts = line_to_update[alert_index:].split()
        # Aquí se sustituyen los campos presentes
        line_parts[0] = "pass"
        if src_ip:
            line_parts[2] = src_ip
        if src_port:
            line_parts[3] = src_port
        if dst_ip:
            line_parts[5] = dst_ip
        if dst_port:
            line_parts[6] = dst_port

        # Se vuelve a juntar todo en una línea
        wrong_line = line_to_update[:alert_index] + " ".join(line_parts)
        # y se actualiza el SID para evitar conflictos
        pattern = r'sid:(\d+),'
        replacement = r'sid:{},'.format(global_sid)
        new_line = re.sub(pattern, replacement, wrong_line)

        # Se añade la nueva línea al fichero de excepciones
        with open(fichero_excepciones, "a") as file:
            file.write(new_line + '\n')
        global_sid += 1
        subprocess.run("suricatasc -c reload-rules", shell=True, check=False)
    else:
        print("No se ha encontrado la regla a excepcionar.")
```

Ilustración 18: Servidor – Caso de uso de añadir excepción

Como se ve en la Ilustración 18, si el identificador (SID) se encuentra en el fichero de reglas, se utilizará el formato de esta regla actualizando los campos provenientes del cliente y cambiando la acción a pass, y se añadirá al fichero de excepciones con un SID nuevo para evitar conflicto con la regla ya existente. Una vez insertada la nueva excepción, se recargan las reglas de Suricata para que se aplique.

4.3 Actualización de las reglas del NIDS

El sistema NIDS debe actualizar sus reglas periódicamente, ya que cada día se descubren nuevos IoC (del inglés *Indicator Of Compromise*, indicador de compromiso), muchos de los cuales se añaden a las reglas de Emerging Threats.

Para ello, en el caso del proyecto (una Raspberry Pi con Linux/RaspberryOS) se establece una tarea en crontab con el comando que se puede ver en la Ilustración 19:

```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 5 * * * suricata-update --no-test; suricatasc -c reload-rules
```

Ilustración 19: crontab con comando suricata-update cada mañana a las 5

El comando lleva la opción –no-test para evitar un error por el que, al comprobarse el resultado, algunas actualizaciones exitosas pueden ser revertidas al finalizar.

Después de actualizar las reglas desde el repositorio, se recargan las reglas locales para aplicar los cambios.

4.4 Cliente Android

Para programar la aplicación de móvil, se ha utilizado el SDK de Android en Android Studio [26]. Se han creado diversas vistas en archivos de recursos, concretamente en archivos de *layouts*, archivos en los que se especifica la disposición o colocación de los distintos elementos. El resultado final se expone en el apartado 5.2 Casos de uso de la aplicación

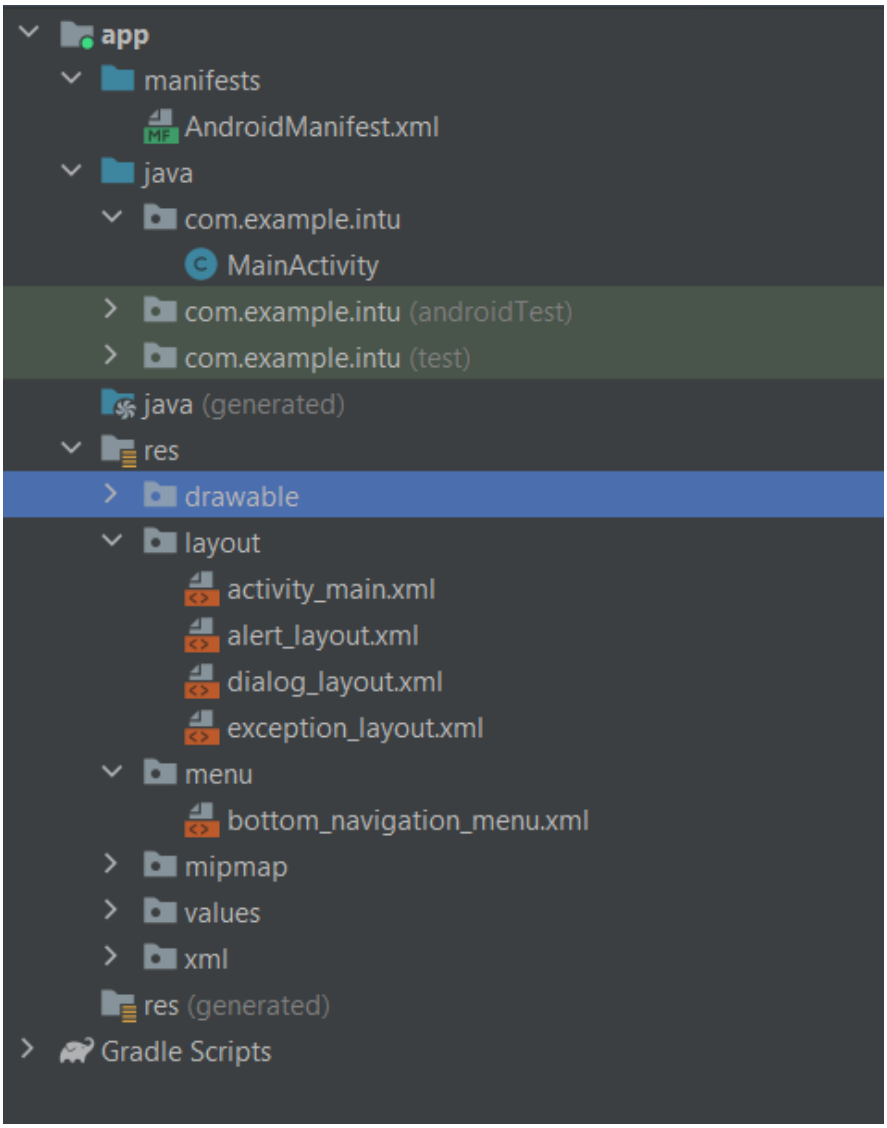


Ilustración 20: Estructura de la aplicación – archivos más relevantes

La Ilustración 20 muestra la estructura de la aplicación, con los archivos que se han creado o modificado durante su desarrollo. Los archivos de *layout* y *50enú* contienen el diseño de los elementos, mientras que el archivo de java contiene la lógica y transporte de la aplicación y referencia estos elementos para asignarles propiedades.

En la Ilustración 21 se puede ver el esqueleto de la aplicación (técnicamente el código que se ejecuta al abrirla), con referencias a variables declaradas anteriormente (líneas

1-36, no incluidas) y con algunos métodos comprimidos (líneas 56, 62, 68 y 91) que se comentarán y/o se mostrarán expandidas más adelante.

Ilustración 21: Esqueleto de la interfaz

Lo que está ocurriendo en el código de la imagen es:

- Líneas 41 a 46: las variables globales `host`, `port` y `pass` se inicializan usando su último valor guardado (la última vez que se abrió la aplicación) o se inicializan a un valor por defecto. Esto evitará tener que introducir la dirección y puerto del servidor o la contraseña cada vez que se abra la aplicación.
- Líneas 48 a 55: se asignan a variables ciertos elementos de los archivos de layout, para poder utilizarlos en el código Java.
- Líneas 56 (y ocultas), 62 (y ocultas), 68 (y ocultas): se establece la utilidad de ciertos botones. Concretamente, `alertButton` y `exceptButton` llaman a los métodos correspondientes a los botones CARGAR NUEVAS de la pestaña de alertas y de excepciones, respectivamente. Por su parte, `saveButton` está implementado directamente sobre el método `onCreate`, y lo que hace es sustituir las variables `host`, `port` y `pass`, así como sus contrapartes persistentes mediante el editor creado en la línea 43.
- Líneas 90, 91 y ocultas: Como se ve en la Ilustración 22, se trata de las pestañas de la aplicación, controladas por botones cada uno de los cuales provoca la desaparición de la pestaña actual con `setVisibility(View.GONE)` y la aparición del layout deseado con `setVisibility(View.VISIBLE)`.

```
92          @Override
93          public void onTabSelected(TabLayout.Tab tab) {
94              // Handle tab selection
95              int position = tab.getPosition();
96              switch (position) {
97                  case 0:
98                      // Alertas tab selected
99                      alertasView.setVisibility(View.VISIBLE);
100                     excepcionesView.setVisibility(View.GONE);
101                     configView.setVisibility(View.GONE);
102                     //alertasLayout.setVisibility(View.VISIBLE);
103                     //excepcionesLayout.setVisibility(View.GONE);
104                     break;
105                 case 1:
106                     alertasView.setVisibility(View.GONE);
107                     excepcionesView.setVisibility(View.VISIBLE);
108                     configView.setVisibility(View.GONE);
109                     //excepcionesLayout.setVisibility(View.VISIBLE);
110                     //alertasLayout.setVisibility(View.GONE);
111                     break;
112                 case 2:
113                     // Configuración tab selected
114                     alertasView.setVisibility(View.GONE);
115                     excepcionesView.setVisibility(View.GONE);
116                     configView.setVisibility(View.VISIBLE);
117                     break;
118             }
119         }
```

Ilustración 22: Pestañas de la aplicación

Se muestra ahora, en la Ilustración 23, el código de `alertButtonClicked()`, el método al que llama el botón CARGAR NUEVAS de la pestaña Alertas. Se explicará su funcionamiento y se señalarán las diferencias en los métodos de los otros casos de uso (obtención de excepciones o CARGAR NUEVAS en la pestaña Excepciones, y adición de excepción o AÑADIR en el diálogo de excepción).

```
274        new Thread(new Runnable() {
275            @Override
276            public void run() {
277                try {
278                    Socket socket = new Socket(host, port);
279                    OutputStream outputStream = socket.getOutputStream();
280
281                    JSONObject json = new JSONObject();
282                    json.put( name: "password", pass);
283                    json.put( name: "action",  value: "alert");
284                    json.put( name: "content", lastDate);
285                    String jsonStr = json.toString();
286
287                    outputStream.write(jsonStr.getBytes());
288
289                    InputStream inputStream = socket.getInputStream();
290                    BufferedReader reader = new BufferedReader(new InputStreamReader(inputStream));
291                    String line;
292                    JSONObject response;
293                    while ((line = reader.readLine()) != null) {
294                        response = new JSONObject(line);
295                        processAlert(response);
296                    }
297                    outputStream.close();
298                    reader.close();
299                    socket.close();
300                } catch (IOException | JSONException e) {
301                    e.printStackTrace();
302                }
303            }
304        }).start();
```

Ilustración 23: Conectividad en el botón de alertas

Se abre un nuevo hilo (líneas 274, 275, 303 y 304) para no dejar la interfaz visual colgada durante la comunicación. En este hilo, se abre un socket hacia el servicio de Python en el servidor. Se envía al servidor la contraseña, el código de acción alert, y la última fecha de la que se tiene una alerta (por defecto es el 1 de enero de 1970, por lo que por defecto se enviarán todas las alertas del archivo).

En el caso de querer añadir una excepción, el contenido enviado será el contenido de los campos de texto editable en el diálogo que se abre al pedir añadir una excepción (dialog_layout en la *Ilustración* 20), y en el caso de pedir todas las excepciones al servidor, el contenido será vacío (“”) pero se eliminarán todos los rectángulos de excepción mostrados hasta el momento.

Como se podrá ver en la Ilustración 24, para añadir cada una de las nuevas alertas del bucle (líneas 293 a 296), el método processAlert simplemente llama al método addRectangle[5] que veremos a continuación, enviándole las variables JSON de la respuesta.

[5] addRectangle recibe este nombre porque originalmente se iba a compartir un mismo layout “Rectángulo” para alertas y excepciones. Finalmente no fue así, por lo que cualquier referencia a un rectángulo en el código se refiere al tipo de rectángulo que muestra una alerta, no una excepción.

Ilustración 24: Mostrar la alerta en el hilo principal

La importancia de llamar a este método addRectangle desde un método aparte processAlert es que debe ser llamado desde el hilo original en el que está la interfaz visual (líneas 315 a 318 y sus respectivos cierres '}' 331 a 333).

Cabe mencionar que el método tips() de la línea 326, mostrado parcialmente en la Ilustración 25, es una simple recopilación de los consejos redactados en el apartado 3.5 de forma que el título de la alerta determine el consejo que se da. Concretamente, es la segunda palabra después de "ET" la que lo determina (ver 2.2.2 para más información sobre el formato de los títulos de Emerging Threats)

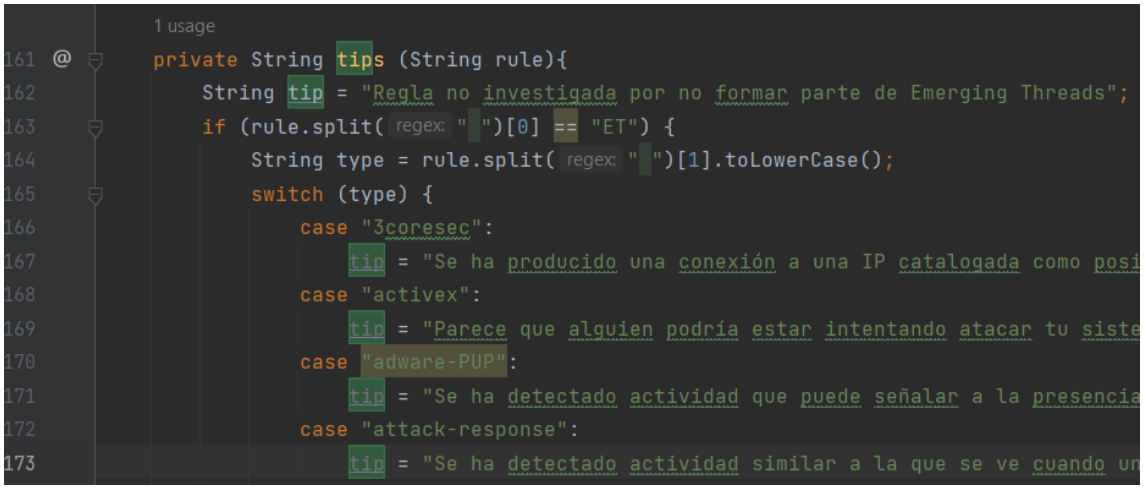


Ilustración 25: Método para los consejos

Para recibir las excepciones del servidor, el funcionamiento es similar. Por su parte, para enviar una nueva excepción, se llama al método processExcept análogo a processAlert una vez la comunicación ha terminado, para reflejar la nueva excepción en la interfaz visual sin tener que llamar al método que las actualiza todas desde servidor.

```
134     private void addRectangle(String date, String src_ip_port, String dst_ip_port, String regla, String tip) {
135         LayoutInflater inflater = LayoutInflater.from( context: this);
136         View rectangleView = inflater.inflate(R.layout.alert_layout, alertasLayout,  attachToRoot: false);
137
138         TextView fecha = rectangleView.findViewById(R.id.fecha);
139         TextView ip_puerto_origen = rectangleView.findViewById(R.id.ip_puerto_origen);
140         TextView ip_puerto_destino = rectangleView.findViewById(R.id.ip_puerto_destino);
141         TextView regla_texto = rectangleView.findViewById(R.id.rule);
142         TextView consejo = rectangleView.findViewById(R.id.consejo);
143         Button expandButton = rectangleView.findViewById(R.id.expandButton);
144
145         fecha.setText("Fecha: " + date);
146         ip_puerto_origen.setText("IP y puerto origen: " + src_ip_port);
147         ip_puerto_destino.setText("IP y puerto destino: " + dst_ip_port);
148         regla_texto.setText("Regla: " + regla);
149         consejo.setText("Consejo: " + tip);
150
151         expandButton.setOnClickListener(new View.OnClickListener() {
152             @Override
153             public void onClick(View v) { toggleExpandableRectangle(rectangleView); }
156         });
157
158         alertasLayout.addView(rectangleView,  index: 0);
159     }
```

Ilustración 26: Añadir una alerta a la interfaz visual

El método addRectangle puede verse en la Ilustración 26, donde, tras unas primeras declaraciones e inicializaciones de variables (l. 135 a 143), se añade el texto apropiado a cada campo (145 a 149) y se establece que el botón MÁS/MENOS llame a la función toggleExpandableRectangle, que veremos en la Ilustración 27.

```
471 @   ivate void toggleExpandableRectangle(View rectangleView) {
472     LinearLayout expandedLayout = rectangleView.findViewById(R.id.expandedLayout);
473     Button excepcionarButton = rectangleView.findViewById(R.id.excepcionarButton);
474     excepcionarButton.setOnClickListener(new View.OnClickListener() {
475         @Override
476         public void onClick(View v) {
477             TextView rule = rectangleView.findViewById(R.id.rule);
478             String regla = rule.getText().toString();
479             String reglaFormat = regla.substring( beginIndex: regla.indexOf(":") + 2);
480             TextView ip_puerto_origen = rectangleView.findViewById(R.id.ip_puerto_origen);
481             String ip_puerto_origen_string = ip_puerto_origen.getText().toString();
482             String ip_puerto_origenFormat = ip_puerto_origen_string.substring( beginIndex: ip_puerto_origen_string.indexOf(":") + 2);
483             String ip_origen = ip_puerto_origenFormat.split( regex: ":")[0];
484             String puerto_origen = ip_puerto_origenFormat.split( regex: ":")[1];
485             TextView ip_puerto_destino = rectangleView.findViewById(R.id.ip_puerto_destino);
486             String ip_puerto_destino_string = ip_puerto_destino.getText().toString();
487             String ip_puerto_destinoFormat = ip_puerto_destino_string.substring( beginIndex: ip_puerto_destino_string.indexOf(":") + 2)
488             String ip_destino = ip_puerto_destinoFormat.split( regex: ":")[0];
489             String puerto_destino = ip_puerto_destinoFormat.split( regex: ":")[1];
490             newExceptionDialog(reglaFormat, ip_origen, puerto_origen, ip_destino, puerto_destino);
491         }
492     });
493     if (expandedLayout.getVisibility() == View.VISIBLE) {
494         expandedLayout.setVisibility(View.GONE);
495         excepcionarButton.setVisibility(View.GONE);
496     } else {
497         expandedLayout.setVisibility(View.VISIBLE);
498         excepcionarButton.setVisibility(View.VISIBLE);
499     }
```

Ilustración 27: Cambio entre versión resumida y versión compleja de la alerta

Tras declarar variables desde los archivos de layout (l. 472 y 473), se programa la utilidad del botón de excepcionar (l. 474 a 492, que consiste en crear un diálogo de excepción con los campos por defecto que tiene la alerta) y se muestra u oculta tanto este botón como el layout que contiene el campo Consejo.

Como se ha mencionado, los demás casos de uso están programados de forma similar. El método más distinto, que merece especial mención, es `newExceptionDialog`, el método que disparan los botones Excepcionar de las Alertas y Editar de las Excepciones. Este método puede verse en la Ilustración 28:

```
381  private void newExceptionDialog(String regla_text, String ip_origen, String puerto_origen, String ip_destino, String puerto_destino) {
382      // Create a dialog builder
383      AlertDialog.Builder builder = new AlertDialog.Builder( context: MainActivity.this);
384      builder.setTitle("Añadir Excepción");
385
386      // Inflate the dialog layout
387      LayoutInflater inflater = getLayoutInflater();
388      View dialogView = inflater.inflate(R.layout.dialog_layout,  root: null);
389      builder.setView(dialogView);
390      EditText regla = dialogView.findViewById(R.id.rule);
391      EditText src_ip = dialogView.findViewById(R.id.src_ip);
392      EditText src_port = dialogView.findViewById(R.id.src_port);
393      EditText dst_ip = dialogView.findViewById(R.id.dst_ip);
394      EditText dst_port = dialogView.findViewById(R.id.dst_port);
395      regla.setText(regla_text);
396      src_ip.setText(ip_origen);
397      src_port.setText(puerto_origen);
398      dst_ip.setText(ip_destino);
399      dst_port.setText(puerto_destino);
400      // Set up the buttons
401      builder.setPositiveButton( text: "Añadir", new DialogInterface.OnClickListener() {
402          @Override
403          public void onClick(DialogInterface dialog, int which) {
404              // Handle añadir button click
405              // Retrieve data from the text boxes
406              String reglaText = regla.getText().toString();
407              String ip_origen = src_ip.getText().toString();
408              String puerto_origen = src_port.getText().toString();
409              String ip_destino = dst_ip.getText().toString();
410              String puerto_destino = dst_port.getText().toString();
411              newException(reglaText, ip_origen, puerto_origen, ip_destino, puerto_destino);
412              // Retrieve data from other text boxes similarly
413
414              // Perform necessary actions with the data
415          }
416      });
417
418      builder.setNegativeButton( text: "Cancelar", new DialogInterface.OnClickListener() {
419          @Override
420          public void onClick(DialogInterface dialog, int which) {
421              // Handle cancelar button click
422              dialog.dismiss();
423          }
424      });
425
426      // Show the dialog
427      AlertDialog dialog = builder.create();
428      dialog.show();
```

Ilustración 28: Diálogo de campos para nueva excepción

En las líneas 390 a 399, se establece que el texto por defecto en cada campo de texto editable tenga por defecto el texto de la regla o excepción desde la que se ha llamado al método.

En las líneas 401 a 424, se establece que el botón Añadir utilice el método `newException` para comunicarse con el servidor y añadir la nueva excepción a la interfaz, y que el botón Cancelar haga desaparecer el diálogo.

5. Pruebas

Se ha replicado el uso esperable de la aplicación para comentar las distintas fases de los casos de uso.

5.1 Detección de actividad

Por la arquitectura disponible, no se ha podido establecer ninguna de las situaciones en las que el servidor pueda recibir una copia de las conexiones. Para comprobar la efectividad de las reglas IDS, se ejecutará Suricata sobre un archivo de captura de paquetes (extensión .pcap, o .pcapng para PCAP New Generation) extraído mediante WireShark [27] de un equipo sobre el que se realizarán las pruebas o supuestos ataques. Esto simulará un entorno en el que el servidor tuviera acceso directo (port mirror, hub, etc.) a los paquetes que vayan desde el equipo y hacia el mismo.

Las pruebas se han realizado en un entorno controlado, y en los casos necesarios se ha impedido completamente el acceso a Internet desde router al que se conectan los equipos.

Los ataques que se van a probar son similares en categoría a algunos de los más llamativos entre los registrados por TrendMicro en 2017 [28]:

- TELNET Login con contraseña por defecto: Se instala un servidor Telnet [29] y se ataca desde un equipo con el cliente Telnet activado (por defecto en Windows viene deshabilitado). Se ha tratado de acceder sin contraseña varias veces y, tras acceder mediante la contraseña adecuada, se han ejecutado comandos que no funcionarían en el servidor Windows pero están relacionados con alertas de ET TELNET.
- Login por fuerza bruta mediante RDP: Tras activar el control remoto del equipo víctima, se accede desde el equipo atacante. Además de introducir varias contraseñas erróneas, viendo que la mayoría de alertas de Emerging Threats respecto a RDP son de DoS, se ha intentado simular este comportamiento accediendo y cortando la conexión varias veces en 30 segundos.
- MS17-010 SMB: Se intenta hacer login en SMB. Tras varios accesos denegados y credenciales erróneas, se transmite un paquete con un contenido extracto de una regla de EternalBlue (MS17-010)
- Ejecución de comandos en remoto por Shell Script: desde la propia conexión Telnet se abre un terminal CMD, desde el que se abre un terminal Powershell, desde el que se abre otro CMD. Es oportuno hacerlo desde Telnet ya que es tráfico no seguro y podrá ser leído por Suricata.

Esto ha dado lugar a varios paquetes .pcapng, que Wireshark permite *Fusionar* en uno solo (Ilustración 29).

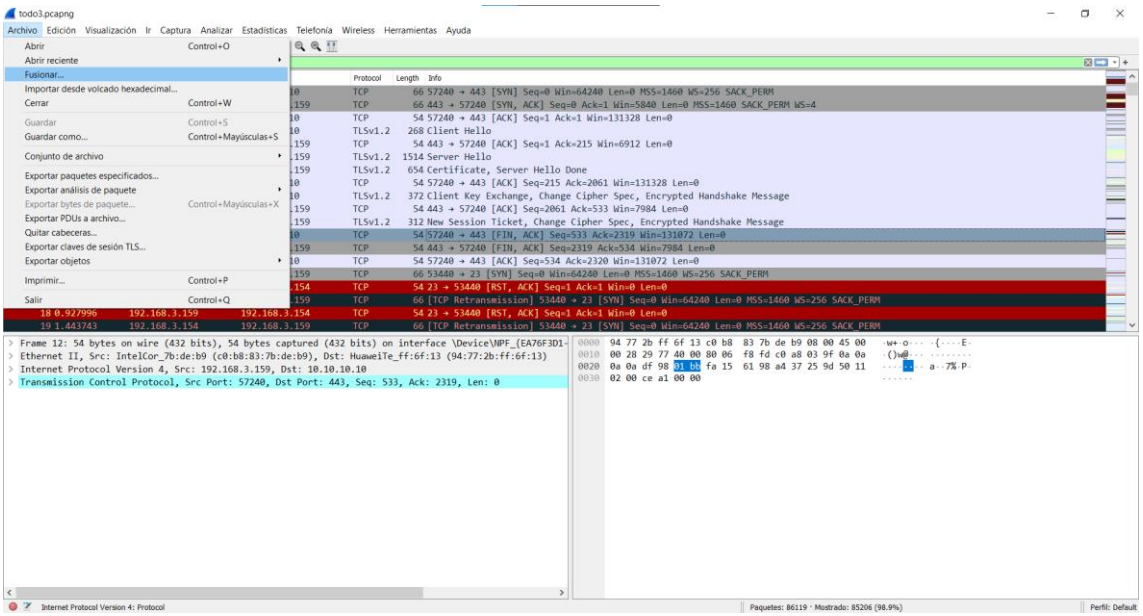


Ilustración 29: Wireshark con archivo abierto y la opción Fusionar resaltada

Este archivo .pcapng se transmite por SFTP al servidor NIDS, donde se analizará con Suricata.

Para ello, se ha utilizado el siguiente comando:

```
legnam@raspberrypi:~ $ sudo suricata -r todo3.pcapng -c suricata.yaml
28/6/2023 -- 16:46:52 - <Notice> - This is Suricata version 6.0.1 RELEASE running in USER mode
28/6/2023 -- 16:46:53 - <Error> - [ERRCODE: SC_ERR_STATS_LOG_GENERIC(278)] - eve.stats: stats are disabled globally: set stats.enabled to true. See https://su
ricata.readthedocs.io/en/suricata-6.0.1/configuration/suricata-yaml.html#stats
28/6/2023 -- 16:48:39 - <Notice> - all 5 packet processing threads, 2 management threads initialized, engine started.
28/6/2023 -- 16:48:46 - <Notice> - Signal Received.  Stopping engine.
28/6/2023 -- 16:48:48 - <Notice> - Pcap-file module read 1 files, 86119 packets, 46352108 bytes
```

Ilustración 30: Comando para analizar archivo .pcapng

Como se puede ver en la Ilustración 30, se especifica con la opción `-r` el archivo que se va a analizar, y se concreta con `-c` el archivo de configuración, en este caso una copia de suricata.yaml. Se ha hecho una copia por la necesidad de modificar el archivo para estas pruebas, ya que el atacante deberá ser considerado “externo”. Por eso el nuevo archivo suricata.yaml deberá tener el aspecto que se muestra en la Ilustración 31:

```
legnam@raspberrypi:~ $ head -50 suricata.yaml
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.3.159/32]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
    SQL_SERVERS: "$HOME_NET"
    DNS_SERVERS: "$HOME_NET"
    TELNET_SERVERS: "$HOME_NET"
    AIM_SERVERS: "$EXTERNAL_NET"
    DC_SERVERS: "$HOME_NET"
    DNP3_SERVER: "$HOME_NET"
    DNP3_CLIENT: "$HOME_NET"
    MODBUS_CLIENT: "$HOME_NET"
    MODBUS_SERVER: "$HOME_NET"
    ENIP_CLIENT: "$HOME_NET"
    ENIP_SERVER: "$HOME_NET"

  port-groups:
    HTTP_PORTS: "80"
    SHELLCODE_PORTS: "!80"
    ORACLE_PORTS: 1521
    SSH_PORTS: 22
    DNP3_PORTS: 20000
    MODBUS_PORTS: 502
    FILE_DATA_PORTS: "[$HTTP_PORTS,110,143]"
    FTP_PORTS: 21
    GENEVE_PORTS: 6081
    VXLAN_PORTS: 4789
    TEREDO_PORTS: 3544
```

Ilustración 31: Inicio del archivo suricata.yaml de pruebas

Una vez lanzado el comando de la Ilustración 30, se puede comprobar el resultado mirando las reglas de Emerging Threats que han saltado en eve.json:

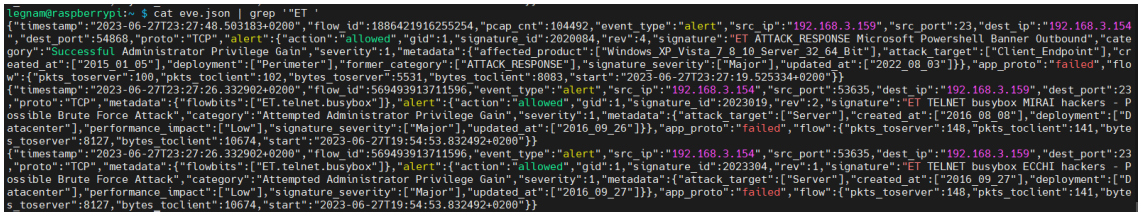


Ilustración 32: eve.json de pruebas

La Ilustración 32 puede resultar poco legible, por lo que se ha formateado el resultado con el comando de la Ilustración 33:

```
legnam@raspberrypi:~ $ cat eve.json | sed 's/.*signature":"//' | sed 's/".*//' | grep "ET "
ET TELNET busybox MIRAI hackers - Possible Brute Force Attack
ET TELNET busybox ECCHI hackers - Possible Brute Force Attack
ET ATTACK_RESPONSE Microsoft Powershell Banner Outbound
```

Ilustración 33: eve.json de pruebas clarificado

Se han detectado 2 alertas relativas a TELNET y una relativa a la iniciación de una Shell remota. Las dos primeras son por haber ejecutado comandos sospechosos relacionados con estos grupos de hackers MIRAI y ECCHI. La última es por haber abierto un Powershell controlado desde el exterior.

Por parte del resto de ataques simulados, se puede comprobar que unos reinicios manuales de conexión RDP o un archivo sin más contenido que una ristra de caracteres no hacen saltar unas reglas bien hechas como son las de Emerging Threats, y de hecho es buena señal porque indica que las reglas no saltarán a menudo con una actividad cualquiera en la que se usen estas tecnologías.

Es importante mencionar que sin buscar específicamente las reglas de Emerging Threats, aparecen múltiples alertas de SURICATA. Sería apropiado excepcionarlas por defecto, pero pueden servir como ejemplo de en qué casos es muy necesaria una excepción, tanto en el apartado 5.2 como en un posible tutorial (ver capítulo 7.Trabajos futuros).

5.2 Casos de uso de la aplicación

Se sustituye intencionalmente el archivo eve.json de la ruta por defecto de Suricata por el nuevo archivo eve.json generado. Así se podrán visualizar las alertas generadas en el apartado anterior:

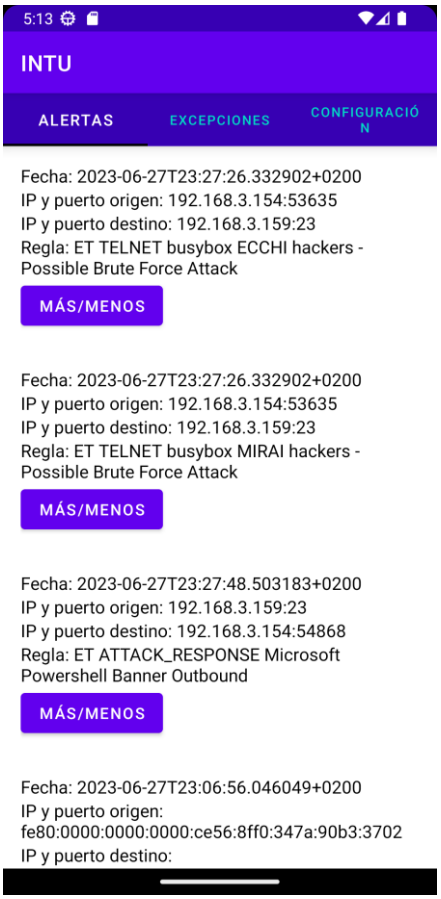


Ilustración 34: Alertas detectadas, vistas en la aplicación

La Ilustración 34 muestra las alertas detectadas en el apartado anterior, además de una de las alertas generadas por las reglas por defecto de Suricata.

Cada una de estas alertas puede ser aumentada para ver su consejo asociado y el botón de excepción, como se puede comprobar en la Ilustración 35:

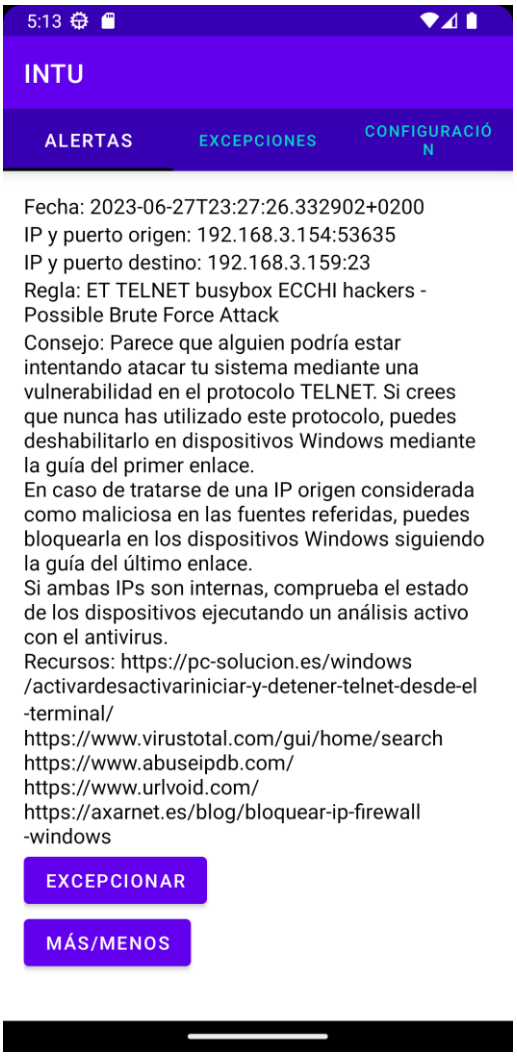


Ilustración 35: Alerta expandida, con su explicación

Aunque no todo es tan útil, ya que las alertas por defecto de tipo SURICATA superan enormemente en número a las de ET (Emerging Threats).

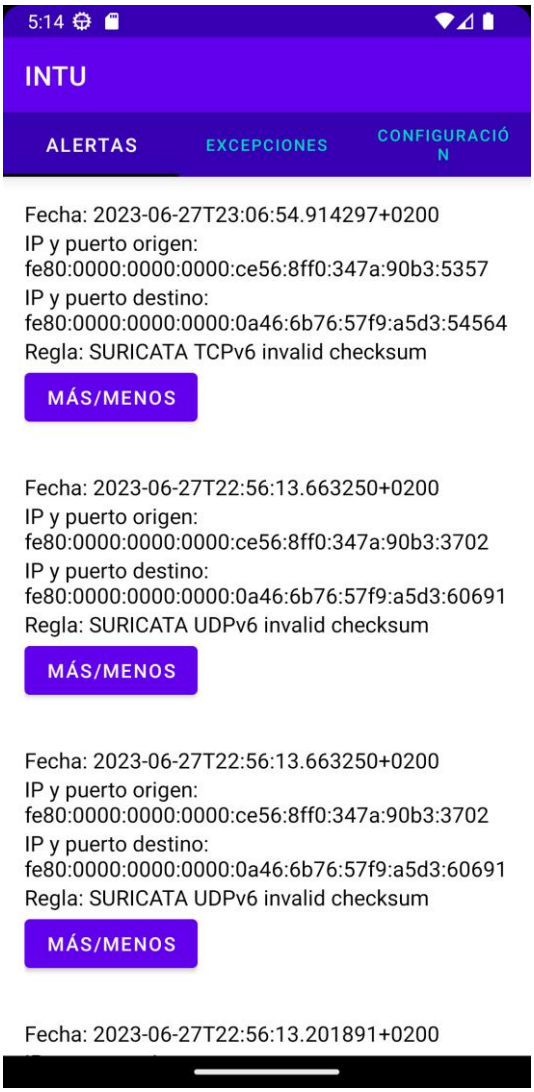


Ilustración 36: Alertas no deseadas

Aunque la Ilustración 36 ya da una idea de las alertas de SURICATA, es importante señalar que la aplicación ha aguantado sin mayor problema la transmisión y generación de casi 400 alertas. Prueba de ello es el mensaje que muestra en terminal el servidor, que puede verse en la Ilustración 37.

```
Sent 397 lines to ('192.168.3.159', 51836)
```

Ilustración 37: Líneas enviadas por el servidor

Por tanto, va a haber que excepcionar estas reglas.

En este apartado, mostraremos la excepción de una sola regla, pero se puede ver cómo las distintas reglas a excepcionar podrían dar pie a distintos aspectos del tutorial.

Lo primero es que una vez se pulsa en el botón de Excepcionar, se ve el diálogo con los campos rellenados por defecto según la alerta. La Ilustración 38 demuestra que la aparición de direcciones IPv6 ha roto ligeramente esta función de autocompletado:

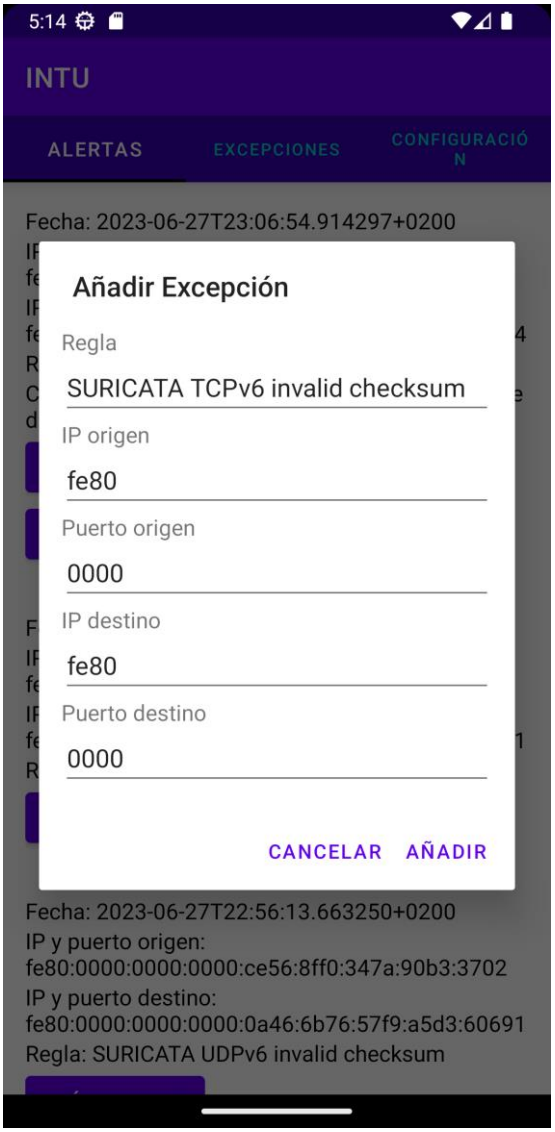


Ilustración 38: Diálogo de excepción

Por suerte, la excepción que pretendemos añadir es para la regla entera, por lo que bastará con vaciar todos los campos como se puede ver en la Ilustración 39:

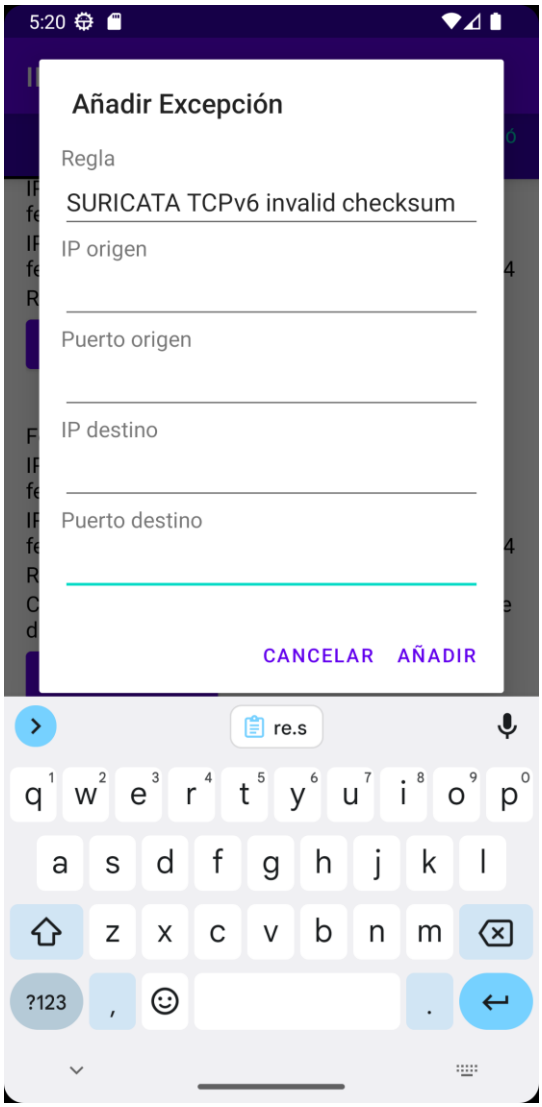


Ilustración 39: Excepción a aplicar

Al pulsar en AÑADIR, podremos ver la excepción en la pestaña Excepciones (Ilustración 40), y confirmar su presencia en el fichero `/var/lib/suricata/rules/local.rules` del servidor (Ilustración 41):

Ilustración 40: Excepción aplicada visible en cliente

```
pass tcp any any -> any any (msg:"SURICATA TCPv6 invalid checksum"; tcpv6-csum:invalid;
classtype:protocol-command-decode; sid:10000000; rev:2;)
```

Ilustración 41: Excepción aplicada en servidor

Tras cerrar y volver a abrir la aplicación, utilizando el botón CARGAR NUEVAS de EXCEPCIONES se vuelve a visualizar la misma excepción (no se incluye una nueva ilustración por presentar el mismo aspecto que la Ilustración 40)

6. Conclusiones

De entre los múltiples elementos que mejoran la seguridad de una red, hay muchos que no están enfocados al entorno doméstico de un usuario no técnico. En muchos casos, esto no es así porque ese elemento no sea aplicable conceptualmente a una red doméstica, sino porque no se ha aplicado a dichas redes y/o porque ha sido diseñado con un perfil técnico de usuario en mente.

Uno de estos elementos es un sistema NIDS. Se ha diseñado una aplicación con la que se puede gestionar un NIDS desde el móvil y obtener información clara y útil que requiere de mucho menos conocimiento previo. Se ha demostrado así que es posible adaptar un sistema ya existente creado para usuarios técnicos y entornos corporativos, y adaptar unas reglas ya existentes creadas con una mira similar, de forma que sean útiles para el ciudadano de a pie.

Se han estudiado los tipos de alerta que cubre una de las fuentes más conocidas de reglas para NIDS, determinando qué categorías son o no útiles para un entorno doméstico y confeccionando, para las que sí son útiles, textos explicativos que bajan el nivel técnico requerido para entender la situación y qué hacer al respecto.

El objetivo de la aplicación desarrollada es permitir la visualización de alertas por amenazas de ciberseguridad, y la personalización de esta visualización para evitar una cantidad de alertas que desborde al usuario. Además, se ha hecho para Android y se ha diseñado con unos elementos comunes a muchas otras aplicaciones móviles, lo que favorece que un usuario no técnico pueda comunicarse con la aplicación de una forma a la que está acostumbrado.

La aplicación que se ha desarrollado, en definitiva, cumple con los objetivos presentados y además sirve como punto de partida para futuros trabajos enfocados en facilitar a los usuarios no técnicos el conocimiento y control de sus sistemas.

7. Trabajos futuros

En este apartado, se recogen ciertas mejoras posibles para la aplicación, que no se han implementado por salir del alcance determinado para el mismo, pero pueden aumentar su utilidad o calidad.

- Diseñar un producto físico para la captura de datos y como servidor de la aplicación, que también integre las funciones del propio router. Esto permitiría simplificar al máximo la instalación y abriría una puerta importante a la comercialización, dado que este tipo de usuario no suele ser propicio a pagar por algo intangible.
- Alternativamente, incluir instrucciones o aclaraciones sobre distintas opciones de infraestructura para conseguir el resultado necesario.
- Crear tutoriales para la primera vez que se utilice cada funcionalidad, incluyendo un tutorial que presente al usuario la infraestructura de su red por si no la conoce.
- Programar un instalador que, al ser ejecutado en un servidor, lo configure como servidor NIDS con el NIDS en cuestión, las reglas adecuadas, la tarea de actualización y, por supuesto, la lógica de comunicación con los clientes.
- Desarrollo de distintos sets de reglas: sets optimizados según la posición del servidor respecto a los dispositivos (según si se puede o no ver la IP origen de las alertas), set de reglas para control parental, set de reglas contra acciones ilegales, etc.
- Nuevos casos de uso: edición o borrado de excepciones, guardar la configuración del servidor, envío de alertas críticas sin esperar a la recarga desde la aplicación.
- Mejoras de calidad de vida para la aplicación móvil: barra de búsqueda de alertas o excepciones, ampliación de reglas por toque en el rectángulo sin botón, borrado retroactivo de alertas que correspondan a una excepción.
- Diseño de reglas específicamente creadas para los riesgos característicos de un entorno doméstico.

8. Bibliografía y referencias

[1] Audit Analytics, "Trends in Cybersecurity Breach Disclosures," 2020.

[2] A. O'Driscoll, «Estadísticas sobre ciberseguridad y cibercrimen en España (2020-2022),» 06 Diciembre 2022. [En línea]. Available: https://www.comparitech.com/es/blog/seguridad-de-informacion/espana-estadisticas-ciberseguridad/. [Último acceso: 15 06 2023].

[3] CheckPoint, «CheckPoint 2023 Security Report,» 2023.

[4] Y. Dennis, «Medium,» 1 11 2021. [En línea]. Available: https://web.archive.org/web/20211119085922/https://medium.com/illumination/data-is-more-valuable-than-gold-193b3b3e5c77. [Último acceso: 15 06 2023].

[5] V. Cherukuri, «KD Nuggets,» 01 03 2022. [En línea]. Available: https://www.kdnuggets.com/2022/03/data-valuable-commodity-businesses.html#:~:text=Why%20Data%20Is%20So%20Valuable,different%20value%20for%20various%20companies.. [Último acceso: 15 06 2023].

[6] CyberLinkASP, «CyberLinkASP,» 31 05 2023. [En línea]. Available: https://www.cyberlinkasp.com/insights/why-an-intrusion-detection-system-is-a-must-have-for-cybersecurity/. [Último acceso: 15 06 2023].

[7] theozebua, «telegram-bot-for-snort via GitHub».

[8] Digital Journal, «Network Intrusion Detection System (NIDS) Market Size 2023, Growth, Upcoming trends, Development Ideas, Industrial Key Factors, Distribution Overview, Regional Opportunities and Forecast to 2028,» 2022.

[9] Microsoft, «¿Qué es SIEM?,» [En línea]. Available: https://www.microsoft.com/es-es/security/business/security-101/what-is-siem#:~:text=La%20Administraci%C3%B3n%20de%20eventos%20e%20informaci%C3%B3n%20de%20seguridad%2C%20SIEM%2C%20para,a%20las%20operaciones%20del%20negocio. [Último acceso: 16 06 2023].

[10] AlienVault, «AlienVault OSSIM».

[11] Wazuh, «Instalación de Wazuh».

[12] SolarWinds, «Security Event Manager».

[13] Fortinet, «Información de seguridad y Administración de eventos (SIEM)».

[14] S2 Grupo, «GLORIA».

[15] CompariTech, «The Best Network Intrusion Detection Systems Software & NIDS Tools,» 28 04 2023. [En línea]. Available: https://www.comparitech.com/net-admin/nids-tools-software/. [Último acceso: 17 06 2023].

[16] Snort, «Snort,» [En línea]. Available: https://www.snort.org/. [Último acceso: 22 06 2023].

[17] Suricata, «Suricata,» [En línea]. Available: https://suricata.io/. [Último acceso: 22 06 2023].

[18] Zeek, «Zeek,» [En línea]. Available: https://zeek.org/. [Último acceso: 22 06 2023].

[19] AT&T Business, «AT&T Cybersecurity Blog,» [En línea]. Available: https://cybersecurity.att.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview. [Último acceso: 25 06 2023].

[20] Zeek, «Writing Bro Scripts,» [En línea]. Available: https://old.zeek.org/manual/2.5.5/scripting/index.html. [Último acceso: 17 06 2023].

[21] Snort, «Downloads».

[22] Proofpoint, «Proofpoint Emerging Threats Rules».

[23] Proofpoint, «ET Category Descriptions,» [En línea]. Available: https://tools.emergingthreats.net/docs/ETPro%20Rule%20Categories.pdf. [Último acceso: 17 06 2023].

[24] C. Rigg, «Are torrents actually dangerous?,» 16 09 2022. [En línea]. Available: https://www.tomsguide.com/features/are-torrents-actually-dangerous#:~:text=Malware%20and%20viruses,parties%20looking%20to%20infect%20systems.. [Último acceso: 25 06 2023].

[25] C. P. G. W. Markus Kammerstetter, «Vanity, Cracks and Malware,» *Publikationsdatenbank der Technischen Universität Wien,* 2012.

[26] Android, «Android Studio».

[27] WireShark, «WireShark,» [En línea]. Available: https://www.wireshark.org/download.html. [Último acceso: 27 06 2023].

[28] TrendMicro, «A Look Into the Most Noteworthy Home Network Security Threats of 2017,» [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/a-look-into-the-most-noteworthy-home-network-security-

threats-of-2017. [Último acceso: 27 06 2023].

[29] K. Grigorov, «KpyM Telnet/SSH Server,» [En línea]. Available: https://www.kpym.com/2/kpym/download.htm. [Último acceso: 27 06 2023].

[30] VirusTotal, «VirusTotal search,» [En línea]. Available: https://www.virustotal.com/gui/home/search. [Último acceso: 25 06 2023].

[31] AbuseIPDB, «Abuse IP Database,» [En línea]. Available: https://www.abuseipdb.com/. [Último acceso: 25 06 2023].

[32] Axarnet, «¿Cómo bloquear una IP desde Firewall de Windows?【Pasos】,» [En línea]. Available: https://axarnet.es/blog/bloquear-ip-firewall-windows. [Último acceso: 25 06 2023].

[33] informaticamadridmayor.es, «Formación Informática para Mayores,» [En línea]. Available: https://informaticamadridmayor.es/tips/como-bloquear-un-dominio-o-sitio-web-en-el-firewall-de-windows-defender-con-powershell/. [Último acceso: 25 06 2023].

[34] Redes Zone, «¿Puede sufrir tu router un ataque DDoS? Evítalo,» [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/como-evitar-ataques-ddos-router/. [Último acceso: 25 06 2023].

[35] Redes Zone, «Desactiva NetBIOS en Windows con estos sencillos pasos,» [En línea]. Available: https://www.redeszone.net/tutoriales/redes-cable/desactivar-netbios-windows/. [Último acceso: 25 06 2023].

[36] PC SOLUCIÓN, «Activar,desactivar,iniciar y detener telnet desde el terminal,» [En línea]. Available: https://pc-solucion.es/windows/activardesactivariniciar-y-detener-telnet-desde-el-terminal/. [Último acceso: 25 06 2023].

[37] Microsoft, «Controles ActiveX no actualizados,» [En línea]. Available: https://support.microsoft.com/es-es/windows/controles-activex-no-actualizados-3ad33b2d-1cee-5d46-1234-e70714324850. [Último acceso: 25 06 2023].

ANEXO A - ODS

Los Objetivos de Desarrollo Sostenible (ODS), también conocidos como Agenda 2030, son una serie de metas e indicadores establecidos por las Naciones Unidas para abordar los desafíos mundiales y promover un desarrollo sostenible en todo el mundo. Estos objetivos buscan equilibrar las dimensiones económica, social y ambiental del desarrollo, con el fin de mejorar la calidad de vida de las personas, proteger el planeta y asegurar un futuro sostenible para las generaciones venideras.

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No procede**
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**				X
ODS 4. **Educación de calidad.**	X			
ODS 5. **Igualdad de género.**				X
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**				X
ODS 8. **Trabajo decente y crecimiento económico.**			X	
ODS 9. **Industria, innovación e infraestructuras.**				X
ODS 10. **Reducción de las desigualdades.**	X			
ODS 11. **Ciudades y comunidades sostenibles.**				X
ODS 12. **Producción y consumo responsables.**				X
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**			X	
ODS 17. **Alianzas para lograr objetivos.**				X

El TFG que se ha presentado está alineado con los Objetivos de Desarrollo Sostenible que muestra la tabla, por las siguientes razones:

- Educación de calidad: la aplicación permite a usuarios que tengan curiosidad por el mundo de la ciberseguridad y las redes acercarse a este mundo desde un entorno lo menos hostil posible.
- Trabajo decente y crecimiento económico: como ya se ha mencionado, la aplicación acerca a los usuarios al mundo de la ciberseguridad, lo cual puede desembocar en una oportunidad de empleo en el futuro.
- Reducción de las desigualdades: la aplicación permite a cualquier tipo de usuario acceder a una área de conocimiento y de actuación, la ciberseguridad,

que de otra forma estaría reservada a aquellos que tengan el tiempo y los medios para adentrarse en esta área.