

EXCELENCIA PROYECTOS PRIMARIOS



JUNTA DE EXTREMADURA



Financiado por
la Unión Europea
NextGenerationEU



*"En cada búsqueda apasionada
cuenta más la persecución que el
objeto perseguido"*

—El Tao del Jeet Kune Do” (1975), Bruce Lee

¿Centro de excelencia?



- **2 centros en Extremadura**
- **45+21 centros en toda España (solo 3 ciber)**
- **Financiación = instalaciones + equipamiento**
- **Formación para el profesorado**
- **Actividades para el alumnado**
- **Prestigio**
- **Trabajo extra por y para el alumnado**



Proyecto Primario 3



Introducción de los Principios de Ciberseguridad en los Currículos de FP de la familia de Informática y Comunicaciones



Herramientas de análisis de vulnerabilidades





¿Qué es la seguridad en las aplicaciones informáticas?



¿En qué fase del desarrollo software tenemos que introducirla?



Perdón que entonces esta va antes...

¿Cuántas fases tenemos dentro del desarrollo software?

¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con las responsabilidades de los Técnicos de Operación?





...esta también está antes entonces:

¿qué es una debilidad y a que elementos afecta? ¿y una vulnerabilidad?



... y para terminar, al grano:

¿cómo puedo ver si mis
equipos y sistemas son
vulnerables?

Contenidos

01 Seguridad en el ciclos de desarrollo Software

02 Principales amenazas de seguridad relacionadas con técnicos de operación

03 Mitigación y/o corrección de vulnerabilidades

04 Herramientas de análisis de vulnerabilidades

05 Conclusiones

01. Seguridad en el ciclos de desarrollo Software

¿Qué es el SDLC?

El SDLC es el ciclo de vida de desarrollo software

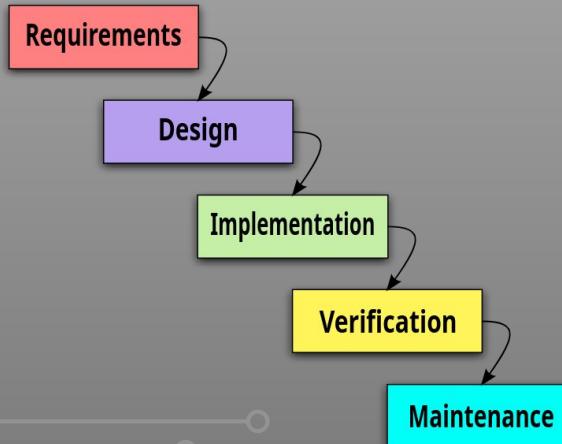
Fases del SDLC

- Planificación
- Análisis
- Diseño
- Implementación
- Pruebas
- Integración
- Mantenimiento

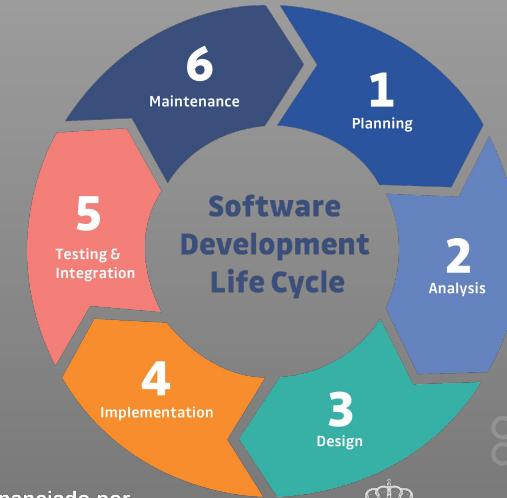
01. Seguridad en el ciclos de desarrollo Software

¿Cómo se desarrollan estas fases?

- Módelo Clásico o en cascada



- Modelos circular, en espiral y ágil



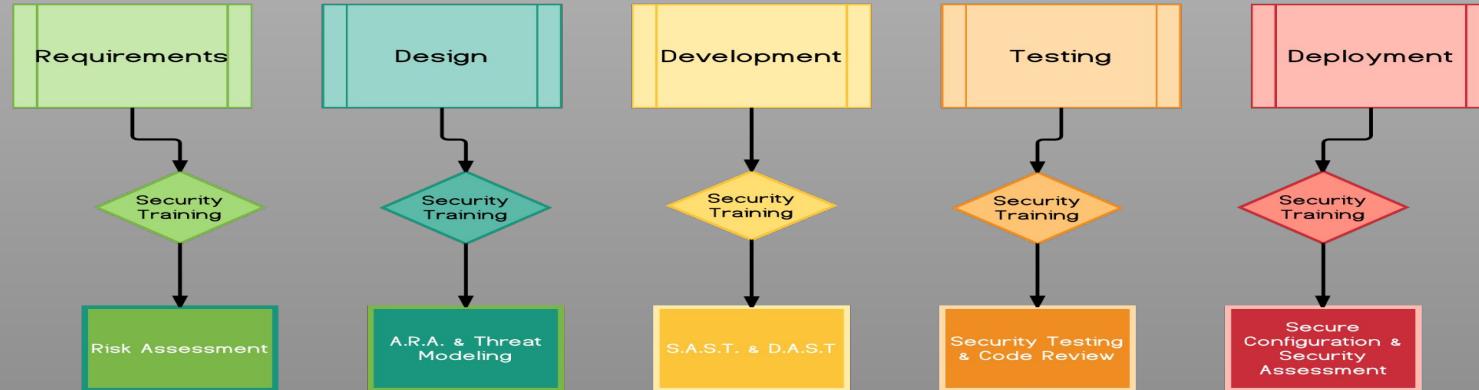
01. Seguridad en el ciclos de desarrollo Software

La pregunta es...

¿En cuál de estas fases introduzco la seguridad?

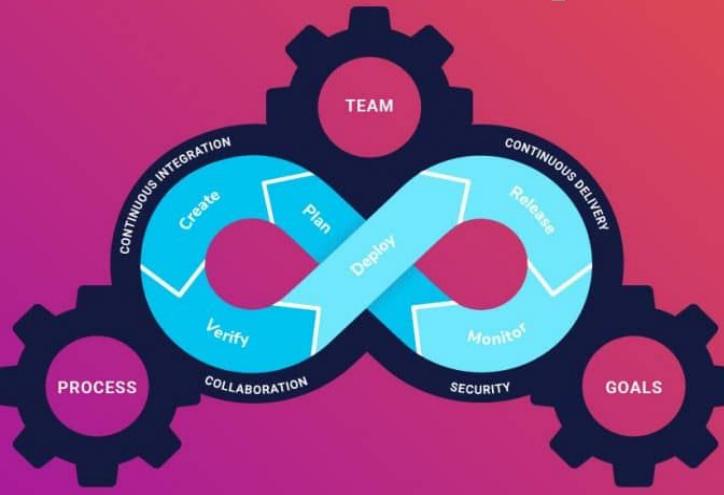
01. Seguridad en el ciclos de desarrollo Software

FROM SDLC TO S-SDLC



01. Seguridad en el ciclos de desarrollo Software

DevSecOps



JUNTA DE EXTREMADURA



Plan de
Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU

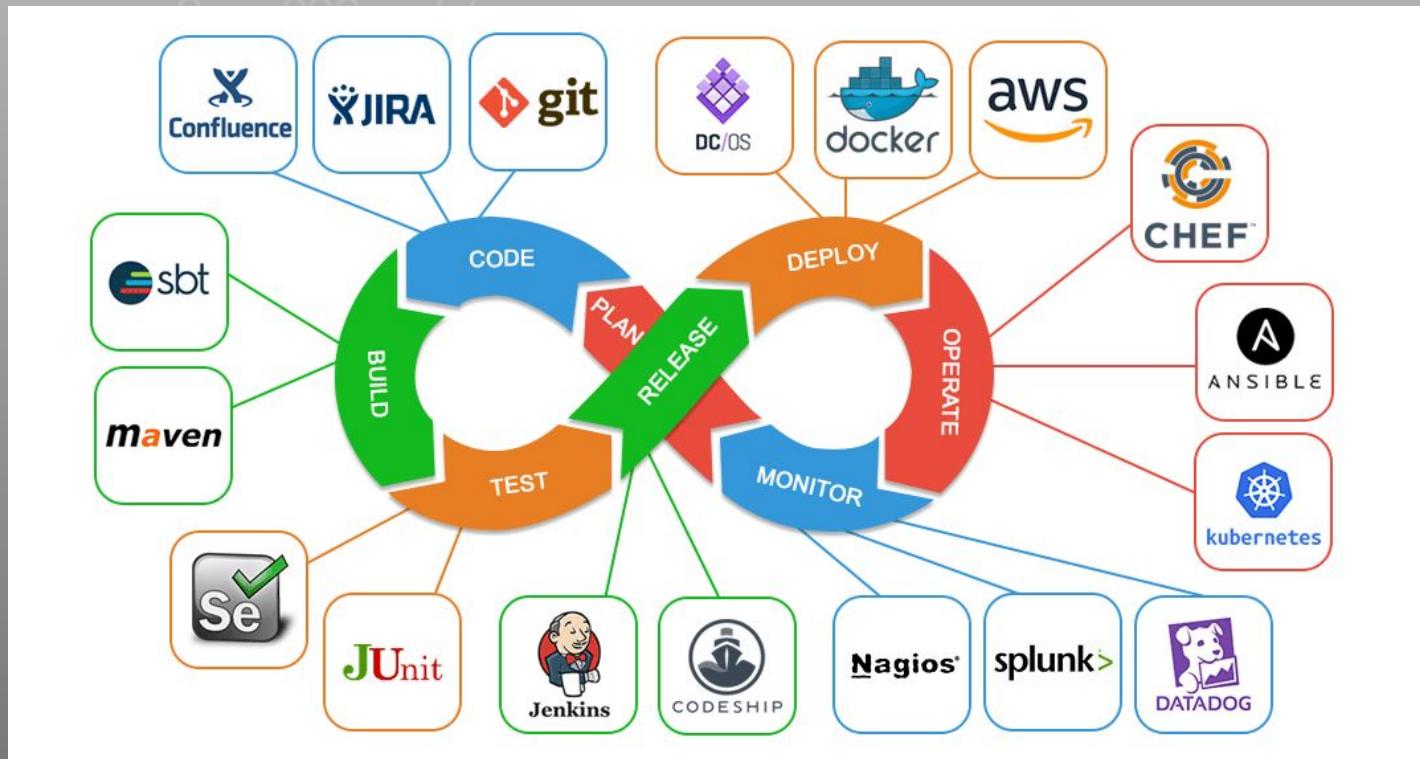


Fases del SDLC

- Planifica
- Construye
- Integración y Despliegue continuo
- Operación
- Observación
- Feedback continuo

01. Seguridad en el ciclos de desarrollo Software

Herramientas en DevOps



02. Principales amenazas de seguridad relacionadas con el desarrollo de software

¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con los Técnicos de Operaciones?



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

¿qué es una debilidad y a que elementos afecta? ¿y una vulnerabilidad?



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

Conceptos de ciberseguridad

- Sistema
- Activos
- Debilidad



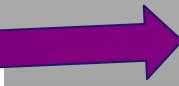
- Vector de ataque
- Vulnerabilidad
- Amenaza
- Ataque



Vector de ataque



Debilidad



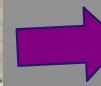
Vulnerabilidad



Amenaza



Ataque



Nuestros Activos



Nuestro Sistema
Informático o
aplicación

02. Principales amenazas de seguridad relacionadas con los técnicos de operación

Organismos y organizaciones

Estas organizaciones mantienen bases de datos e información sobre debilidades, vulnerabilidades etc. También han establecido estándares de seguridad web, que son directrices y prácticas recomendadas para desarrollar, probar y mantener aplicaciones web seguras. Ayudan a prevenir, detectar y mitigar vulnerabilidades y amenazas web comunes.



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

CWE (Common Weakness Enumeration) es una lista de tipos de debilidades de software dirigida a desarrolladores y profesionales de la seguridad,

Se puede ver como un catálogo de debilidades documentadas que se suelen cometer programando, y que podría derivar en vulnerabilidades.

Es muy utilizada por distintas herramientas de seguridad encargadas de identificar estas debilidades y para promover la identificación de las vulnerabilidades, mitigación y su prevención.

CWE satisface la necesidad que tienen las grandes organizaciones de conocer y tener catalogadas las distintas debilidades existentes, permitiendo asegurar sus productos frente a fallos de seguridad ya conocidos.



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

CVE (Common Vulnerabilities and Exposures) es una lista de vulnerabilidades de seguridad de la información públicamente conocidas.



Es quizás el estándar más usado. Permite identificar cada vulnerabilidad, asignando a cada una un código de identificación único.

Se conoce como identificador CVE (CVE-ID) y está formado por las siglas de este diccionario seguidas por el año en que es registrada la vulnerabilidad o exposición y un número arbitrario de al menos cuatro dígitos según el siguiente formato:

CVE-2013-7518		
Siglas de Common Vulnerabilities and Exposures	Año de registro	Número de cuatro cifras asignado a la vulnerabilidad

02. Principales amenazas de seguridad relacionadas con los técnicos de operación

CAPEC (Common Attack Pattern Enumeration and Classification) es un catálogo en forma de esquema de clasificación exhaustiva de patrones de ataque con información relativa a ellos.

Las entradas de esta lista intentan dar a conocer la perspectiva del atacante y los métodos utilizados para explotar los sistemas.

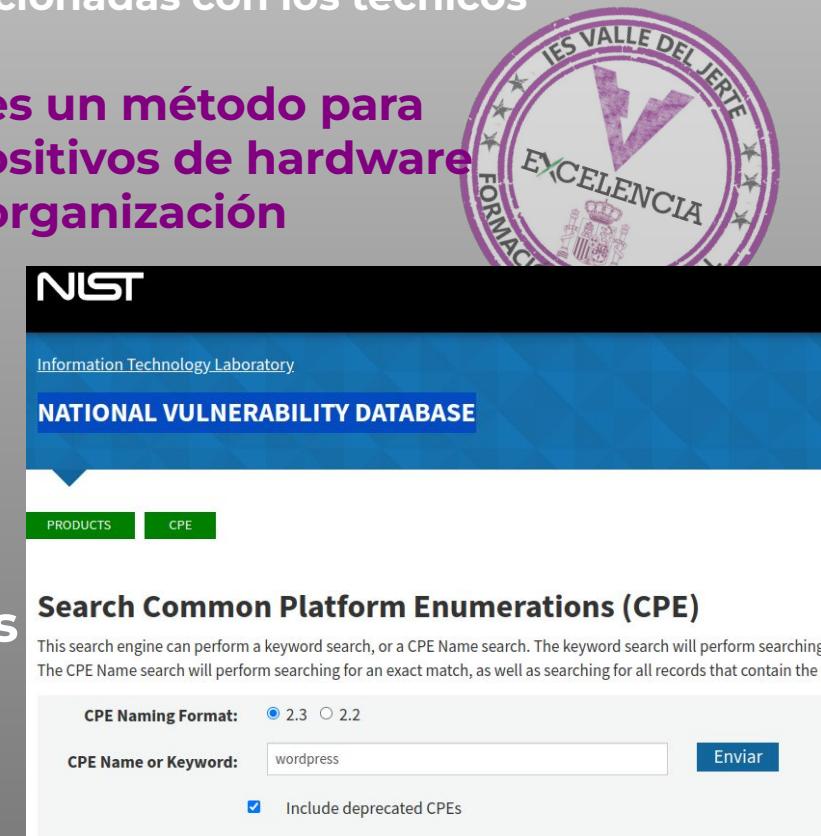
Al igual que los demás catálogos, CAPEC intenta ofrecer la información necesaria para ayudar a mejorar la seguridad en todo el ciclo de vida de desarrollo de software y también apoyar las necesidades de los desarrolladores.



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

CPE (Common Platform Enumerations) es un método para identificar sistemas, aplicaciones y dispositivos de hardware que forman parte de los activos de una organización

En este caso dentro de la NVD (National Vulnerability Database) del NIST, podemos hacer una búsqueda por palabras clave (Sistema Operativo, software, hardware, plataforma, etc. teniendo acceso a las vulnerabilidades asociadas con ellos.



NIST
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

PRODUCTS | CPE

Search Common Platform Enumerations (CPE)

This search engine can perform a keyword search, or a CPE Name search. The keyword search will perform searching...
The CPE Name search will perform searching for an exact match, as well as searching for all records that contain the

CPE Naming Format: 2.3 2.2

CPE Name or Keyword:

Include deprecated CPEs

Enviar

02. Principales amenazas de seguridad relacionadas con los técnicos de operación

¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con las responsabilidades de los Técnicos de Operación?



02. Principales amenazas de seguridad relacionadas con los técnicos de operación

Del top 10 de los principales riesgos del 2023 según la organización OWASP nos encontramos con que los siguientes tienen que ver con las fases de despliegue, operación y observación:



- Rotura del control de acceso
- Fallos criptográficos
- Configuración de seguridad defectuosa

- Componentes vulnerables y obsoletos
- Fallos de identificación y autorización
- Fallos de integridad de software y datos
- Fallos en el registro y la supervisión de la seguridad
- Falsificación de Solicitud del Lado del Servidor SSRF

03. Mitigación y/o corrección de vulnerabilidades

Y... ¿Qué puedo hacer yo como Técnico de Operaciones para prevenirlo o mitigarlo?



03. Mitigación y/o corrección de vulnerabilidades

- Formarnos e informanos.
- Introducir la seguridad en todo el ciclo de desarrollo software
- Controlar y tener actualizados los Sistemas y Aplicaciones que utilizamos.
- Establecer sistemas y políticas apropiadas para el control de acceso



03. Mitigación y/o corrección de vulnerabilidades

- Controlar los registros del sistema.
- Testear las vulnerabilidades conocidas.
- Implementar políticas eficaces de autorización y permisos.
- Implementar y mantener herramientas y escudos de red: firewall, WAF, etc.

Y aparte de todo esto:



03. Mitigación y/o corrección de vulnerabilidades

- Utilizar herramientas de detección de vulnerabilidades:
 - SAST: Análisis estático de código
 - DAST: Análisis dinámico
 - IAST (interactivo), etc...



04. Herramientas de análisis de vulnerabilidades

Las herramientas de análisis de vulnerabilidades son capaces de detectar los problemas que tienen nuestras aplicaciones, por lo tanto nos dan una medida de la calidad de nuestro código.

Tenemos diferentes tipos de herramientas:

- SAST: Análisis estático de código. Realizan pruebas de caja blanca, es decir analizan directamente el código en busca de las vulnerabilidades.
- DAST: Análisis dinámico de código. En este caso realizan pruebas de caja negra, es decir, analizan el funcionamiento (atacan) para buscar fallos o vulnerabilidades.
- IAST: Análisis interactivo: estas herramientas se encuentran en el servidor y necesitan interactuar con la aplicación, pudiendo necesitar acceder también al código
- HAST o híbridas: es la combinación de distintos tipos de análisis en una solución.



04. Herramientas de análisis de vulnerabilidades

Escaneo de red con nmap

Nmap es una comando que nos permite escanear equipos en una red y obtener los:

- Equipos presentes.
- Puertos abiertos
- Servicios
- Sistemas Operativos
- Versiones, etc...

Una vez que conocemos estos datos podemos buscar si hay algún elemento susceptible de posibles vulnerabilidades.



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades

En este caso Nessus es una herramienta con la cual vamos a poder escanear un equipo o red y nos va a dar un informe de las vulnerabilidades presentes en los objetivos escaneados.

Una vez conocemos las vulnerabilidades presentes, podríamos intentar explotar esas vulnerabilidades mediante los procedimientos específicos para ella.



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades

Creamos un contenedor docker creando un archivo con nombre docker-compose.yml con el siguiente contenido:

```
# Nessus Vulnerability Scanner
version: '3.3'
services:
  nessus:
    image: jmmedinac03/nessus_plugins
    # acceso a la máquina por https://localhost:8834
    # creado usuario:usuario passwd:usuario
    ports:
      - 8834:8834
```

Y accedemos a través de navegador por <https://localhost:8834>(https://ip_maquina:8834) con usuario:usuario y password:usuario



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades

Scan Templates

[Back to Scans](#)

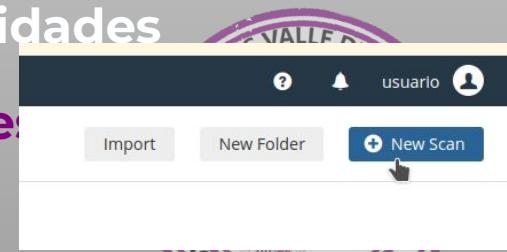
Scanner

DISCOVERY

- Host Discovery**
A simple scan to discover live hosts and open ports.

VULNERABILITIES

- Basic Network Scan**
A full system scan suitable for any host.
- Advanced Scan**
Configure a scan without using any recommendations.
- Advanced Dynamic Scan**
Configure a dynamic plugin scan without recommendations.
- Malware Scan**
Scan for malware on Windows and Unix systems.
- Mobile Device Scan**
Assess mobile devices via Microsoft Exchange or an MDM.
- Web Application Tests**
Scan for published and unknown web vulnerabilities using Nessus Scanner.
- Credentialed Patch Audit**
Authenticate to hosts and enumerate missing updates.
- Intel AMT Security Bypass**
Remote and local checks for CVE-2017-5689.
- Spectre and Meltdown**
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware**
Remote and local checks for MS17-010.
- Ripple20 Remote Scan**
A remote scan to fingerprint hosts potentially running the Trekk stack in the network.
- Zerologon Remote Scan**
A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).
- Solorigate**
Remote and local checks to detect.
- ProxyLogon : MS Exchange**
Remote and local checks to detect.
- PrintNightmare**
Local checks to detect the.
- Active Directory Starter Scan**
- Log4Shell**
Detection of Apache Log4j CVE-2021-44228.
- Log4Shell Remote Checks**
Detection of Apache Log4j CVE-2021-44228.

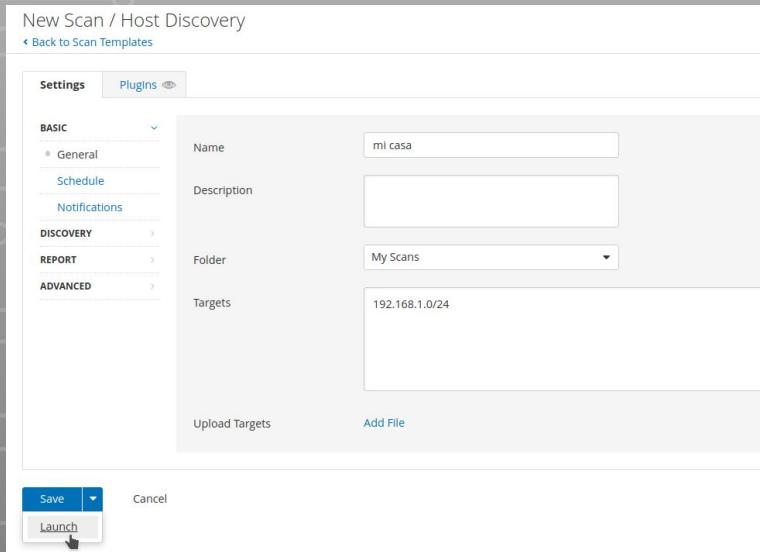


Creamos un nuevo escaneo.
Elegimos el tipo de escaneo
sobre todas las opciones:

- **Host Discovery** para encontrar equipos y puertos abiertos
- **Basic Network** para un escaneo de la red
- **Advanced** para escaneo en profundidad

04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades



New Scan / Host Discovery

Back to Scan Templates

Settings Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

REPORT

ADVANCED

Name: mi casa

Description:

Folder: My Scans

Targets: 192.168.1.0/24

Upload Targets Add File

Save Launch

Crear un escaneo es sencillo:

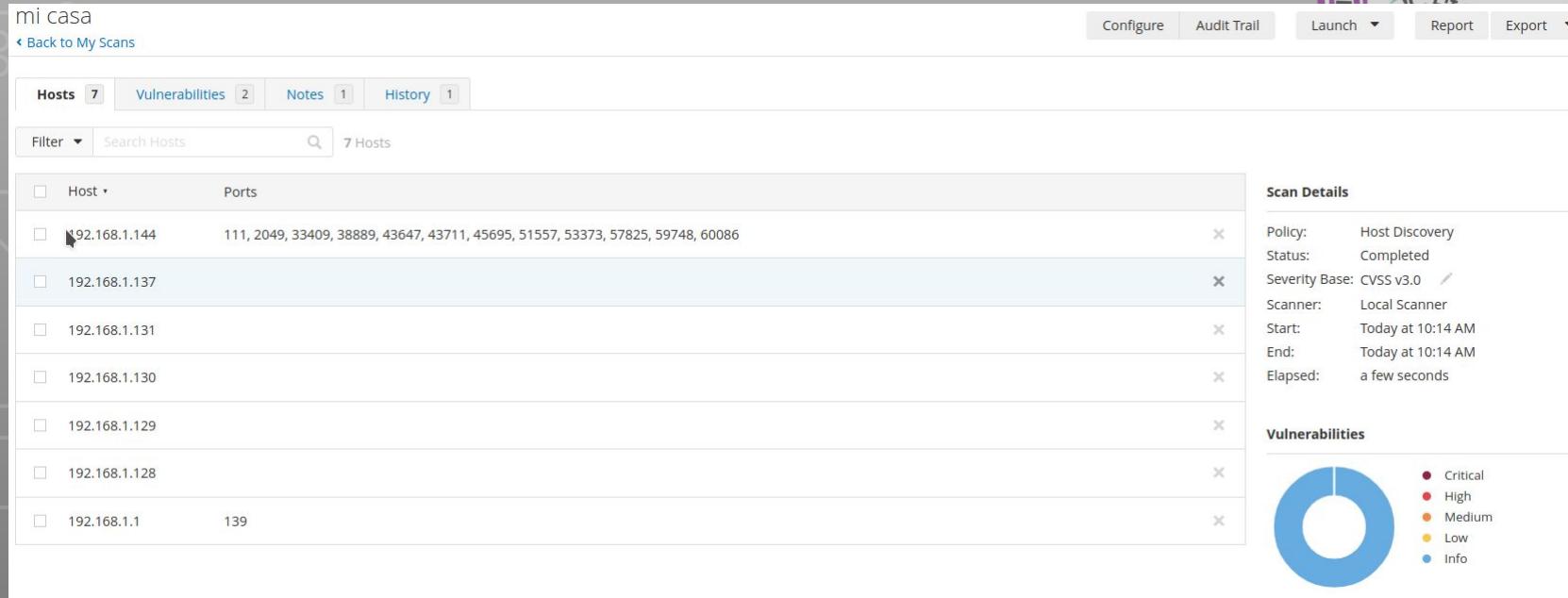
- Ponemos nombre de escaneo.
- Indicamos el destino en forma:
IP red o equipo/ máscara de red

Después de darle a **Save** o **Launch** comenzará el escaneo y luego podremos ver los resultados



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades



The screenshot shows the Nessus web interface with the following details:

- Scan Name:** mi casa
- Scan Status:** Completed
- Severity Base:** CVSS v3.0
- Scanner:** Local Scanner
- Start:** Today at 10:14 AM
- End:** Today at 10:14 AM
- Elapsed:** a few seconds

Scan Details:

Host	Ports	Status
192.168.1.144	111, 2049, 33409, 38889, 43647, 43711, 45695, 51557, 53373, 57825, 59748, 60086	Up
192.168.1.137		Up
192.168.1.131		Up
192.168.1.130		Up
192.168.1.129		Up
192.168.1.128		Up
192.168.1.1	139	Up

Vulnerabilities:

- Critical: 0
- High: 0
- Medium: 0
- Low: 0
- Info: 0

04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades

Sobre un escaneo avanzado vemos cómo nos aparecen vulnerabilidades, de las que podemos ver detalles.

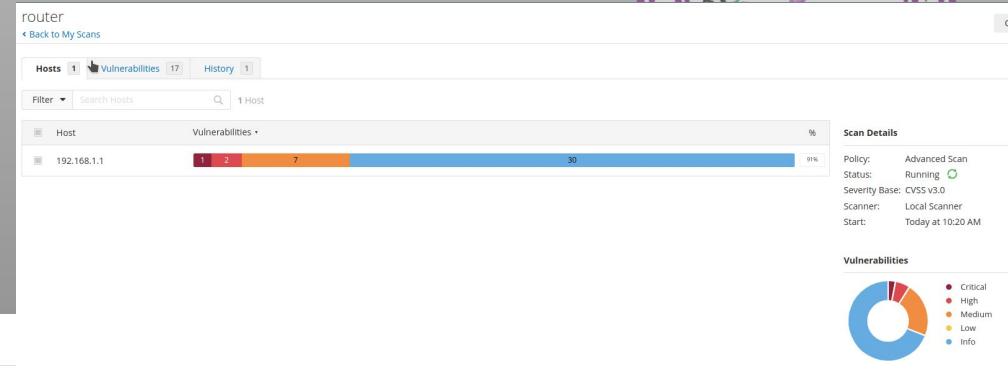
router

< Back to My Scans

Hosts 1 Vulnerabilities 20 History 1

Filter Search Vulnerabilities 20 Vulnerabilities

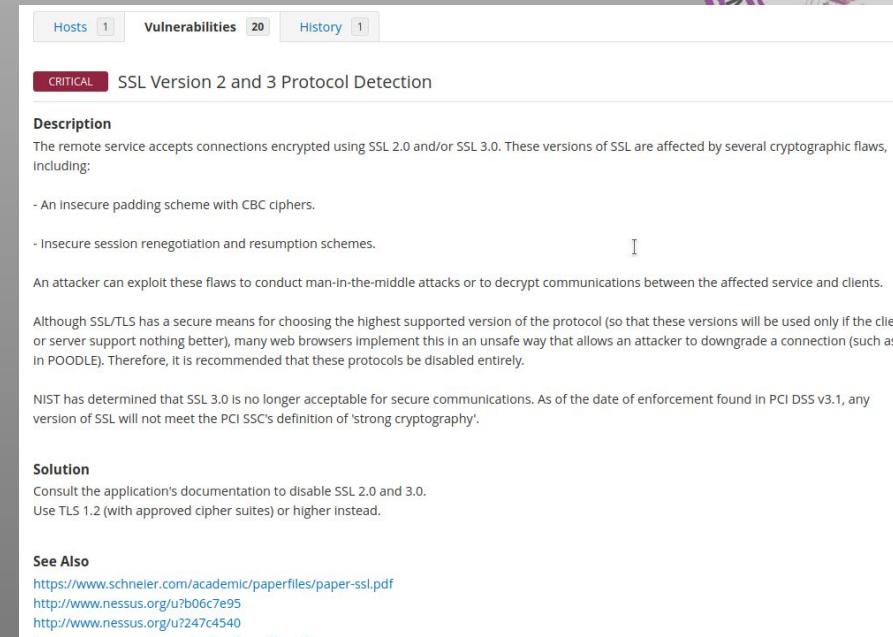
Sev	CVSS	VPR	Name	Family	Count
Critical	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	1
High	7.5		SSL Certificate Signed Using Weak Hashing Algorithm	General	1
Mixed			SSL (Multiple Issues)	General	10



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades

Al pulsar sobre una vulnerabilidad en concreto podemos acceder información sobre la vulnerabilidad, por qué se produce, y también cómo solucionarla o mitigarla.



The screenshot shows the Nessus interface with the 'Vulnerabilities' tab selected, displaying 20 findings. A specific finding is highlighted:

CRITICAL SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also
<https://www.schneler.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u/b06c7e95>
<http://www.nessus.org/u/247c4540>



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades



JUNTA DE EXTREMADURA



Plan de
Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU



Y DEPORTES

04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades



JUNTA DE EXTREMADURA



Plan de
Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU



04. Herramientas de análisis de vulnerabilidades

Nessus: herramienta de escaneo de vulnerabilidades



JUNTA DE EXTREMADURA



Plan de
Recuperación,
Transformación
y Resiliencia



Financiado por
la Unión Europea
NextGenerationEU





Si te has quedado con ganas... para ampliar:

JUNTA DE EXTREMADURA



Financiado por
la Unión Europea
NextGenerationEU



Agradecemos tu colaboración

Por favor rellena el
siguiente
formulario para
evaluar la actividad:



Y ahora una competición:

Accede al siguiente enlace,
completa las misiones y sé
el primero en capturar las
banderas:

<https://ctf-he.iesvjp.es:35888/>



Gracias!

¿Alguna pregunta?



informatica.iesvalledeljerteplasencia.es



coordinacion.cenfp@iesvp.es



C/ Pedro y Francisco González, s/n
10600, Plasencia (Cáceres)



927 01 77 74



Las imágenes utilizadas corresponden al repositorio de wikimedia Commons, Wonderlane y están protegidos por la licencia Creative Commons.

**Imagen de herramientas de DevOps perteneciente a geniusitt.com
Logo de OWASP de OWASP Fundation.**



informatica.iesvalledeljerteplasencia.es



coordinacion.cenfp@iesvp.es



C/ Pedro y Francisco González, s/n
10600, Plasencia (Cáceres)



927 01 77 74

