

**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**Actividad Evaluable Integral**

DAM: Sistemas Informáticos

DAW: Sistemas Informáticos

ASIR: Seguridad y Alta Disponibilidad

FECHA: 9 de febrero de 2024  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



**Centro iFP   
Actividad Evaluabl 2ª Evaluación**

**Información del documento**

**Información general**

|  |  |
| --- | --- |
|  | |
| Nombre de Documento | **iFP Actividad Evaluable Integral** |
| Organización/Cliente | **iFP Innovación en Formación Profesional** |
| Categoría de Documento | **Enunciado de Actividad Evaluable** |
| Subcategoría | **Sistemas Informáticos y Seguridad** |
| Fecha | **9 de febrero de 2024** |

**Destinatarios**

|  |  |  |
| --- | --- | --- |
| Nombre | Puesto | Detalles de Contacto |
| **Técnico Superior en:**   * **DAM, Desarrollo de Aplicaciones Multiplataforma** * **DAW Desarrollo de Aplicaciones Web** * **ASIR, Administrador de Sistemas Informáticos en red** |  | **C\ Julián Camarillo, 6A**  **E-28037 Madrid** |

**Histórico del documento**

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Versión** | **Comentarios** |
| 30/01/2024 | 0.1 | Borrador inicial |
| 9/02/2024 | 0.5 | Correcciones y actualizaciones |
|  |  |  |

**ÍNDICE**

[1 IDENTIFICACIÓN DE LA ACTIVIDAD EVALUABLE 4](#_Toc158371213)

[1.1 Identificación del proyecto 4](#_Toc158371214)

[1.2 Formato de la actividad 5](#_Toc158371215)

[1.3 Evaluación de la actividad 9](#_Toc158371216)

[2 IDENTIFICACIÓN DEL EJERCICIO EVALUABLE 10](#_Toc158371217)

[2.1 Objetivo del proyecto 10](#_Toc158371218)

[2.2 Ámbito general del proyecto 10](#_Toc158371219)

[2.3 Ámbito específico de la infraestructura 11](#_Toc158371220)

[2.4 Alcance global del proyecto 12](#_Toc158371221)

[3 ACTIVIDADES MODULARES NETWORK 13](#_Toc158371222)

[3.1 Módulo Network 1: Script de Host activos 13](#_Toc158371223)

[3.2 Módulo Network 2: Calculadora de direcciones IP en binario 14](#_Toc158371224)

[3.3 Módulo Network 3: Sniffer Captura de tráfico de red 17](#_Toc158371225)

[3.4 Módulo Network 4: Network Scanner, escaneador de red 19](#_Toc158371226)

[4 ACTIVIDADES MODULARES WEB 22](#_Toc158371227)

[4.1 Módulo Web1: Interfaz Web 22](#_Toc158371228)

[5 ACTIVIDADES MODULARES SYSTEM 24](#_Toc158371229)

[5.1 Módulo System1:Agent, agente local Windows y Linux 24](#_Toc158371230)

[6 ACTIVIDADES MODULARES SECURITY 32](#_Toc158371231)

[6.1 Módulo Security1: IDS, detección de intrusiones 32](#_Toc158371232)

[6.2 Módulo Security2: Vulnerability scanner, análisis de vulnerabilidades 34](#_Toc158371233)

[7 ACTIVIDADES MODULARES SOC 38](#_Toc158371234)

[7.1 Servicio MSSP-CTI Ciberinteligencia 38](#_Toc158371235)

[7.2 Servicio MSSP-Detetc Detección de amenazas 42](#_Toc158371236)

[7.3 Servicio MSSP-EDR Respuesta a Incidencias 46](#_Toc158371237)

[8 ANEXO DE METODOLOGÍAS 47](#_Toc158371238)

[8.1 Esquema Nacional de Seguridad 47](#_Toc158371239)

# IDENTIFICACIÓN DE LA ACTIVIDAD EVALUABLE

## Identificación del proyecto

**Identificación del documento**

El siguiente documento supone el enunciado de la Actividad Evaluable Integral para los alumnos del centro **iFP, Innovación en Formación Profesional**, situado en C\ Julián Camarillo, 6A. E-28037 Madrid; cuya propiedad reside en el **Centro Superior de Altos Estudios Internacionales, S.L.**, con NIF **B-66346925** y domicilio en Barcelona, Av. Diagonal 662-664, E-08034 Barcelona, a su vez propiedad del **Grupo Planeta**.

**Modularidad de la actividad**

La actividad está dividida en varias fases modulares para poder adaptarse a las diferentes circunstancias y niveles, siendo un valor añadido la flexibilidad para combinar distintas fases en una única práctica integral Esta propuesta se concibe a la vez para servir de propósitos como:

* **Actividad evaluable.** Siendo el porcentaje de nota final:
  + un 50% de esta actividad evaluable,
  + un 20% la participación en aula
  + un 30% el examen;

tiene sentido que la mayor carga académica resida en esta actividad evaluable para que pueda ser incorporada en un ciclo de mejora continua, personalización y actualización permanente hasta su fecha de entrega.

* **Material de referencia.** Está concebida para servir de ayuda a los alumnos, dada la cantidad de referencias, material adicional, ejemplos y todo tipo de apoyos para su realización. A este respecto se dispone de
  + Los libros de Referencia
  + Los ficheros PDF correspondientes a las presentaciones de las unidades
  + Presentaciones adicionales subidos por el profesor a la plataforma como ampliación del temario oficial, útiles para obtener posteriores certificaciones.
  + Materiales de colaboración de otros profesores, relevantes para la asignatura correspondiente.
* **Adecuación al mercado.** Se ha procurado adaptar el contenido académico a las necesidades reales de las empresas, que los alumnos se van a encontrar al incorporarse al mercado laboral. Esta adecuación no penaliza el contenido del temario oficial del BOE y su correspondiente adaptación al temario del BOCM.
* **Ejercicio de documentación**, dado que de forma general los perfiles técnicos de tecnologías STEM suelen olvidar, subestimar o tener lagunas en los temas relacionados con la documentación de proyectos, esta actividad evaluable permite, potencia y valora la explicación en detalle de la actividad y la transferencia de conocimiento que evidencia la comprensión de cómo funcionan los procesos. sistemas en su interior. Es decir, el porqué de las cosas.
* **Refresco de redes:** dadas las lagunas en general en el ámbito de redes LAN, se ha hecho especial énfasis en este tema, revisando teoría, conceptos, estructuras de datos, explicación de campos, análisis de protocolos y forense de trazas de red,

**Legislación aplicable**

Respecto a la legislación aplicable, se hace expresa mención al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

* **LCSP**: Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. Última actualización publicada el 01/03/2023. <https://www.boe.es/buscar/act.php?id=BOE-A-2017-12902&tn=1&p=20230301>
* Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
* Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, publicada el 3 de abril de 2018 en
* <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-4573>
* Código del Derecho de la Ciberseguridad, disponible en el siguiente enlace:

<https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad>

**Buenas prácticas**

* ISO 27001 Sistema de Gestión de Seguridad de la Información (SGSI)
* ISO 22301 es la norma internacional para la Gestión de la Continuidad de Negocio (SGCN)

## Formato de la actividad

**Objetivos de la actividad**

Los objetivos de esta actividad evaluable son los siguientes:

* Conseguir para los alumnos una experiencia práctica en el temario de las siguientes asignaturas:
  + **Seguridad y Alta Disponibilidad**, para un nivel técnico equivalente al segundo curso de Administrador de Sistemas Informáticos en Red (ASIR)
  + **Sistemas Informáticos**, para un nivel técnico equivalente al de primer curso de Desarrollo de Aplicaciones Multiplataforma (DAM) y Desarrollo de Aplicaciones Web (DAW)
* Repasar los conceptos teóricos vistos en clase
* Fomentar el trabajo en equipo y los aspectos de documentación y captura de evidencias
* Orientar la actividad a necesidades prácticas reales del mercado y hacerle consciente de la aplicación prácticas de la teoría vista en clase, para facilitar su incorporación laboral, la motivación para el trabajo freelance o el espíritu emprendedor para montar una start-up.
* Quitar el miedo a desarrollar sus propias herramientas y script, demostrando que con tiempo suficiente y la ayuda de la inteligencia artificial, pueden conseguir autonomía en el desarrollo de herramientas y el uso intensivo del open-source.
* Motivar a aquellos alumnos que quieran profundizar en el temario académico, para desarrollar sus propias ideas y premiar el esfuerzo de aquellos trabajos sobresalientes.

**Trabajo en equipo o individual**

La práctica se realizará de forma modular, por grupos o de forma individual.

En el caso de entrega por grupos, la nota será la misma para todos los miembros de un mismo grupo, delegando en ellos la responsabilidad de asignar tareas equitativas entre todos los miembros del mismo grupo.

Aunque el trabajo se entregue por grupos, cada alumno de forma individual, debe subir el trabajo a su plataforma, siendo el trabajo el mismo para todos e indicando los miembros del grupo; pero es necesario que cada uno suba su trabajo.

**Documentación entregable**

* **Fichero comprimido:** fichero .zip (o fichero .rar) con el formato PSN\_Actidad\_Evaluable2ev.zip, siendo P la inicial del primer apellido, S la inicial del segundo apellido y N el nombre. Para alumnos con NIE de países sin segundo apellido, el valor de S será “X”.
* **Memoria técnica:** Documento principal en formato Word (extensión -docx) con tipo de letra Arial 12, espaciado anterior y posterior de 0pto, ninguna sangría e interlineado sencillo. Adicionalmente al fichero Word, se proporcionará en formato Adobe PDF (extensión .pdf).

En caso de no disponer de Microsoft Office se puede utilizar cualquier Suite, de tipo de las disponibles de forma gratuita en https://portableapps.com/

Este documento incluirá la resolución de la actividad añadiendo un nuevo capítulo al enunciado denominado **“Memoria Técnica”** con el siguiente contenido para cada módulo:

* + **Introducción:**

Introducción técnica de la tecnología, adaptada al temario de la asignatura

* + **Metodología**

Descripción técnica de los pasos a realizar para descargar el software necesario, instalarlo, configurarlo, ejecutarlo y conseguir los objetivos descritos.

* + **Resolución de incidencias**

Descripción de las problemáticas encontradas (troubleshooting) y las formas que se han elegido para resolverlas (workaround), indicando una taxonomía de:

* + - Los pasos que se han realizado de forma manual, de memoria con los conocimientos previos o con la información vista en clase, en los apuntes, en el material de la plataforma, o en el libro de referencia.
    - Los pasos que se han aprendido gracias a buscadores de internet, indicando las cadenas de búsqueda y las URLs de referencia utilizadas, mediante técnicas OSINT y Google Hacking.
    - Los pasos aprendidos gracias a la inteligencia artificial, indicando la plataforma utilizada y las consultas realizadas mediante técnicas de “Prompt Engineering” (OpenAI ChatGPT, Google Gemini, Perplexity, etc.)

La intención en este sentido en orientar al alumno hacia las nuevas técnicas de aprendizaje, basado en consultas en buscadores y cadenas de interacciones con las plataformas de inteligencia artificial como apoyo y ayuda a la rápida resolución de situaciones de atasco y bloqueo, para que, con su posterior procesamiento y depuración, aplicando el sentido común y su propio conocimiento, se logra una aceleración de los resultados en poco tiempo.

* + **Evidencias**

Acompañar la descripción técnica del proceso con capturas de pantalla de resultado por pantalla de las líneas de comando, scripts, o interfaz gráfico de las herramientas utilizadas.

* + **Bibliografía**

Listado de URLs de la bibliografía consultada, estándares, guías de buenas prácticas, etc,

* **Diseños de arquitectura:** Fichero en MS Powerpoint con el diseño de la arquitectura, con una diapositiva para cada módulo, incluyendo, entradas y salidas de (ficheros, datos, tráfico, telemetría, formatos, etc.).
* **Código fuente:** fficheros con el código de los scripts (lenguajes Batch, PowerShell, Python, bash, perl) o código (C, Java, C++, C#, etc) incluyendo librerías y ficheros necesarios para su reproducibilidad en el caso de utilizar un entorno de desarrollo IDE. Incluir la URL de github en caso de liberarse estos scripts como fuentes abiertas (open source) al público en general.
* **Ficheros auxiliares:** Ficheros de configuración necesarios para las herramientas, los parámetros, así como ficheros auxiliares o capturas de tráfico de red (formato .pcap) o información adicional de la práctica.

## Evaluación de la actividad

La puntuación de la actividad se realizará de la siguiente forma:

* **De 0 a 4 puntos:** si no se llega al nivel mínimo de poder entregar una mínima versión funcional de los contenidos educativos, con la explicación de su funcionamiento y captura de pantalla que evidencien su ejecución en el dispositivo.
* **5 puntos:** entregar la memoria técnica con el resultado que pide el enunciado, en especial una explicación de cómo funciona por dentro y captura de pantalla de su ejecución. Hay que tener en cuenta que ya el propio enunciado de la práctica y las ayudas y consejos que contiene, están diseñadas para poder aprobar con conocimiento suficiente, solamente leyendo dicho enunciado.
  + Para DAM y DAW: mínimo actividades Network 1, 2, 3 y 4 en el segundo trimestre. La Actividad System es para el tercer trimestre pero se valorará que se entregue en el segundo trimestre con lo visto en clase.
  + Para ASIR: además: las actividades Network 1, 2, 3 y 4 y System,
* **De 6 a 10 puntos:** la puntuación de la práctica se irá incrementado gradualmente en base a la utilización de herramientas o fuentes adicionales o mejoras sobre el enunciado solicitado, que incluyen:
  + Mejoras los scripts, del tipo solicitud de parámetros., documentación en el propio script, añadir llamadas a funciones, añadir estructuras de control (errolevel), crear un Banner ASCII Art, etc.
  + Realizarlo en otros lenguajes de script distintos al del ejemplo
  + Generar un interfaz web lo más usable posible (UX /UI) como resultado de la salida por pantalla.
  + Para ASIR: realizar además las actividades Security 1 y 2.

etc.

**Puntuación:**

* 30 puntos por indicar la explicación técnica de cómo funciona por dentro
* 20 puntos por la realización de scripts o sistemas de automatización para generar lo resultados obtenidos mediante líneas de comandos, parámetros. scripts, etc.
* 20 puntos por indicar una metodología para la realización del ejercicio.
* 15 puntos por la inclusión de evidencias (ficheros de salida, capturas de pantalla, etc.) que demuestren la ejecución personalizada de la actividad solicitada
* 5 puntos: por la realización del resumen ejecutivo en Powerpoint con un diseño de arquitectura.
* 5 puntos por la explicación de las dificultades encontradas, queries de Google, prompt de la AI, etc.
* 5 puntos por añadir Bibliografía de referencia

# IDENTIFICACIÓN DEL EJERCICIO EVALUABLE

## Objetivo del proyecto

**Objetivo**

El objetivo de esta práctica es la realización de una serie de ejercicios evaluables, simulando un proyecto de generación de un Informe de Revisión de la Ciberseguridad de la Infraestructuras TIC, mediante el escaneo de la red interna y la generación de los informes correspondientes NVA (Network Vulnerability Assessment.

La realización de cada uno de los módulos está orientada a aplicar los conocimientos vistos en clase, a la realización en el mundo profesional de este tipo de proyectos.

## Ámbito general del proyecto

**Ámbito del proyecto**

El SuC (System under Consideration) sobre el que ejecutar la plataforma en este caso se define como todos los equipos de la clase y su espacio de direcciones, sistemas operativos y aplicaciones, exceptuando el switch compartido y hasta la ruta por defecto (el cortafuegos de re do el Access Point inalámbrico).

De esta forma se simula la ejecución sobre una organización del tipo Pequeña Empresa (10 a 49 equipos) con unos 32 equipos informáticos en la red local de clase. Es importante observar que al tener la red una máscara /22 se están realizando un escaneo de 4 clases C; a la hora de limitar el ámbito de escaneos para no realizar el escaneo de otras clases en nuestra red.

**Ámbito del entorno tecnológico**

De forma general, el ámbito de aplicación del proyecto, que en terminología de ciberseguridad industrial, según el estándar ISA/IEC 62443, se denomina “Sistema bajo Consideración” o (SuC, System under Consideration), se refiere a los siguientes entornos:

* **Sistemas TIC** (Tecnologías de la Información y de las Comunicaciones) necesarios o relacionados con el sistema productivo, salvo que se especifique lo contrario en las exclusiones dentro de este documento. **En este caso, los equipos de clase.**

El ámbito del proyecto incluye la determinación de los dispositivos, componentes, grupos de componentes de la infraestructura de sistemas, que dispongan de dirección IP y que formen parte de la plataforma, dentro del Sistema bajo Consideración (SuC).

## Ámbito específico de la infraestructura

**Ámbito**

Los sistemas de información utilizados en el aula, son los siguientes, constituyendo el Sistema bajo Consideración y el ámbito de actuación del proyecto en lo que respecta a la infraestructura TIC.

* **[P] Personal**
  + Un máximo de 32 alumnos por clases, con acceso a la red corporativa
* **[L] Instalaciones**
  + las instalaciones existentes son las aulas 6, 7 y 8
* **[SS] Servicios subcontratados:**
  + se excluye de esta revisión las aplicaciones en nube relacionadas con la parte académica (Campus Virtual Black Board, TEAMS, Esemtia, Coupa, etc.) disponibles para alumnos y/o profesores. Queda estrictamente prohibida cualquier acción en estas plataformas o sobre cualquier aplicación alojadas fuera de los equipos del aula.
* **[COM] Redes de comunicaciones**
  + El router predeterminado de los equipos es un sistema cortafuegos Fortinet FortiGate, descubierto analizando los primero octetos de la MAC de respuesta a una petición ICMP (ping)
  + Electrónica de res (routers y switches)
  + Punto de Acceso WiFi (Access Point)

Se permite la revisión de estos equipos siempre que sean accesibles, o gestionables y no se intente ninguna intrusión más allá de un escaneo de puertos, identificación de servicios y comprobación de potenciales vulnerabilidades en red. Se prohíbe de forma explícita el acceso (login) a estos equipos y cualquier intento de explotación de vulnerabilidades está específicamente prohibido.

* **[HW] Hardware**
  + Equipos DELL de usuario

Se permite la identificación de parámetros del equipo, tanto vía red como mediante ejecución de agentes locales. Se permite complementar la información con evidencia fotográfica de las opciones de configuración de la BIOS/UEFI.

* **[SW] Software**
  + Sistema Operativo Windows
  + Máquina VirtualBox con Sistema Operativo Ubuntu

Se permite la identificación de parámetros del equipo, tanto vía red como mediante ejecución de agentes locales. Se permite todo tipo de captura de parámetros sin miedo a dañar el equipo, pues al reiniciar se restaura una imagen limpia del sistema.

Se prohíbe de forma explícita cometer daños en el contenido del almacenamiento o estructuras de tablas para la unidad D:, que debe respetarse como medio de almacenamiento persistente.

## Alcance global del proyecto

**Alcance**

El alcance del proyecto contempla la redacción de los siguientes entregables:

* Informe de resultados de un NVA (Network Vulnerability Assessment).
* Informe de Revisión de la ciberseguridad de la Infraestructura, con recomendaciones de remediación y un Plan de Acciones Correctivas.

**Metodologías y herramientas**

* En la realización de las pruebas técnicas se utilizarán las metodologías OSSTMM para las vulnerabilidades en red y OWASP para vulnerabilidades web, así como las buenas prácticas del sector..
* El informe de revisión de ciberseguridad se basará en las recomendaciones del del estándar ISO 27001:2022 y del Esquema Nacional de Seguridad.

# ACTIVIDADES MODULARES NETWORK

## Módulo Network 1: Script de Host activos

**Objetivo**

El objetivo de esta práctica es generar un script para indicar los equipos de la red que están vivos y generar un fichero con dichos hosts.

Para mejorar las práctica, se puede aprovechar dicho fichero para generar un interfaz web de equipos vivos.

**Ámbito**

El ámbito de la red a escanear es la 192.168.128.0 / 22; o el rango de direcciones del equipo donde se esté realizando la práctica; por ejemplo: para aquellos alumnos que accedan por WiFi en vez de por red local, o bien para los que realicen la práctica en casa, con otro direccionamiento.

**Entradas**

El parámetro de entrada será el rango de direcciones IP de las distintas aulas 6, 7 y 8 para DAM, DAW y ASIR respectivamente. Un ejemplo sería la red 192.168.128.0 / 22 con ruta predeterminada 192.168.128.1

**Salidas**

La salida será un fichero conteniendo los siguientes elementos:

* Equipos visibles a nivel IP (responden a ping icmp)

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Se permite la llamada al comando ping del sistema con los parámetros necesarios, así como tuberías “pipes” para parsear la salida por pantalla

**Ejemplo 1**

Un ejemplo de script para realizar el escaneo de toda la red podría ser el siguiente:

@echo off

cls

for %%j in (128, 129,130, 131) do (

for /L %%i in (1, 1, 254) do (

ping 192.168.%%j.%%i -n 1 | find "TTL"

)

)

pause

exit

**Ejemplo 2**

@echo off

cls

echo ^<html^>

echo ^<body^>

for /L %%y in (40, 1, 43) do (

for /L %%x in (20, 1, 25) do (

ping 192.168.%%y.%%x -n 1 | find "TTL" > NUL

if not errorlevel 1 (

echo ^<p^> El equipo 192.168.%%y.%%x está vivo ^</p^>

)

)

)

echo ^</ body^>

echo ^</ html^>

pause

exit

**Ayudas:**

* El pause antes del exit permite que se visualicen los resultados antes que se cierre la venta, si el script se ejecuta en Windows.
* Para ejecutar el script, mejor en línea de comandos que en ventana Windows
* Para generar un fichero de texto en línea de comandos, utilizar el símbolo de redirección > para crear el fichero o >> para anexar contenido a un fichero existente.
* Importante recordad que en la sintaxis del bucle for, el párametro /L indica que el primer número es el inicio, el segundo número es el número de incremento del contador y el tercero es el fin, siendo todos los caracteres números enteros. Cuando no se utiliza parámetro, el contenido del paréntesis se trata como cadena de texto y no tiene tres parámetros sino un número indefinido de cadenas de texto.
* La sintaxis del find en Windows es buscar una cadena entre comillas. El caso de utilizar el comando findstr no se utilizan comillas, El equivalente en Linux es grep.
* Es importante recordad que por cada paréntesis abierto es necesario el parénteis cerrado equivalente, por ello se utiliza la indentación (mover un bloque de texto a la derecha para que estén alineados elementos del mismo bloque)

**Referencias**

<https://www.delftstack.com/howto/batch/batch-for-loop/>

## Módulo Network 2: Calculadora de direcciones IP en binario

**Objetivo**

* El objetivo de esta práctica es generar un fichero de texto ASCII denominado IP\_address.txt con todas las posibles direcciones IP dentro de un rango de red determinado, dada una dirección IP y una máscara.
* Cada dirección IP se debe representar en binario; es decir en formato B1.B2.B3.B4 siendo Bn el octeto correspondiente en binario.
* La dirección IP y la máscara pueden estar “hardcodeadas” en binario en el script.

**Entradas**

La dirección IP y su máscara estará fijada para una dirección IP y máscara específica; por ejemplo:

* Dirección IP: 192.168.8.23
* Máscara: 255.0.250.255

**Salidas**

* La salida será un fichero de texto ASCII denominado IP\_address.txt
* El fichero contendrá todas las direcciones IP posibles. Se excluyen las direcciones de la red y de broadcast.
* Cada uno de los 4 octetos de la dirección IPv4 se debe representar en binario; es decir en formato B1.B2.B3.B4 siendo Bn el octeto correspondiente en binario.

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Aunque la realización del script se realizará en lenguaje Batch, se permite la comprobación de resultados con herramientas del tipo Solarwinds Free Subnet Calculator, disponible en

<https://www.solarwinds.com/free-tools/advanced-subnet-calculator>

**Ayuda 1**

La siguiente información puede ser de utilidad para la práctica

* Decimal 0 Binario: 0000 0000
* Decimal 255 Binario: 1111 1111
* Decimal 192: Binario: 1100 0000
* Decimal 168 Binario: 1010 1000
* Decimal 250 Binario: 1111 1010
* Decimal 23 Binario:0001 0111

**Ayuda 2**

En el caso que sean máscaras CIDR del tipo /22, /23 /24 etc, las opciones del nmap como

nmap -sL 192.168.0.0/22

podrían resolver la lista de direcciones IP posibles pero si se quiere utilizar un rango de direcciones, debe usarle la notación con el rango en cada octeto; por ejemplo 192.168.0-255.1-254.

Más información en <https://nmap.org/book/man-target-specification.html>

**Ejemplo**

Un ejemplo de script para mostrar todas las direcciones IP de la red en binario sería:

@ echo off

cls

echo Calculadora de Direcciones IP

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo.

echo IP Address: 192.168.8.23

echo Network Mask: 255.0.250.255

echo.

echo IP Address: 11000000.10101000.00001000.00010111

echo Network Mask: 11111111.00000000.11111010.11111111

echo.

echo Sintaxis de las posibles direcciones IP

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

echo.

echo IP Address: 11000000.10101000.00001000.00010111

echo Máscara: 11000000.xxxxxxxx.00001x0x.00010111

echo IP Address: 11000000.%%a%%b%%c%%d%%e%%f%%g%%h.00001%%i0%%j.00010111

echo.

echo Posibles combinaciones

echo \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

for /l %%a in (0,1,1) do (

for /l %%b in (0,1,1) do (

for /l %%c in (0,1,1) do (

for /l %%d in (0,1,1) do (

for /l %%e in (0,1,1) do (

for /l %%f in (0,1,1) do (

for /l %%g in (0,1,1) do (

for /l %%h in (0,1,1) do (

for /l %%i in (0,1,1) do (

for /l %%j in (0,1,1) do (

echo 11000000.%%a%%b%%c%%d%%e%%f%%g%%h.00001%%i0%%j.00010111

)

)

)

)

)

)

)

)

)

)

## Módulo Network 3: Sniffer Captura de tráfico de red

**Objetivo**

Realizar la captura de tráfico de red local en el equipo, simulando la operación normal de un usuario en un espacio definido de tiempo para capturar el patrón del tipo de tráfico normal y diferenciarlo del tipo de tráfico que se encuentra cuando se están realizando operaciones de tipo hacking ético o telemetría de datos,

El tráfico a capturar es una petición web a la página raíz principal de la web <http://www.confianza23.es>

**Entradas**

El parámetro de entrada será un indicador único de la máquina, por ejemplo la dirección IP, el nombre de host, o el dns. En este caso el stream a verificar sería una petición web por http a la web [www.confianza23.es](http://www.confianza23.es)

**Salidas**

* La salida será un fichero en formato “.pcap” con un nombre de fichero estándar indicando lso siguientes campos:
  + Dirección MAC de origen (resuelta)
  + Dirección IP de origen
  + Puerto de origen
  + Dirección MAC de destino (no resuelta)
  + Dirección IP de destino
  + Puerto de destino (resuelto)
  + Protocolo
  + Campo de informac´pn
* El fichero exportado .pcap o .pcapng (pcap next generation) deberá incluir solamente los registros de las conexiones en el stream marcado.
* El fichero de salida debería filtrar únicamente aquellas conexiones relevantes de esta transmisión, sin incluir ruido de otros streams.
* Se deberá adjuntar captura de pantalla del seguimiento del flujo de tráfico web, es decir, la decodificación del protocolo http para ese stream.

El formato de salida será el siguiente:

* Fichero .pcap ó pcapng
* Capturas de pantalla con el diseño de la topología de red en base a los flujos de tráfico detectados.
* Filtros utilizados para la captura y exportación del tráfico.

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Herramienta Wireshark para entorno gráfico de captura de tráfico, así como la utilidad TShark para manipulación de tráfico en línea de comandos,
* Herramienta NSA Grassmarlin para dibujado gráfico de la arquitectura y análisis de tipos de tráfico

**Ayudas**

* Para filtrar tráfico de un mismo stream (por ejemplo el triple handshaking de una conexión TCP y su posterior tráfico http ó ftp) se puede utilizar el identificador del stream con el filtro siguiente: **tcp.stream == 17**
* Para encontrar una cadena de texto en ese stream se utiliza el filtro **tcp contains "confianza23"**
* Otro tipo de filtros útiles podrían ser los siguientes:
  + **ip.src == 192.168.40.23** para ver la IP de origen
  + **tcp.completeness.syn == True**  para ver el flag de SYN
  + **eth.src == 40:1c:83:5a:66:99**  para ver la dirección MAC

**Nivel avanzando**

De forma opcional, se genera una segunda salida incluyendo

* Generación de fichero ASCII parseable con los tipos de tráfico
* Generación del seguimiento de un tipo de tráfico concreto (por ejemplo http, ftp, etc.) para reconstruir una sesión a nivel forense.

## Módulo Network 4: Network Scanner, escaneador de red

**Objetivo**

Este módulo realizará el escaneo de red del SuC (System under Consideration). Debido a los tiempos de escaneo, se escanearán:

* El router por defecto y la dirección IP del equipo local, para todos los puertos TCP y UDP del 0 al 65535 y detección del sistema operativo, aunque no responda a Ping
* Para el resto de los equipos de la red, solamente escanear los 100 puertos más comunes.

**Entradas**

El parámetro de entrada será el rango de direcciones IP de las distintas salas 6, 7 y 8 para DAM, DAW y ASIR respectivamente. Un ejemplo sería la red 192.168.128.0 / 22 con ruta predeterminada 192.168.128.1

**Salidas**

La salida será un fichero conteniendo los siguientes elementos:

* Equipos visibles a nivel IP (responden a ping icmp)
* Listado completo de todos los puertos tcp y udp desde el 0 hasta el 65535 inclusive, de aquellos equipos que responden a ping, así como su estado (abierto, cerrado, filtrado)
* Servicio más probable en ejecución en cada puerto en base al estándar de mapeo de puertos con servicios de la IANA, Estos servicios están en esta URL:

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

El formato de salida será el siguiente:

* Fichero ASCII resultado de redireccionar la salida estándar de pantalla
* Fichero XTML

**Herramientas**

Este módulo podrá utilizar alguna o todas las siguientes herramientas:

* Herramienta nmap 7.94 en línea de comandos para Windows

<https://nmap.org/download#windows>

* Herramienta nmap en línea de comandos para Linux

<https://nmap.org/download#linux-rpm>

* Entorno gráfico Zenmap

<https://nmap.org/zenmap/>

* Otras herramientas open source de escaneo de redes

**Niveles de escaneo:**

A modo de ayuda, se muestran a continuación diversas combinaciones de parámetros del escaneo de equipos, mostrados por el entorno gráfico ZenMap:

* **Intense scan:** map -T4 -A -v
* **Intense scan plus UDP:**  nmap -sS -sU -T4 -A -v
* **Intense scan, all TCP ports:** nmap -p 1-65535 -T4 -A -v
* **Intense scan, no ping:** nmap -T4 -A -v -Pn
* **Ping scan:** nmap -sn
* **Quick scan:**  nmap -T4 -F
* **Quick scan plus:** nmap -sV -T4 -O -F --version-light
* **Quick traceroute:** nmap -sn –traceroute
* **Regular scan** nmap
* **Slow comprehensive scan:** nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"

**Escaneo en entornos industriales**

nmap -Pn -sT –scan-delay 1s –max-parallelism 1 – p80, 102, 443, 502, 593, 789, 1089-1091, 1911, 1962, 2222, 2404, 4000, 4840, 4843, 4911, 9600, 19999, 20000, 2057, 34962-34964, 44818, 46823, 46824, 55000-55003 PLC.

**Parámetros interesantes:**

* nmap -iL ips.txt escanea una lista de direcciones IP
* nmap -Pn fuerza el escaneo sin realizar un ping previo
* nmap -sN realiza un escaneo solamente a host vivos (responden a ping)
* nmap -O muestra el sistema operativo remoto
* nmap -sV: prueba puertos abiertos con la versión del servicio
* El parámetro -s es acumulativo; rro ejemplo -sSUV
* Nmap -F escanea los 100 puertos más comunes

**Nivel avanzando**

De forma opcional

* Se genera una segunda salida incluyendo
  + Optimización de parámetros para un ataque lento y evadir las regas de snort (sincronizar equipo de red team con equipo de blue team).
  + Generación de un informe automatizado con la herramienta MagicTree

<https://www.gremwell.com/using_magictree_quick_intro>

**Referencias**

* Puertos comunes de la IANA Internet Assigned Numbers Authority

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

* Fichero de texto en ASCII para “parsear” puertos:

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>

* Guía de referencia de de nmap

<https://nmap.org/man/es/index.html>

* Parámetros de nmap:

<https://www.redeszone.net/tutoriales/configuracion-puertos/nmap-escanear-puertos-comandos/>

<https://www.redeszone.net/seguridad-informatica/listado-de-parametros-de-nmap/>

# ACTIVIDADES MODULARES WEB

## Módulo Web1: Interfaz Web

**Objetivo**

Este módulo mostrará un interfaz web para la visualización de los resultados de los módulso anteriores.

**Entradas**

El parámetro de entrada será el resultado de salida por pantalla de los módulos anteriores pero con un interfaz gráfico Web

**Salidas**

La salida será un fichero conteniendo las combinaciones de los siguientes elementos:

* Página web estática
* Páginas web con ficheros CSS
* Estructuras de carpetas con los ficheros de la página web
* Ficheros de configuración de la herramienta o IDE utilizado para generarlo

**Herramientas**

Se generá un interfaz web para visualizar el resultado. Se permiten todo el rango de opciones posibles, realizando de forma incremental la calidad de la visualización

* Fichero index.html estático generado con la salida de texto del script
* Fichero en HTML5 / CSS
* Mejoras del fichero HTML con biblioteca de scripts Java para visualización de datos personalizada, del tipo D3.js

<https://d3js.org/getting-started>

* Parsearlo desde un CSV, XML o JSON
* Generarlo desde algún framework Python, por ejemplo Flask, Django o FastAPI

Ej: <https://flask.palletsprojects.com/en/3.0.x/tutorial/>

* Generarlo con frameworks del tipo React, Angular, Vue.,jQjuery, etc.

**Ayudas**

* Al escribir un fichero batch y realizar un echo, hay que tener cuidado al escribir códigos html como <html> porque se confunde el carácter “>” al parsear el script. La solución para resolver este tema es poner un carácter ^ delante de cada carácter especial (ASCII > 128 bits).
* Algunas librerías gratuitas de JavaScript permiten ayudas visuales muy impactantes simplemente añadiendo unas pocas líneas en el código HTML, como por ejemplo D3Js. Una idea sería el poder localizar en un mapa el direccionamiento IP del sistema auditado: <https://observablehq.com/@d3/versor-dragging?intent=fork>

# ACTIVIDADES MODULARES SYSTEM

## Módulo System1:Agent, agente local Windows y Linux

**Objetivo**

Este módulo realizará la obtención de datos del sistema operativo local del equipo con las siguientes entradas y salidas:

**Entradas**

El parámetro de entrada será un indicador único de la máquina, por ejemplo la dirección IP, el nombre de host, o el dns.

**Salidas**

La salida será un fichero conteniendo los siguientes elementos:

* Datos de la máquina (hostname, etc.)
* Datos estáticos de red (dirección ip, máscara, Gateway por defecto, rutas, etc.)
* Datos dinámicos de red (tabla de arps, dns cacheados, estadísticas de red netstat, etc.)
* Datos internos de procesos en memoria (memoria, cpu, disco, particiones, etc.)
* Datos de aplicaciones instaladas y en ejecución (tasklist)
* Parches instalados en el sistema operativo

El formato de salida será el siguiente:

* Fichero ASCII resultado de redireccionar la salida estándar de pantalla

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Herramientas del sistema operativo en línea de comandos o script que llama a estos comandos, con los parámetros adecuados
* Otras herramientas o scripts open source del tipo Microsoft Sysinternals Suite de Mark Russinovich

**Ejemplo script en bash**

@echo off

REM Agent Script v1.1

REM Usage: agent\_script.cmd >> agent\_results.txt

REM Cambio de página de códigos para que aparezcan los acentos

CHCP 1252

REM Display current date and time

echo Current date:

date /T

echo Current time:

time /T

REM Display timezone information

echo Timezone:

tzutil /g

echo Available timezones:

tzutil /L

REM System Info

systeminfo

REM Basic system information

echo Operating System Version:

ver

echo Hostname:

hostname

echo Current User:

whoami

echo Volumes and Drives:

vol

echo Network Users:

net user

echo System PATH:

path

echo Logged-in Users:

quser

echo Power Configuration:

powercfg /L

REM Network settings

echo Network Configuration:

ipconfig /all

echo ARP Table:

arp -a

echo MAC Address:

getmac

echo Routing Table:

route print

echo Network Statistics:

netstat -nr

echo Network Adapters:

netcfg -s n

REM Internal processes

echo Service Status:

sc query

echo Running Apps:

tasklist /APPS

echo Running Services:

tasklist /SVC

echo Loaded Modules:

tasklist /m

echo Running Processes (CSV format):

tasklist /FO CSV

REM Win32\_QuickFixEngineering

echo Windows QuickFixes:

wmic qfe list full /format:htable > updates\_list.html

REM Filesystem information

echo Directory Tree:

tree

echo All Files and Folders:

dir /s

REM End of script

echo Script execution completed.

**Ejemplo de conversión a agente Python con llamadas al sistema:**

import os

import platform

import subprocess

def obtener\_parametros\_del\_sistema():

# Change code page

print("Current Code Page:")

os.system("chcp 1252")

# Display current date and time

print("Current date:")

os.system("date /T")

print("Current time:")

os.system("time /T")

# Display timezone information

print("Timezone:")

os.system("tzutil /g")

print("Available timezones:")

os.system("tzutil /L")

# Basic system information

print("Operating System Version:")

os.system("ver")

print("Hostname:")

os.system("hostname")

print("Current User:")

os.system("whoami")

print("Volumes and Drives:")

os.system("vol")

print("Network Users:")

os.system("net user")

print("System PATH:")

os.system("path")

print("Logged-in Users:")

os.system("quser")

print("Power Configuration:")

os.system("powercfg /L")

# Systeminfo

print("Systeminfo:")

os.system("systeminfo")

# Network settings

print("Network Configuration:")

os.system("ipconfig /all")

print("ARP Table:")

os.system("arp -a")

print("MAC Address:")

os.system("getmac")

print("Routing Table:")

os.system("route print")

print("Network Statistics:")

os.system("netstat -nr")

print("Network Adapters:")

os.system("netcfg -s n")

# Internal processes

print("Service Status:")

os.system("sc query")

print("Running Apps:")

os.system("tasklist /APPS")

print("Running Services:")

os.system("tasklist /SVC")

print("Loaded Modules:")

os.system("tasklist /m")

# Running Processes (CSV format)

print("Running Processes (CSV format):")

subprocess.run(["tasklist", "/FO", "CSV"], stdout=subprocess.PIPE)

# Win32\_QuickFixEngineering

print("Windows QuickFixes:")

subprocess.run(["wmic", "qfe", "list", "full", "/format:htable"], stdout=subprocess.PIPE)

# Filesystem information

print("Directory Tree:")

os.system("tree")

print("All Files and Folders:")

os.system("dir /s")

print("Script execution completed.")

if \_\_name\_\_ == "\_\_main\_\_":

obtener\_parametros\_del\_sistema()

**Ejemplo agente Python con librerías**

import psutil

import platform

def obtener\_parametros\_del\_sistema():

# Información sobre la CPU

cpu\_count = psutil.cpu\_count(logical=False)

logical\_cpu\_count = psutil.cpu\_count(logical=True)

cpu\_percent = psutil.cpu\_percent(interval=1, percpu=True)

print("Información de la CPU:")

print(f"Núcleos Físicos: {cpu\_count}")

print(f"Núcleos Lógicos: {logical\_cpu\_count}")

for i, percent in enumerate(cpu\_percent):

print(f"Uso de CPU en el núcleo {i}: {percent}%")

# Información sobre la memoria

memoria\_info = psutil.virtual\_memory()

print("\nInformación de la Memoria:")

print(f"Memoria Total: {memoria\_info.total} bytes")

print(f"Memoria Disponible: {memoria\_info.available} bytes")

# Información sobre el disco

disco\_info = psutil.disk\_usage("/")

print("\nInformación del Disco:")

print(f"Espacio Total en Disco: {disco\_info.total} bytes")

print(f"Espacio Usado en Disco: {disco\_info.used} bytes")

# Información sobre el sistema operativo

sistema\_info = {

"Sistema Operativo": platform.system(),

"Versión del Sistema Operativo": platform.version(),

"Nombre de la Máquina": platform.node(),

}

print("\nInformación del Sistema Operativo:")

for key, value in sistema\_info.items():

print(f"{key}: {value}")

if \_\_name\_\_ == "\_\_main\_\_":

obtener\_parametros\_del\_sistema()

**Nivel avanzando**

De forma opcional, se generará un script estándar que llame a estos comandos y genere un formato estándar normalizado, con campos definidos, para facilitar la telemetría en una consola estándar.

# ACTIVIDADES MODULARES SECURITY

## Módulo Security1: IDS, detección de intrusiones

**Objetivo**

Este módulo realizará la captura de tráfico proveniente, o bien de un fichero en formato .pcap, ya capturado; o bien la detección de tráfico entrante y saliente en tiempo real con el fin de poder determinar alertas y alarmas que puedan constituir una potencial incidencia de ciberseguridad.

**Entradas**

El parámetro de entrada será un indicador único de la máquina, por ejemplo la dirección IP, el nombre de host, o el dns, habiendo previamente configurado el fichero snort.conf con lso paths necesarios para encontrar los ficheros de reglas y de clasificación.

**Salidas**

* La salida será un fichero en formato de texto ASCII plano con un nombre de fichero estándar indicando el identificador de la máquina, la fecha, la hora y el periodo (por ejemplo 5 mins indicando las posibles alertas y alarmas ocuridas en ese periodo.

El formato de salida será el siguiente:

* Fichero .ASCII

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Herramienta snort en línea de comandos, Esta herramienta se puede descargar del siguiente enlace: <https://snort.org/downloads>
* La versión Snort 2.9.20 permite instalarse en Windows, mientras que la versión Snort3 requiere sistemas operativos basados en Linux.
* En el caso de Windows, Snort requiere para funcionar la librería Npcap 0.9984, descargable desde <https://nmap.org/npcap>; en este caso la versión 1.79.

**Nivel avanzando**

De forma opcional pero no obligatorio, se podría utilizar, además de snort, para comparar el resultado, rendimiento, falsos positivos, etc. otras herramientas open source de detección de intrusiones IDS como por ejemplo las siguientes:

* Suricata
* Bro / Zeek

**Referencias**

* Manual de Snort: <https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/037/699/original/snort_user.html>

## Módulo Security2: Vulnerability scanner, análisis de vulnerabilidades

**Objetivo**

Este módulo realizará el análisis de las distintas vulnerabilidades de red del SuC (System under Consideration), con las siguientes entradas y salidas:

**Entradas**

El parámetro de entrada será el rango de direcciones IP de la sala 8.

**Salidas**

La salida será un fichero conteniendo los siguientes elementos:

* Equipos analizados
* Potenciales vulnerabilidades encontradas, con su CVE asociado
* Recomendaciones de remediación de la vulnerabilidad (definitiva como temporal).

El formato de salida será el siguiente:

* Fichero CSV
* Fichero HTML

**Herramientas**

Este módulo utilizará las siguientes herramientas:

* Herramienta openvas

**Ejemplos de Playbook**

{

"type": "playbook",

"spec\_version": "cacao-2.0",

"id": "p0001.playbook.OpenVas",

"name": "Playbook\_OpenVas",

"description": "OpenVas install & scripting in Kali",

"playbook\_types": ["detection", "investigation", "prevention", "mitigation", "remediation"],

"playbook\_activities": [ "configure-systems" ],

"created\_by": "identity--Confianza23\_[kzemlyan]",

"created": "2024-01-26T18:40:00.123456Z",

"modified": "2024-01-28T20:32:00.123456Z",

"revoked": false,

"valid\_from": "2024-01-28T20:35:00.123456Z",

"valid\_until": "2024-12-31T23:59:59.999999Z",

"derived\_from": ["playbook--template"],

"priority": 3,

"severity": 70,

"impact": 5,

"labels": [ "Template", "Network Support", "Network Traffic, "Domain", "Mitigation", "Malicious", "malware", "apt"],

"external\_references": [

{

"name": "Security Playbooks Version 2.0",

"description": "CACAO Security Playbooks Version 2.0 Committee Specification 01 27 November 2023",

"source": "OASIS",

"url": "http://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.pdf",

"external\_id": "OASIS Security Playbooks v2.0"

}

],

{

"workflow": {

"start—OpenVas\_install": {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "OpenVas\_installation",

"description": "OpenVas\_installation",

"command": "sudo apt update;

sudo apt upgrade;

sudo apt install gvm;

sudo gvm-setup;

sudo apt-get install ufw;

sudo ufw enable & sudo ufw allow 80 & sudo ufw allow 9392;

sudo gvm-check-setup;

sudo runuser -u \_gvm -- greenbone-feed-sync --type SCAP;

sudo runuser -u \_gvm -- greenbone-feed-sync --type CERT;

sudo runuser -u \_gvm -- greenbone-feed-sync --type GVMD\_DATA"

},

"action--2": {

"type": "bash",

"name": "If you can not install OpenVas in Kali due to pg-gvm extension error"

"description": "change the port for pgsql16, the port number should be 5432",

"command": "sudo systemctl stop postgresql;

sudo vim /etc/postgresql/16/main/postgresql.conf;

pg\_lsclusters;

sudo systemctl restart postgresql;

sudo apt install postgresql-16-pg-gvm;

sudo runuser -u \_gvm -- gvmd --create-user=username --password=userpassword"

"action--3": {

"type": "bash",

"name": "OpenVas start & stop",

"description": "Username & password are "confiaza23".",

"command": "sudo gvm-start;

sudo gvm-stop"

}

{

"workflow": {

"start—OpenVas\_nmap\_hostchecking\_list\_script: {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "Script",

"description": " "

"command": "!/bin/bash

nmap -sn -oA nmap-subnet-phisical 192.168.1.0/24

grep Up nmap-subnet-phisical.gnmap | cut -d " " -f 2 > live-hosts.txt"

}

"workflow": {

"start—Checking\_for\_updates: {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "Checking\_for\_updates",

"description":"This is done either from the browser in the Administation section. (sequentially in all three sections:nvt,scap,cert)"

"command": "sudo runuser -u \_gvm -- greenbone-feed-sync --type SCAP;

sudo runuser -u \_gvm -- greenbone-feed-sync --type CERT;

sudo runuser -u \_gvm -- greenbone-feed-sync --type GVMD\_DATA"

}

}

}

"external\_references": [

{

"name": "OpenVas\_Reporting",

"description": "A tool to convert OpenVAS XML into reports",

"url": "https://github.com/TheGroundZero/openvasreporting?ysclid=lrxuu6wun9842869657",

}

]

# ACTIVIDADES MODULARES SOC

## Servicio MSSP-CTI Ciberinteligencia

* Generación de un Powerpoint con el diseño de los componentes de la arquitectura del servicio de Ciberinteligencia
* Generación de una máquina virtual con el componente MISP activo y funcional, incluyendo todos los ficheros, scripts y manuales, así como la generación de Howtos necesarios para poder traspasar el conocimiento rápidamente a cualquier nuevo miembro del equipo técnico.
* Integración de las fuentes por defecto en MISP y añadir nuevas fuentes gratuitas, de ciberinteligencia, entre ellas:
  + Alienvault OTX
  + Recorded Future
  + Fortinet
  + F5
* Generación de un informe periódico semanal de ciberinteligencia en formato correo electrónico en HTML, que se distribuirá por email y de forma gratuita entre la base de clientes, conteniendo un resumen de las informaciones de fuentes abiertas recopiladas a lo largo de la semana.
* Diseñar los entregables en formato Powerpoint (enviado como PDF) con terminología e iconos STIX, para un informe periódico semanal.

**Ejemplo de Playbook**

{

"type": "playbook",

"spec\_version": "cacao-2.0",

"id": "p0001.playbook.misp",

"name": "Playbook\_misp",

"description": "Instalalling MISP",

"playbook\_types": ["detection", "investigation", "prevention", "mitigation", "remediation"],

"playbook\_activities": [ "configure-systems" ],

"created\_by": "identity--ITE\_Equipo\_I+D+i\_[kzemlyan]",

"created": "2024-01-09T16:30:00.123456Z",

"modified": "2024-01-09T16:30:00.123456Z",

"revoked": false,

"valid\_from": "2024-01-09T16:30:00.123456Z",

"valid\_until": "2024-12-31T23:59:59.999999Z",

"derived\_from": ["playbook--template"],

"priority": 3,

"severity": 70,

"impact": 5,

"labels": [ "Template", "Network Support", "Network Traffic, "Domain", "Mitigation", "Malicious", "malware", "apt"],

"external\_references": [

{

"name": "Security Playbooks Version 2.0",

"description": "CACAO Security Playbooks Version 2.0 Committee Specification 01 27 November 2023",

"source": "OASIS",

"url": "http://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.pdf",

"external\_id": "OASIS Security Playbooks v2.0"

}

],

{

"workflow": {

"start--misp": {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "Debian previous configuration",

"description": "SSH install",

"command": "sudo apt-get install openssh-server; sudo systemctl enable ssh"

},

"action--2": {

"type": "bash",

"name": "MISP install bash script",

"description": "use of -i is obligatory for Debian",

"command": "wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh; bash /tmp/INSTALL.sh -c"

},

"action--3": {

"type": "bash",

"name": "Reconfiguración de baseurl",

"description": "Reconfiguración de baseurl to the IP address of your VM (a.b.c.d), by default it is localhost",

"command": "sudo -u www-data /var/www/MISP/app/Console/cake Baseurl https://a.b.c.d; sudo systemctl restart apache2"

},

"end--misp": {

"type": "end",

}

}

}

# 1) The procedure to install a ssh servReconfiguración de baseurler in Ubuntu Linux is as follows:

sudo apt-get install openssh-server.

sudo systemctl enable ssh.

# 2) Instatalación de MISP CORE en Ubuntu

wget --no-cache -O /tmp/INSTALL.sh https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/INSTALL.sh

bash /tmp/INSTALL.sh -c

# 3) Reconfiguración de baseurl to the IP address of your VM (a.b.c.d)

sudo -u www-data /var/www/MISP/app/Console/cake Baseurl https://a.b.c.d

sudo systemctl restart apache2

## Servicio MSSP-Detetc Detección de amenazas

* Generación de un Powerpoint con el diseño de los componentes de la arquitectura del servicio de Detección de Amenazas
* Generación de una máquina virtual con el componente Wazuh activo y funcional, incluyendo todos los ficheros, scripts y manuales, así como la generación de Howtos necesarios para poder traspasar el conocimiento rápidamente a cualquier nuevo miembro del equipo técnico.
* Integración de las fuentes necesarias para la telemetría de los agentes Wazuh:
  + Logs
    - Registro de Windows: El agente de Wazuh recopila los logs del registro de Windows, que incluyen eventos de seguridad, eventos de aplicaciones, eventos de sistema, etc.
    - Registro de Linux: El agente de Wazuh recopila los logs del registro de Linux, que incluyen eventos de seguridad, eventos de aplicaciones, eventos de sistema, etc.
    - Logs de aplicaciones: El agente de Wazuh puede recopilar los logs de diferentes aplicaciones, como servidores web, bases de datos, etc.
    - Logs de firewalls: El agente de Wazuh puede recopilar los logs de diferentes firewalls, como firewalls de hardware, firewalls de software, etc.
  + Eventos
    - Eventos de seguridad: El agente de Wazuh recopila eventos de seguridad, como intentos de acceso no autorizados, malware, etc.
    - Eventos de red: El agente de Wazuh recopila eventos de red, como tráfico malicioso, conexiones sospechosas, etc.
    - Eventos de sistema: El agente de Wazuh recopila eventos de sistema, como cambios en el sistema operativo, cambios en los archivos, etc.
  + Metadatos
    - Sistema operativo: El agente de Wazuh recopila el sistema operativo del endpoint.
    - Arquitectura: El agente de Wazuh recopila la arquitectura del endpoint.
    - Versión del software: El agente de Wazuh recopila la versión del software del endpoint.
    - Configuración: El agente de Wazuh recopila la configuración del endpoint.

**Ejemplos de Playbook**

{

"type": "playbook",

"spec\_version": "cacao-2.0",

"id": "p0001.playbook.wazuh",

"name": "Playbook\_wazuh",

"description": "Instalalling Wazuh central components and Wazuh agent",

"playbook\_types": ["detection", "investigation", "prevention", "mitigation", "remediation"],

"playbook\_activities": [ "configure-systems" ],

"created\_by": "identity--ITE\_Equipo\_I+D+i\_[kzemlyan]",

"created": "2024-01-09T14:30:00.123456Z",

"modified": "2024-01-09T14:30:00.123456Z",

"revoked": false,

"valid\_from": "2024-01-09T14:30:00.123456Z",

"valid\_until": "2024-12-31T23:59:59.999999Z",

"derived\_from": ["playbook--template"],

"priority": 3,

"severity": 70,

"impact": 5,

"labels": [ "Template", "Network Support", "Network Traffic, "Domain", "Mitigation", "Malicious", "malware", "apt"],

"external\_references": [

{

"name": "Security Playbooks Version 2.0",

"description": "CACAO Security Playbooks Version 2.0 Committee Specification 01 27 November 2023",

"source": "OASIS",

"url": "http://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.pdf",

"external\_id": "OASIS Security Playbooks v2.0"

}

],

{

"workflow": {

"start--wazuh\_central\_components\_debian": {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "Debian previous configuration",

"description": "Curl install",

"command": "sudo apt-get install curl"

},

"action--2": {

"type": "bash",

"name": "Wazuh install bash script",

"description": "use of -i is obligatory for Debian",

"command": "curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i"

},

"end--wazuh\_central\_components\_debian": {

"type": "end",

}

}

{

"workflow": {

"start--wazuh\_agent\_debian": {

"type": "start",

},

"action--1": {

"type": "bash",

"name": "Install the GPG key",

"description": "Install the GPG key",

"command": "curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg"

},

"action--2": {

"type": "bash",

"name": "Add the Wazuh repository",

"description": "Add the repository",

"command": "echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list"

},

"action--3": {

"type": "bash",

"name": "Update the package",

"description": "Update the package",

"command": "apt-get update"

},

"action--4": {

"type": "bash",

"name": "Deployment",

"description": "put instead of a,b,c,d your Wazuh manager IP",

"command": "WAZUH\_MANAGER="a.b.c.d" apt-get install wazuh-agent"

},

"end--wazuh\_agent\_debian": {

"type": "end",

}

}

{

"workflow": {

"start--wazuh\_agent\_windows": {

"type": "start",

},

"action--1": {

"type": "powershell",

"name": "Download Windows installer",

"description": "Download Windows installer",

"command": "Invoke-WebRequest -Uri "https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.1-1.msi""

},

"action--2": {

"type": "powershell",

"name": "Windows installing",

"description": "put instead of a,b,c,d your Wazuh manager IP",

"command": ".\wazuh-agent-4.7.1-1.msi /q WAZUH\_MANAGER="a.b.c.d",

},

"action--3": {

"type": "powershell",

"name": "Deployment",

"description": "put instead of a,b,c,d your Wazuh manager IP",

"command": "NET START Wazuh"

},

"end--wazuh\_agent\_windows": {

"type": "end",

}

}

}

## Servicio MSSP-EDR Respuesta a Incidencias

* Generación de un Powerpoint con el diseño de los componentes de la arquitectura del servicio de Respuesta a Incidencias
* Generación de una máquina virtual con los componentes SOAR The Hive y Cortex, activos y funcionales, incluyendo todos los ficheros, scripts y manuales, así como la generación de playbooks necesarios para poder traspasar el conocimiento rápidamente a cualquier nuevo miembro del equipo técnico.
* Generación de los Playbooks necesarios para la resolución de las incidencias más comunes.
* Integración de las TTPs con las matrices del MITRE Att&CK
* Soporte para la definición de un servicio de respuesta a incidencias.

# ANEXO DE METODOLOGÍAS

## Esquema Nacional de Seguridad

De forma general se utiliza la metodología basada en el Esquema Nacional de Seguridad (ENS) y la verificación de la efectividad de los controles asociados, que se muestran a continuación. Esta metodología recomienda que los sistemas de información deberán ser objeto de una auditoría regular ordinaria, al menos cada dos (2) años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Medidas de Seguridad** |  | **Por categoría o dimensión(es)** | **Nivel de las dimensiones de segurirdad** | | |
| **org** | **Marco organizativo** |  | **BAJO** | **MEDIO** | **ALTO** |
| **org** | **Marco organizativo** |  |  |  |  |
| org.1 | Política de seguridad | Categoría | aplica | aplica | aplica |
| org.2 | Normativa de seguridad | Categoría | aplica | aplica | aplica |
| org.3 | Procedimientos de seguridad | Categoría | aplica | aplica | aplica |
| org.4 | Proceso de autorización | Categoría | aplica | aplica | aplica |
| **op** | **Marco operacional** |  |  |  |  |
| op.pl | Planificación |  |  |  |  |
| op.pl1 | Análisis de riesgos | Categoría | aplica | + R1 | + R2 |
| op.pl2 | Arquitectura de Seguridad | Categoría | aplica | + R1 | + R1 + R2 + R3 |
| op.pl3 | Adquisición de nuevos componentes | Categoría | aplica | aplica | aplica |
| op.pl4 | Dimensionamiento/gestión de la capacidad | D | aplica | + R1 | + R1 |
| op.pl5 | Componentes certificados | Categoría | n.a. | aplica | aplica |
| **op.acc** | **Control de acceso** |  |  |  |  |
| op.acc1 | Identificación | T A | aplica | + R1 | + R1 |
| op.acc2 | Requisitos de acceso | C I T A | aplica | aplica | + R1 |
| op.acc3 | Segregación de funciones y tareas | C I T A | n.a. | aplica | + R1 |
| op.acc4 | Proceso de gestión de derechos de acceso | C I T A | aplica | aplica | aplica |
| op.acc5 | Mecanismo de autenticación (usuarios externos) | C I T A | + [R1 o R2 o R3 o R4] | + [R2 o R3 o R4] + R5 | + [R2 o R3 o R4] + R5 |
| op.acc6 | Mecanismo de autenticación (usuarios de la organización) | C I T A | + [R1 o R2 o R3 o R4] + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9 |
| **op.exp** | **Explotación** |  |  |  |  |
| op.exp.1 | Inventario de activos | Categoría | aplica | aplica | aplica |
| op.exp.2 | Configuración de seguridad | Categoría | aplica | aplica | aplica |
| op.exp.3 | Gestión de la configuración de seguridad | Categoría | aplica | + R1 | + R1 + R2 + R3 |
| op.exp.4 | Mantenimiento y actualizaciones de seguridad | Categoría | aplica | + R1 | + R1 + R2 |
| op.exp.5 | Gestión de cambios | Categoría | n.a. | aplica | + R1 |
| op.exp.6 | Protección frente a código dañino | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |
| op.exp.7 | Gestión de incidentes | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 |
| op.exp.8 | Registro de la actividad | T | aplica | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 + R5 |
| op.exp.9 | Registro de la gestión de incidentes | Categoría | aplica | aplica | aplica |
| op.exp.10 | Protección de claves criptográficas | Categoría | aplica | + R1 | + R1 |
| **op.ext** | **Recursos externos** |  |  |  |  |
| op.ext.1 | Contratación y acuerdos de nivel de servicio | Categoría | n.a. | aplica | aplica |
| op.ext.2 | Gestión diaria | Categoría | n.a. | aplica | aplica |
| op.ext.3 | Protección de la cadena de suministro | Categoría | n.a. | n.a. | aplica |
| op.ext.4 | Interconexión de sistemas | Categoría | n.a. | aplica | + R1 |
| **op.nub** | **Servicios en la nube** |  |  |  |  |
| op.nub.1 | Protección de servicios en la nube | Categoría | aplica | + R1 | + R1 + R2 |
| **op.cont** | **Continuidad del servicio** |  |  |  |  |
| op.cont.1 | Análisis de impacto | D | n.a. | aplica | aplica |
| op.cont.2 | Plan de continuidad | D | n.a. | n.a. | aplica |
| op.cont.3 | Pruebas periódicas | D | n.a. | n.a. | aplica |
| op.cont.4 | Medios alternativos | D | n.a. | n.a. | aplica |
| **op.mon** | **Monitorización del sistema** |  |  |  |  |
| op.mon.1 | Detección de intrusión | Categoría | aplica | + R1 | + R1 + R2 |
| op.mon.2 | Sistema de métricas | Categoría | aplica | + R1 + R2 | + R1 + R2 |
| op.mon.3 | Vigilancia | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 + R5 + R6 |
| **mp** | **Medidas de protección** |  |  |  |  |
| **mp.if** | **Protección de las instalaciones e infraestructuras** |  |  |  |  |
| mp.if.1 | Áreas separadas y con control de acceso | Categoría | aplica | aplica | aplica |
| mp.if.2 | Identificación de las personas | Categoría | aplica | aplica | aplica |
| mp.if.3 | Acondicionamiento de los locales | Categoría | aplica | aplica | aplica |
| mp.if.4 | Energía eléctrica | D | aplica | + R1 | + R1 |
| mp.if.5 | Protección frente a incendios | D | aplica | aplica | aplica |
| mp.if.6 | Protección frente a inundaciones | D | n.a. | aplica | aplica |
| mp.if.7 | Registro de entrada y salida de equipamiento | Categoría | aplica | aplica | aplica |
| **mp.per** | **Gestión del personal** |  |  |  |  |
| mp.per.1 | Caracterización del puesto de trabajo | Categoría | n.a. | aplica | aplica |
| mp.per.2 | Deberes y obligaciones | Categoría | aplica | + R1 | + R1 |
| mp.per.3 | Concienciación | Categoría | aplica | aplica | aplica |
| mp.per.4 | Formación | Categoría | aplica | aplica | aplica |
| **mp.eq** | **Protección de los equipos** |  |  |  |  |
| mp.eq.1 | Puesto de trabajo despejado | Categoría | aplica | + R1 | + R1 |
| mp.eq.2 | Bloqueo de puesto de trabajo | A | n.a. | aplica | + R1 |
| mp.eq.3 | Protección de dispositivos portátiles | Categoría | aplica | aplica | + R1 + R2 |
| mp.eq.4 | Otros dispositivos conectados a la red | C | aplica | + R1 | + R1 |
| **mp.com** | **Protección de las comunicaciones** |  |  |  |  |
| mp.com.1 | Perímetro seguro | Categoría | aplica | aplica | aplica |
| mp.com.2 | Protección de la confidencialidad | C | aplica | + R1 | + R1 + R2 + R3 |
| mp.com.3 | Protección de la integridad y de la autenticidad | I A | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |
| mp.com.4 | Separación de flujos de información en la red | Categoría | n.a. | + [R1 o R2 o R3] | + [R2 o R3] + R4 |
| **mp.si** | **Protección de los soportes de información** |  |  |  |  |
| mp.si.1 | Marcado de soportes | C | n.a. | aplica | aplica |
| mp.si.2 | Criptografía | C I | n.a. | aplica | + R1 + R2 |
| mp.si.3 | Custodia | Categoría | aplica | aplica | aplica |
| mp.si.4 | Transporte | Categoría | aplica | aplica | aplica |
| mp.si.5 | Borrado y destrucción | C | aplica | + R1 | + R1 |
| **mp.sw** | **Protección de las aplicaciones informáticas** |  |  |  |  |
| mp.sw.1 | Desarrollo de aplicaciones | Categoría | n.a. | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 |
| mp.sw.2 | Aceptación y puesta en servicio | Categoría | aplica | + R1 | + R1 |
| **mp.info** | **Protección de la información** |  |  |  |  |
| mp.info.1 | Datos personales | Categoría | aplica | aplica | aplica |
| mp.info.2 | Calificación de la información | C | n.a. | aplica | aplica |
| mp.info.3 | Firma electrónica | I A | aplica | + R1 + R2 + R3 | + R1 + R2 + R3 + R4 |
| mp.info.4 | Sellos de tiempo | T | n.a. | n.a. | aplica |
| mp.info.5 | Limpieza de documentos | C | aplica | aplica | aplica |
| mp.info.6 | Copias de seguridad | D | aplica | + R1 | + R1 + R2 |
| **mp.s** | **Protección de los servicios** |  |  |  |  |
| mp.s.1 | Protección del correo electrónico | Categoría | aplica | aplica | aplica |
| mp.s.2 | Protección de servicios y aplicaciones web | Categoría | + [R1 o R2] | + [R1 o R2] | + R2 + R3 |
| mp.s.3 | Protección de la navegación web | Categoría | aplica | aplica | + R1 |
| mp.s.4 | Protección frente a denegación de servicio | D | n.a. | aplica | + R1 |