

# 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**





JUNTA DE EXTREMADURA

 Plan de  
Recuperación,  
Transformación  
y Resiliencia



Financiado por  
la Unión Europea  
NextGenerationEU



# 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



JUNTA DE EXTREMADURA

 Plan de Recuperación, Transformación y Resiliencia



Financiado por la Unión Europea  
NextGenerationEU

 MINISTERIO  
DE EDUCACIÓN,  
FORMACIÓN PROFESIONAL  
Y DEPORTES





# ¿Qué es la seguridad en las aplicaciones informáticas?

# ¿De dónde provienen las principales amenazas o vulnerabilidades?





**...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** Conceptos de ciberseguridad

**02** Principales amenazas de seguridad

**03** Herramientas de análisis de vulnerabilidades

**04** Conclusiones



## 02. Principales amenazas de seguridad

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

## 02. Principales amenazas de seguridad

### 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

### 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

**¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con los usuarios y profesionales de la informática?**



## 02. Principales amenazas de seguridad sobre los usuarios

### 🔑 Contraseñas débiles o repetidas

- Facilitan el robo de cuentas.
- ✓ Usa contraseñas únicas y largas. Mejor con gestor de contraseñas.

### ✉️ Phishing (correos o mensajes falsos)

- Roban tus datos haciéndose pasar por empresas conocidas.
- ✓ Desconfía de enlaces raros y verifica el remitente.

### 💻 Malware en descargas o apps

- Pueden espiar o dañar tu equipo.
- ✓ Descarga solo de sitios oficiales. Usa antivirus.

## 02. Principales amenazas de seguridad sobre los usuarios

### Guardar datos personales sin protección

→ Riesgo si te roban el móvil o el PC.

 Usa PIN, huella y, si puedes, cifrado



### Exceso de información en redes

→ Te expone a robos o suplantaciones.

 Cuida tu privacidad y revisa lo que publicas.

### Wi-Fi públicas sin protección

→ Otros pueden interceptar tu conexión.

 No accedas a cuentas importantes. Usa

VPN.



### Ingeniería social

→ Te engañan para que des información o acceso.



Siempre duda: ni soporte técnico ni “amigos” piden contraseñas

## PRINCIPALES RIESGOS DE SEGURIDAD COMO USUARIOS



### Contrasenas débiles o reutilizadas

Que algulen acceda a tus cuentas (Gmail, Instagram, Netflix, etc.)

Ejemplo: U-123456 or la misma passívora para c/todo.



### Phishing (engaños por correo, WhatsApp, SMS...)

Robar datos personales o contraseñas mediante mensajes falsos

Ejemplo: "Tu paquete está retenido, paga 2.99 €"

Andóes: No abrir enlaces sospechosos ni introducir datos si no estás seguro del origen.



### Malware en descargas o apps

Instalar un programa malicioso sin saberlo

Ejemplo: Descargar software pirata de sitios dionéuos

Andave: Descargar solo de fuentes oficiales



### Guardar información sensible sin protección

Que otros accedan a información privada o comprometedora. Tener M fotos, claves o documentos bancaria o sin tener ninguna protección

Andave: Activar el bloqueo por PIN, huella o reconocimiento facial



### Uso inseguro de redes Wi-Fi públicas

Alguien en la misma red puede interceptar tu tráfico

Ejemplo: Utilizar la Wi-Fi de aeropuerto para instagrama

Andave: No acceder a servicios sensibles desde



### Compartir demasiada información en redes sociales

Exposición a robos, acoso, suplantación de identidad

es amenazas de seguridad sobre los



[Infografía sobre riesgos de seguridad](#)



... y para terminar, al grano:

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



... Accede al siguiente repositorio:

<https://github.com/jmmedinac03v/jp/IntroduccionCiberseguridad.git>

## 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.



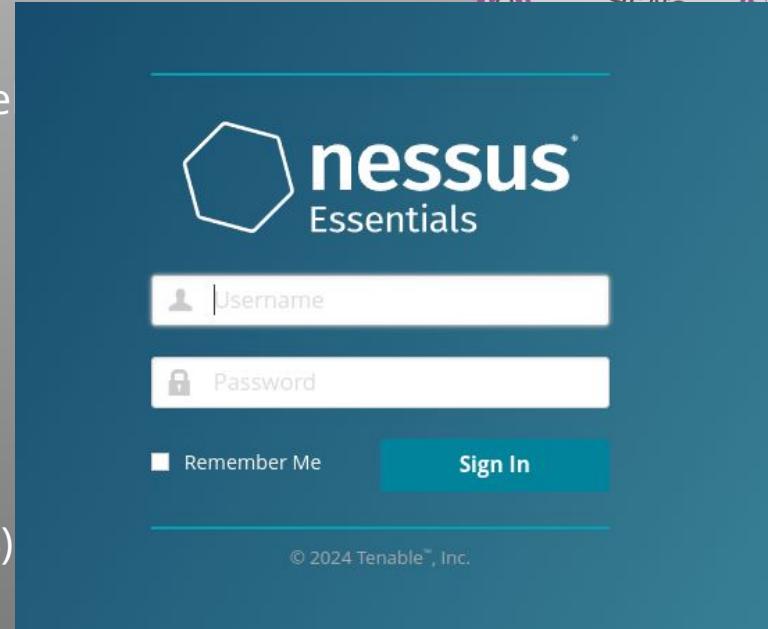
## 04. Herramientas de análisis de vulnerabilidades

### 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](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](#)

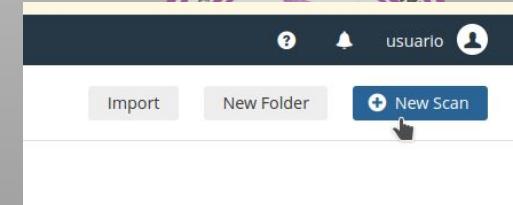
**Scanner**

**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).
-  Soligrate  
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  
Plan de Recuperación, Transformación y Resiliencia
-  Log4Shell  
Detection of Apache Log4j CVE-2021-44228
-  Log4Shell Remote Checks  
Detection of Apache Log4j CVE-2021-44228

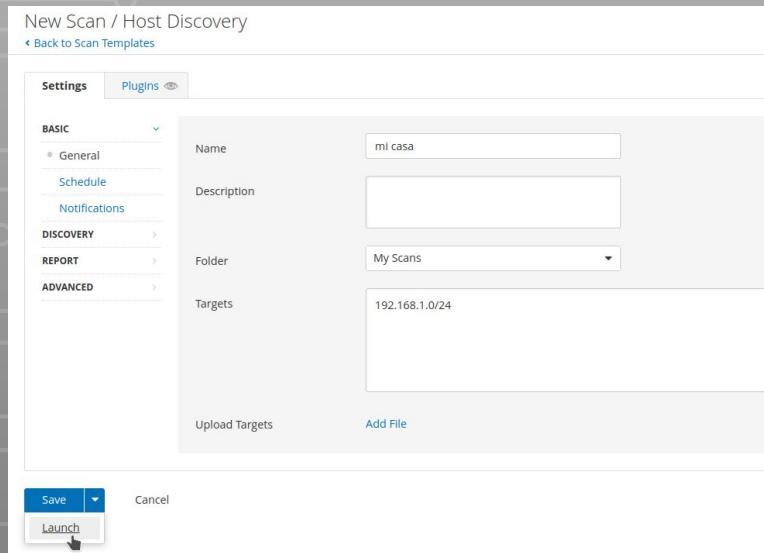


Creamos un nuevo escaneo.  
Elegimos el tipo de escaneo  
sobre todas las opciones:

- **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 Cancel

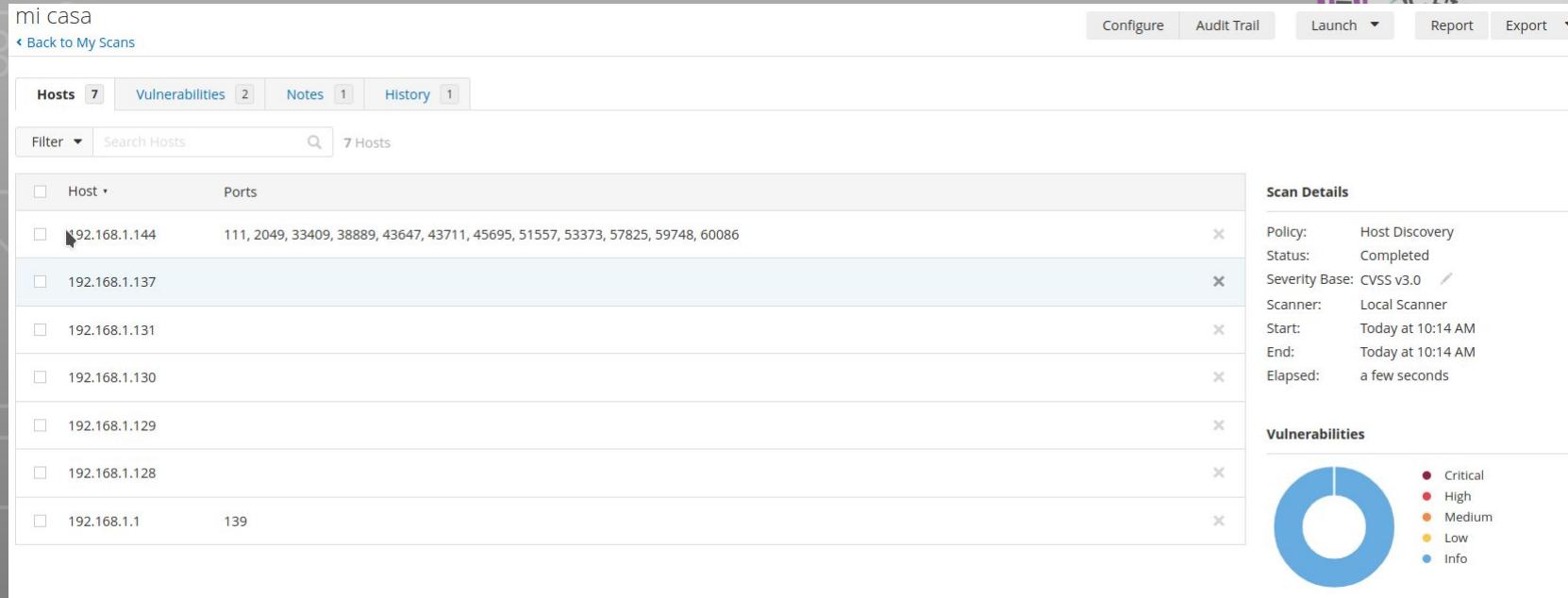
Crear un escaneo es sencillo:

- 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

router

< Back to My Scans

Hosts 1 Vulnerabilities 17 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.1.1	1 2 7

Scan Details

- Policy: Advanced Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:20 AM

Vulnerabilities



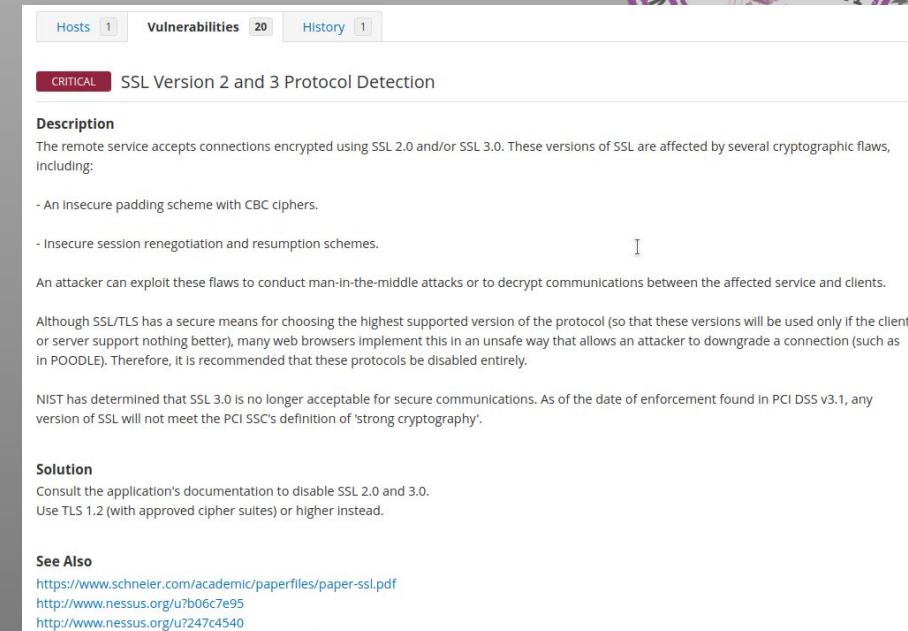
Detailed Vulnerability Data:

Severity	Count
Critical	1
High	2
Medium	7
Low	30
Info	91%

## 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>



# Gracias!

¿Alguna pregunta?



[informatica.iesvalledeljerteplasencia.es](http://informatica.iesvalledeljerteplasencia.es)



[coordinacion.cenfp@iesvp.es](mailto: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](http://informatica.iesvalledeljerteplasencia.es)



[coordinacion.cenfp@iesvp.es](mailto:coordinacion.cenfp@iesvp.es)



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



927 01 77 74

