



# CURSO DE HACKING ÉTICO

## ESCÁNERS DE VULNERABILIDADES

# Análisis de vulnerabilidades

- ☐ Nessus
- ☐ OpenVas
- ☐ Nmap
- ☐ Accunetix
- ☐ Nikto
- ☐ ¿Dónde buscar información sobre vulnerabilidades?

# Tenable Nessus

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

**Nessus** es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio, *nessusd*, que realiza el escaneo en el sistema objetivo, y *nessus*, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.



# Tenable Nessus: Instalación I

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

- ☐ Actualizamos el sistema.

**# apt update && apt upgrade**

- ☐ Descargamos la página oficial de [Tenable](#) la versión correspondiente a nuestro Sistema operativo ([Nessus-8.2.3-debian6\\_amd64.deb](#))

- ☐ Podemos verificar si es 32 o 64 bits con:

**# uname -a**

- ☐ Lo instalamos desde la carpeta donde esté descargado

**# dpkg -i Nessus-8.2.3-debian6\_amd64.deb**

- ☐ Arrancamos el daemon de Nessus

**# /etc/init.d/nessusd start**



# Tenable Nessus: Instalación

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

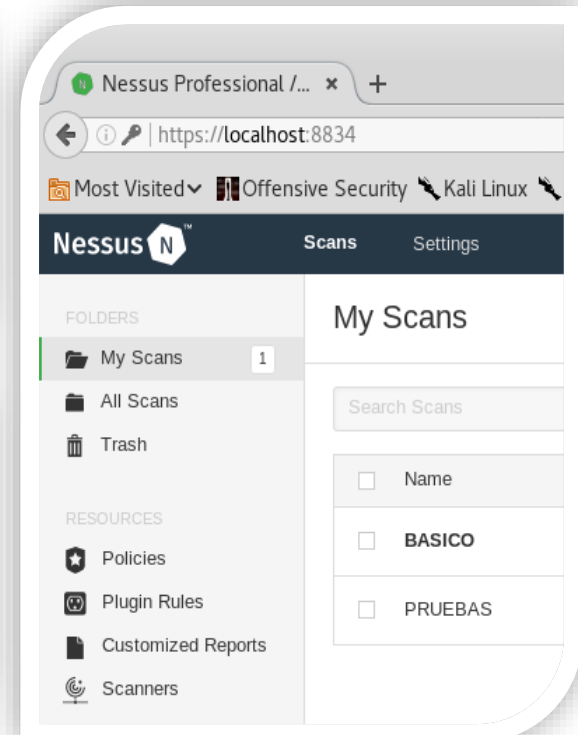
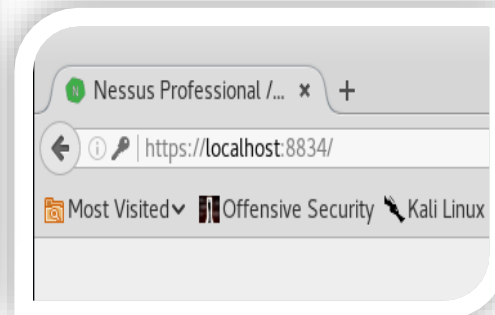
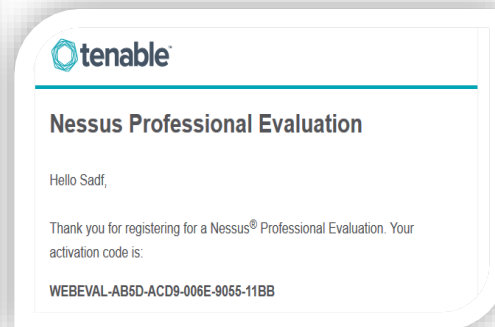
[Try for Free](#) [Buy Now](#)

### Try Nessus Professional Free

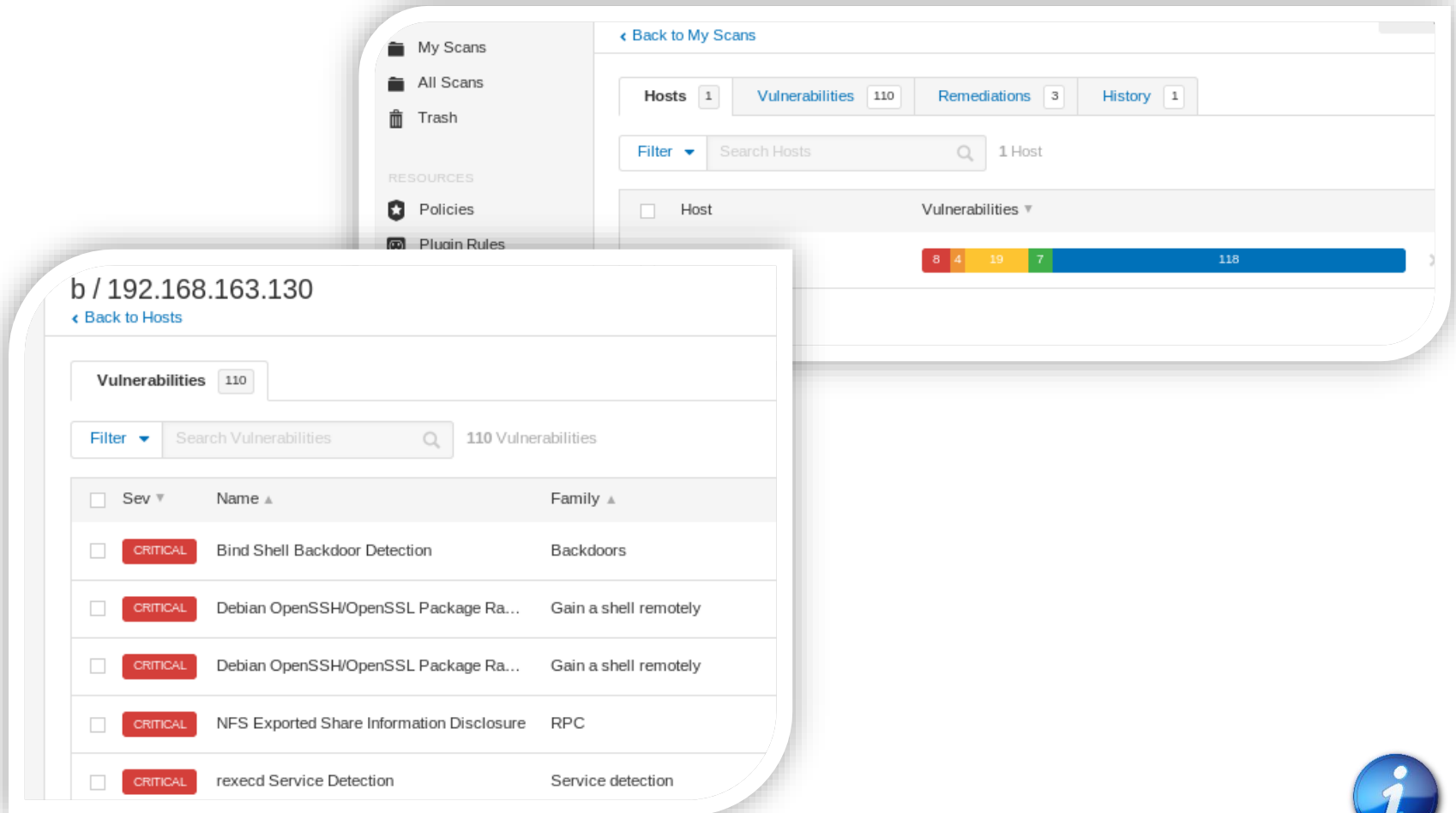
**FREE FOR 7 DAYS**

Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles and allow you to engage your IT team.

[Register](#)



# Tenable Nessus: Scan



The screenshot displays the Tenable Nessus web interface. The main view shows a scan of host **b / 192.168.163.130** with **110** vulnerabilities. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', and 'Trash'. The main content area shows a summary of the scan results, including a bar chart indicating the distribution of vulnerability severity levels: 8 Critical, 4 High, 19 Medium, 7 Low, and 118 Unrated.

**b / 192.168.163.130**  
[Back to Hosts](#)

**Vulnerabilities** 110

**Filter** Search Vulnerabilities 110 Vulnerabilities

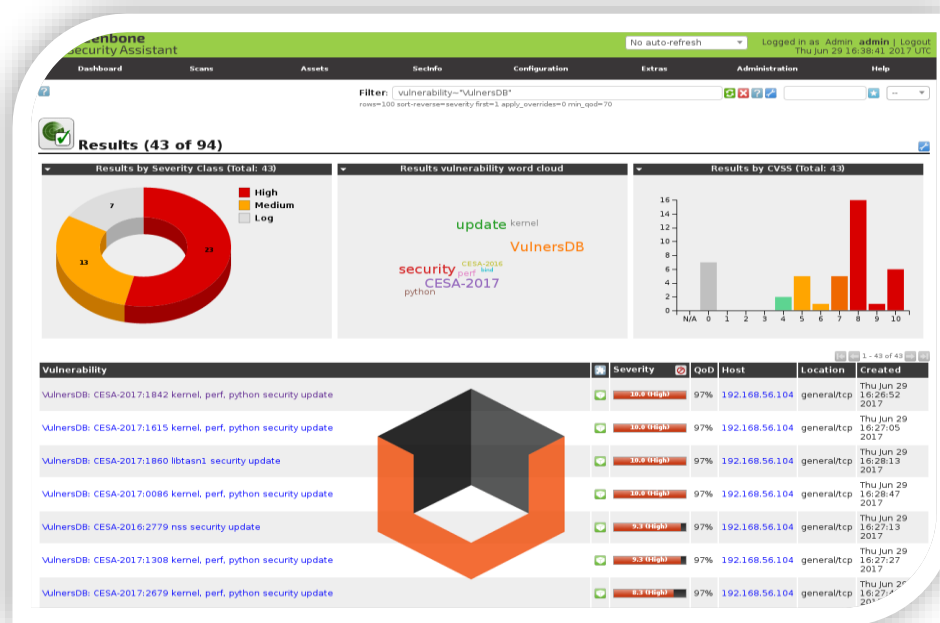
Sev	Name	Family
CRITICAL	Bind Shell Backdoor Detection	Backdoors
CRITICAL	Debian OpenSSH/OpenSSL Package Ra...	Gain a shell remotely
CRITICAL	Debian OpenSSH/OpenSSL Package Ra...	Gain a shell remotely
CRITICAL	NFS Exported Share Information Disclosure	RPC
CRITICAL	rexecd Service Detection	Service detection



# OpenVAS

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

El explorador y administrador de vulnerabilidades de código abierto más avanzado del mundo. **OpenVAS** es un marco de varios servicios y herramientas que ofrece una solución integral y potente de escaneo de vulnerabilidades y gestión de vulnerabilidades.



LIVEDEMO

# Accunetix

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

Acunetix es el escáner de vulnerabilidades web líder utilizado por las Fortune 500 compañías y ampliamente aclamado por incluir la inyección SQL más avanzada y la tecnología de escaneo de caja negra XSS.





# Nikto

Nikto is an Open Source ([GPL](#)) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and pluggins are frequently updated and can be automatically updated..

```
root@educait:~# nikto -h 10.0.0.52
- Nikto v2.1.6
-----
+ Target IP:          10.0.0.52
+ Target Hostname:    10.0.0.52
+ Target Port:        80
+ Start Time:         2018-01-15 09:01:50 (GMT2)
-----
+ Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3
  OpenSSL/0.9.8d mod_autoindex_color PHP/5.1.6
+ Retrieved x-powered-by header: PHP/5.1.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can
  hint to the user agent to protect against some forms of XSS
+ Root page / redirects to: http://10.0.0.52/xampp/
+ OSVDB-877: HTTP TRACE method is active, suggesting the host
  is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP
  reveals potentially sensitive information via certain HTTP
  requests that contain specific + OSVDB-12184: /?=PHPE9568F34-
  D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensit
  information via certain HTTP requests
```



# ¿ Dónde buscar ?

Todos los días se reportan diversos tipos de vulnerabilidades, parte de las cuales son expuestas o publicadas de forma gratuita.

- ☐ Exploit DataBase: <https://www.exploit-db.com/>
- ☐ Rapid7: <https://www.rapid7.com/>
- ☐ Seclist.org (subscription highly recommended)
- ☐ Nist (<http://nvd.nist.gov>)
- ☐ Securityfocus ([securityfocus.com](http://securityfocus.com))
- ☐ CVE- Common vulnerability and exposures (<http://cve.mitre.org/>)
- ☐ 1337day.com
- ☐ Exploitsearch.com
- ☐ Exploitsearch.net (collecting information from various exploit databases)
- ☐ Packetstormsecurity.com (highly recommended)

Kali mantiene un repositorio local de exploits de "Exploit-db"

```
# searchsploit -h
```

```
# searchsploit vsftpd
```