

curso “Experto en Ciberseguridad de Redes y Sistemas”

TEMAS

1. Fingerprinting
2. Footprinting
3. IDSs - Snort
4. Nessus
5. Firewalls
6. SGSI
7. Antiphishing
8. MITRE
9. Red Team y Blue Team
10. Principales procesos de Seguridad



Nessus

4.1 Nessus – Introducción

Nessus es una de las herramientas más conocidas en el ámbito de la ciberseguridad para la **detección de vulnerabilidades** en sistemas informáticos. Se utiliza para analizar redes, servidores, aplicaciones y dispositivos con el objetivo de identificar fallos de seguridad antes de que puedan ser explotados por atacantes.

¿Qué hace Nessus?

Nessus realiza escaneos automatizados que permiten:

- Detectar vulnerabilidades conocidas
- Identificar configuraciones inseguras
- Evaluar el estado de parches y actualizaciones
- Analizar servicios expuestos en red

Gracias a su amplia base de datos de plugins, es capaz de detectar miles de posibles riesgos en distintos entornos.

Importancia en ciberseguridad

Hoy en día, Nessus es una herramienta clave en:

- Auditorías de seguridad
- Tests de penetración (pentesting)
- Cumplimiento normativo (compliance)

Su facilidad de uso y potencia lo convierten en una opción muy extendida tanto en pequeñas empresas como en grandes organizaciones.

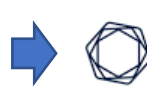
Un poco de historia

Nessus fue desarrollado en 1998 por **Renaud Deraison** como un proyecto de código abierto. En sus inicios, se convirtió rápidamente en una herramienta muy popular entre administradores de sistemas y profesionales de seguridad.

Con el tiempo, el desarrollo pasó a manos de la empresa Tenable, Inc., que transformó Nessus en una solución comercial.



Nessus
vulnerability scanner



tenable Nessus

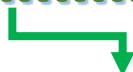


¿No hay Opción gratuita?



Aun así, sigue existiendo una versión gratuita limitada llamada **Nessus Essentials**, orientada a uso educativo o personal.

¡!!! SÍ!!!!!!! !!!



<https://es-la.tenable.com/products/nessus/nessus-faq>

tenable Nessus

A fecha de hoy sigue existiendo esta opción gratuita... pero Tenable no nos lo pone fácil para encontrarla... así que para trabajar con esta herramienta, abre esta URL:

<https://es-la.tenable.com/products/nessus/nessus-faq>

Que es la versión que se presenta a continuación.

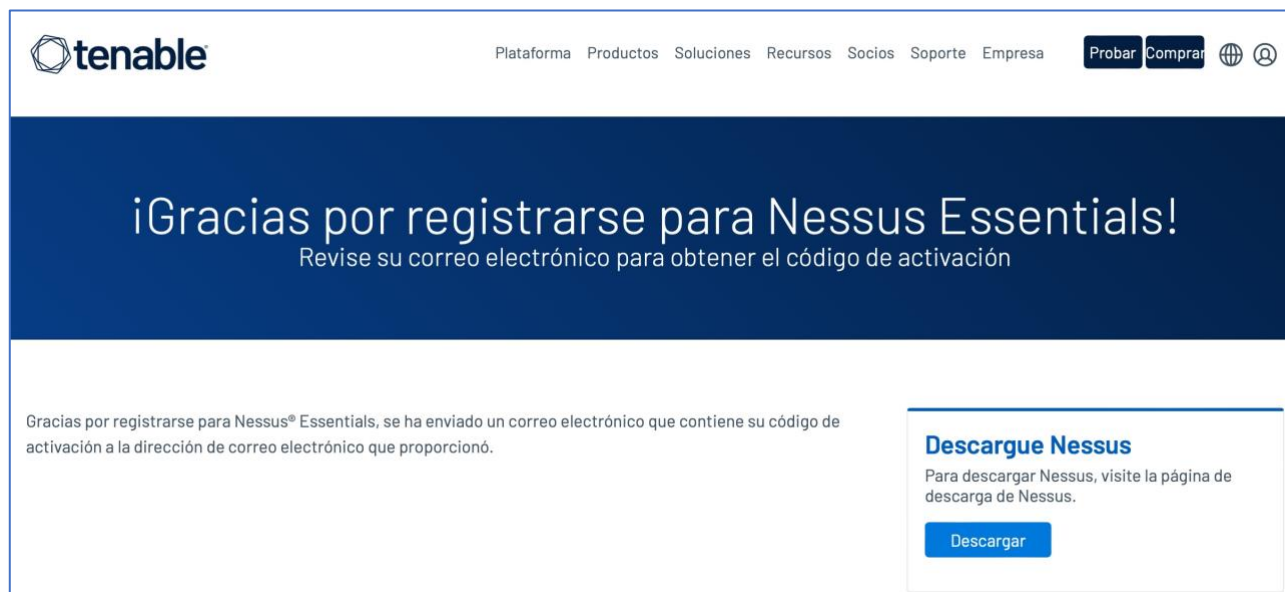
Ofertas de Nessus:

Esta sección contiene detalles de tres ofertas de Nessus, Nessus Expert, Nessus Professional y Nessus Essentials

¿En qué se distinguen las diferentes ofertas?

- **Nessus Essentials:** esta es nuestra oferta de introducción de Nessus orientada a educadores, estudiantes e individuos que inician sus carreras en ciberseguridad. Usted puede usar esta herramienta de manera gratuita para escanear sus activos de TI para fines educativos o incluso en su home office (hasta 16 IP).
- **Nessus Professional:** este es el primer paso hacia ofertas de Nessus más avanzadas, diseñadas para consultores, evaluadores de penetración y SMB. Nessus Professional proporciona escaneos de TI que se pueden usar en cualquier lugar para detectar vulnerabilidades.
- **Nessus Expert:** esta es nuestra oferta premium de Nessus que recomendamos de sobremanera para todos los consultores, evaluadores de penetración, desarrolladores y SMB. Nessus Expert, diseñado para la superficie de ataque moderna, le permite ir más allá de sus activos de TI tradicionales al fortalecer sus aplicaciones web, proteger su infraestructura en la nube y obtener visibilidad de su superficie de ataque conectada a Internet.

Una vez que abres la web de Tenable (en la ruta indicada arriba) te pedirá nombre y email, y quedarás registrado, tal cual se muestra en la imagen de abajo, y te permitirá descargar esta versión.



Nos presentará un acuerdo que debemos aceptar, y una vez hecho esto, nos dará la bienvenida y nos dirá nuestro número de activación, que debemos copiar y guardar, pues nos lo pedirá luego durante la instalación, tal cual se presenta en la imagen de la derecha.

Activating Your Nessus Essentials License
Your activation code for Nessus Essentials is:
PSXX-XXXX-XXXX-XXXX-XXXX

Con todo esto:

!!! NOS VAMOS A UNA INTERFAZ DE LÍNEA DE COMANDOS !!!

Pero... lo dejaremos para el próximo capítulo, por ahora podemos ir descargando la documentación oficial que la encontramos en:

<https://docs.tenable.com/nessus/command-line-reference/Content/PDF/CommandLineReference.pdf>

NOTA: Como ya has visto en charlas anteriores, en estos videos se hace referencia a “**Auditoría remota**”. Este tema, está desarrollado en una serie de videos de nuestro ciclo “Aprendiendo Ciberseguridad paso a paso” y son los videos 77 a 87. No forman parte del curso de Experto, pero

sí te recomendamos que les des una mirada, pues descubrirás una herramienta fundamental para el trabajo de auditoría de redes y sistemas.

Vamos a ver el tema con más detalle en el video 111 **(Obligatorio)**.

 **Nessus - (Parte 1) - Charla 111** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/XAij4AvwaE4>



4.2 Nessus – Línea de comandos

En este tema, avanzaremos sobre la línea de comandos, que recordaros, tenéis toda la información en el manual que en el tema anterior os recomendamos descargar de:

<https://docs.tenable.com/nessus/command-line-reference/Content/PDF/CommandLineReference.pdf>

Todos los comandos los ejecutaremos en nuestro Kali Linux, a través de una consola.

A lo largo de este capítulo iremos ejecutando toda la serie de comandos que se presenta a continuación:

```
sh-3.2# locate nessusd
/Library/Nessus/run/sbin/nessusd
sh-3.2# locate nessuscli
/Library/Nessus/run/sbin/nessuscli

sh-3.2# ./nessuscli fetch --register PSXX-XXXX-XXXX-XXXX-XXXX
Your Activation Code has been registered properly - thank you.
Refreshing Nessus license information... complete; continuing with updates.

sh-3.2# ./nessuscli update --plugins-only
sh-3.2# ./nessuscli fetch --code-in-use
sh-3.2# ./nessusd stop
sh-3.2# ./nessuscli fix --reset
sh-3.2# ./nessuscli fetch --register <mi_Nro_registro>
sh-3.2# ./nessusd -R
sh-3.2# ./nessusd ← Para lanzar el demonio y la interfaz gráfica
```

Pero para comprenderlo en detalle, vamos a ver el tema en el video 112 **(Obligatorio)**.

 **Nessus - (Parte 2) - Charla 112** - Aprendiendo Ciberseguridad paso a paso

<https://youtu.be/WEhYpdS8FYk>



4.3 Nessus – Primeros ataques

En este tema, comenzamos a trabajar con la interfaz gráfica de Nessus.

La interfaz gráfica de Nessus está diseñada para ser intuitiva y accesible desde el navegador web, lo que facilita su uso tanto a principiantes como a profesionales de la ciberseguridad. Su estructura se basa en paneles claros y navegación lateral, permitiendo gestionar escaneos y analizar resultados de forma eficiente.

Panel principal (Dashboard)

Al iniciar sesión, el usuario accede a un **panel de control** que muestra un resumen visual del estado de seguridad:

- Número de vulnerabilidades detectadas
- Clasificación por severidad (crítica, alta, media, baja)
- Tendencias y gráficos de riesgo
- Actividad reciente de escaneos

Este panel permite tener una visión rápida de la situación general del sistema o red analizada.

Menú lateral de navegación

En la parte izquierda se encuentra el menú principal, desde donde se accede a las secciones clave:

- **Scans:** gestión de escaneos (crear, lanzar, programar)
- **Policies:** configuración de políticas de análisis
- **Plugins:** base de datos de vulnerabilidades
- **Settings:** ajustes generales de la herramienta

La navegación es sencilla y sigue una lógica jerárquica.

Gestión de escaneos

La sección de *Scans* permite:

- Crear nuevos análisis mediante plantillas
- Configurar objetivos (IP, dominios, redes)
- Definir credenciales para escaneos más profundos
- Programar ejecuciones automáticas

Cada escaneo aparece listado con su estado (completado, en progreso, fallido).

Visualización de resultados

Una vez finalizado un escaneo, Nessus ofrece informes detallados:

- Listado de vulnerabilidades con su nivel de gravedad
- Descripción técnica del problema
- Soluciones o recomendaciones
- Información del sistema afectado

Además, permite filtrar, ordenar y exportar los resultados en distintos formatos.

Experiencia de usuario

La interfaz destaca por:

- Uso de colores para identificar rápidamente riesgos
- Organización clara de la información
- Navegación fluida entre resultados y configuraciones

En conjunto, la interfaz de Nessus está orientada a facilitar el análisis de vulnerabilidades de forma visual, estructurada y eficiente.

Este tema, es eminentemente práctico por lo que directamente lo veremos en el video 113 (**Obligatorio**).

🌐 **Nessus - (Parte 3) - Charla 113** - Aprendiendo Ciberseguridad paso a paso
<https://youtu.be/ZAeHopQVrbA>



4.4 Nessus – Snort

En este tema, volvemos a trabajar con Snort, y nos basaremos en la metodología que se desarrolla en el artículo “**GENERACION DE ATAQUES / DETECCIÓN CON NIDS**” que podéis descargar en:

<https://darfe.es/download/metodologianessus-snort/?wpdmdl=38042&refresh=6a6d87127c5ea1785562898>

El trabajo que desarrollaremos es fundamental para cualquier arquitectura de redes y sistemas, pues nos permitirá analizar un patrón de tráfico generado desde Nessus con todo detalle, determinar cuál es el vector de este ataque y luego crear nuestra propia “local.rule” en Snort para poder detectarlo.

Este tipo de medidas es sumamente frecuente de encontrar en nuestras infraestructuras, por ejemplo cuando tenemos sistemas que por alguna razón no soporta cierta actualización y/o parche de seguridad, aparece una vulnerabilidad relacionada con esta versión desactualizada, pero no podemos hacer nada para mitigarla. En este tipo de situaciones, que reiteramos son frecuentes, una muy buena medida es dejar activa su detección en el IDS, y también, una vez identificada con toda certeza, se puede bloquear el patrón en un firewall.

Vamos a ver el tema con de forma práctica y con más detalle en el video 114 (**Obligatorio**).

🌐 **Nessus - Snort (Parte 4) - Charla 114** - Aprendiendo Ciberseguridad paso a paso
https://youtu.be/_lbEcENw4Eg



4.5 Nessus – NASL (parte 1)

El **NASL** (Nessus Attack Scripting Language) es un lenguaje de scripting diseñado específicamente para la herramienta de análisis de vulnerabilidades Nessus. Su principal función es permitir la creación de plugins personalizados que detectan fallos de seguridad en sistemas, redes y aplicaciones.

¿Qué es NASL?

NASL es un lenguaje interpretado, ligero y orientado a la seguridad. Fue desarrollado para facilitar la escritura de scripts que puedan ejecutar pruebas automatizadas sobre un objetivo, simulando posibles ataques o comprobaciones de vulnerabilidades.

Estos scripts, llamados *plugins*, son la base del funcionamiento de Nessus, ya que cada uno está diseñado para detectar un tipo concreto de problema.

Características principales

- **Lenguaje sencillo y específico:** su sintaxis es relativamente fácil de aprender, especialmente para tareas de seguridad.
- **Orientado a pruebas de red:** permite interactuar con servicios, puertos y protocolos.
- **Extensible:** los usuarios pueden crear sus propios plugins según sus necesidades.
- **Integración total con Nessus:** todos los escaneos utilizan scripts NASL para realizar comprobaciones.

Cómo funciona?

Durante un escaneo, Nessus ejecuta múltiples scripts NASL contra el objetivo. Cada script:

1. Comprueba si un servicio o puerto está activo
2. Analiza versiones de software
3. Busca vulnerabilidades conocidas
4. Genera un resultado con nivel de gravedad

Estos resultados se agrupan posteriormente en informes detallados.

Evolución e historia

NASL surgió junto con las primeras versiones de Nessus a finales de los años 90. En sus inicios, permitió que la comunidad de seguridad desarrollara y compartiera plugins de forma abierta.

Con la evolución de Nessus bajo Tenable, Inc., el uso de NASL se ha mantenido como parte fundamental del motor de escaneo, aunque gran parte del desarrollo de plugins es ahora gestionado por la propia empresa.

Importancia en ciberseguridad

El lenguaje NASL es clave porque:

- Permite automatizar auditorías de seguridad
- Facilita la detección temprana de vulnerabilidades
- Hace posible adaptar Nessus a entornos específicos

En resumen, NASL es el motor lógico detrás de Nessus, convirtiendo una herramienta de escaneo en un sistema flexible, potente y constantemente actualizado frente a nuevas amenazas.

¡Comenzamos con **NASL** (Nessus Attack Scripting Language)! y por si esto fuera poco, por medio de "línea de comandos" como venimos anunciando. Presentamos el empleo del lenguaje NASL. En este tema, veremos cómo es posible lanzar cualquiera de los miles de "plugins" que ya posee Nessus, pero en vez de hacerlo por medio de la interfaz gráfica, lo haremos por medio del comando "nasl" a través de línea de comandos. Como siempre, capturando y analizando todo con nuestra herramienta "Wireshark". Una vez comprendido el funcionamiento de "nasl", diseñaremos nuestros primeros scripts utilizando este lenguaje. Estaremos dando nuestros primeros pasos en programación nasl para Nessus, y verás "paso a paso" la potencia que esto nos ofrece para seguir avanzando en nuestro "footprinting" como especialistas en escaneos de vulnerabilidades.

Una vez más, este tema se desarrolla de forma eminentemente práctica en el video 115 (**Obligatorio**).

🌐 **Nessus - (Parte 5) - Charla 115 - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/uDJhnJ3MYwg>



4.6 Nessus – NASL (parte 2)

Seguimos con **NASL** (Nessus Attack Scripting Language) operando "Nessus" por "línea de comandos"... casi, casi como si ya fuéramos expertos en detectar vulnerabilidades.

En este capítulo, ya comenzaremos a operar abriendo "socks" TCP para analizar si el target o destino tiene abierto, o no, un determinado puerto, o como seguiremos viendo, todos los puertos que queramos. Finalmente, verás que prácticamente nos estamos programando nuestro propio "nmap" pero en lenguaje "nasl" y mezclando ya comandos "fi", "else", "open_sock_tcp".

Si sabes operar por **CLI** (Command Line Interface), logras acceder a un host y finalmente puedes escalar privilegios, has dejado desnudo al sistema operativo, tienes el control total y absoluto del mismo.

Nos basaremos en un artículo muy bueno que puedes descargar de la siguiente URL:

<https://litux.nl/mirror/networksecuritytools/0596007949/networkst-chp-1-sect-4.html>

Este tema es una continuación más avanzada del anterior, así que lo veremos directamente desde el video 116 (**Obligatorio**).

🌐 **Nessus - (Parte 6) - Charla 116 - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/EBZB7yMjeHU>

4.7 Nessus – NASL (parte 3)

En este capítulo, comenzaremos a lanzar NASL, prácticamente como si fuera "nmap" y luego, a través de bucles, vamos a ir abriendo puertos TCP y accediendo al nivel de aplicación, para terminar realizando una petición "GET" del protocolo http y analizando la respuesta del servidor Web. Todo esto capturándolo con Wireshark para visualizarlo en detalle.

Recordad que estamos tomando como referencia este artículo que puedes descargar de la siguiente URL:

<https://litux.nl/mirror/networksecuritytools/0596007949/networkst-chp-1-sect-4.html>

Vamos a ver el tema con más detalle en el video 117 **(Obligatorio)**.

🌐 **Nessus - (Parte 7) - Charla 117 - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/8piLeBWdXA>



4.8 Nessus – NASL (parte 4)

Seguimos avanzando con NASL, esta vez desarrollaremos más aún sobre los protocolos ftp y http y hasta haciendo los primeros pasos de un **"exploit"** con NASL. Luego veremos la capacidad de **"forge"** (fraguar) que tiene NASL, para crear los paquetes que queramos, en este caso con los protocolos IP, TCP y UDP, de forma similar a como lo hicimos en la charla 52 con la herramienta "Scapy".

Vamos a ver el tema con más detalle en el video 118 **(Obligatorio)**.

🌐 **Nessus - (Parte 8) - Charla 118 - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/H8bQPTC08hg>



4.9 Nessus – NASL (última parte)

En este último tema de NASL, veremos los listados de plugins, analizaremos alguno de ellos para comprender:

- Configuración
- Post configuración (incluyendo header)
- Chequeo de seguridad

Veremos como se relacionan los scripts con la mejor base de datos de conocimiento de vulnerabilidades **"https://cve.mitre.org"**.

Por ahora, solo presentaremos **"MITRE"** pues en el capítulo 8 lo desarrollaremos con todo detalle.

En este capítulo desarrollamos las: funciones de red, las funciones de generación de informes y las Categorías y familias de estos Scripts Y finalmente nos despedimos de NASL y Nessus.

Vamos a ver el tema con más detalle en el video 119 **(Obligatorio)**.

🌐 **Nessus - (Parte 9) - Charla 119 - Aprendiendo Ciberseguridad paso a paso**
<https://youtu.be/EdO3fTwLK-U>



Para cerrar el tema, presentamos a continuación las características más importante que hemos ido desarrollando sobre NASL:

Una regla NASL típicamente consta de tres partes:

- Configuración
- Post configuración (incluyendo header)
- Chequeo de seguridad

Funciones de red:

HTTP Functions (GET, POST, PUT, DELETE)

Packet Manipulation Functions: Internet Gateway Message Protocol (IGMP), Internet Control Message Protocol (ICMP), IP, TCP and UDP

String Manipulation Functions

Cryptographic Functions: Message Digest 2, 4 y 5 (MD2, MD4, MD5), RIPEMD160, Secure Hash Algorithm (SHA Y SHA1), Message Authentication Code from arbitrary data and a provided key. These functions include HMAC_DSS, HMAC_MD2, HMAC_MD4, HMAC_MD5, HMAC_RIPEMD160, HMAC_SHA, and HMAC_SHA1.

Funciones de generación de informes

NASL proporciona cuatro funciones integradas para devolver información del script.

- La función `scanner_status`: permite a los scripts informar de cuántos puertos se han escaneado y cuántos quedan por escanear.
- Las otras tres funciones (`security_note`, `security_warning` y `security_hole`) se utilizan para devolver información de seguridad, advertencias de seguridad no críticas y alertas de seguridad críticas.

Categorías de los Scripts:

- `ACT_INIT`: Plugin sets KB items.
- `ACT_SCANNER`: Plugin is a port scanner or similar (like ping).
- `ACT_SETTINGS`: Plugin sets KB items after `ACT_SCANNER`.
- `ACT_GATHER_INFO`: Plugin identifies services, parses banners.
- `ACT_ATTACK`: For non-intrusive attacks (eg directory traversal)
- `ACT_MIXED_ATTACK`: Plugin launches potentially dangerous attacks.
- `ACT_DESTRUCTIVE_ATTACK`: Plugin attempts to destroy data.
- `ACT_DENIAL`: Plugin attempts to crash a service.
- `ACT_KILL_HOST`: Plugin attempts to crash target host.
- `ACT_FLOOD`
- `ACT_END`

Familias de Scripts.

- Backdoors
- CGI abuses
- CISCO
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely



info@darfe.es

- General
- Misc.
- Netware
- NIS
- Ports scanners
- Remote file access
- RPC
- Peer-to-Peer file sharing
- Settings
- SMTP problems
- SNMP
- Untested
- Useless services
- Windows
- Windows User Management