

# HERRAMIENTAS DE VULNERABILIDADES

MARCOS JAVIER CANCINO HERNÁNDEZ - A200353  
ANÁLISIS DE VULNERABILIDADES - 7° "N"





# NMAP

- Nmap, que significa "Network Mapper," es una herramienta de código abierto ampliamente utilizada para la exploración y el descubrimiento de redes, así como para el análisis de seguridad en sistemas informáticos.
- Fue creado originalmente por Gordon Lyon (conocido por el seudónimo "Fyodor") y es ampliamente utilizado por administradores de sistemas y profesionales de seguridad para evaluar la seguridad de redes y sistemas, así como para llevar a cabo tareas de administración de redes.

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -T4 -A -v scanme.nmap.org
host)
Initiating OS detection (try #1) against scanme.nmap.org
(64.13.134.52)
Initiating Traceroute at 12:05
Completed Traceroute at 12:05, 0.29s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:05
Completed Parallel DNS resolution of 12 hosts. at 12:05, 6.64s
elapsed
NSE: Script scanning 64.13.134.52.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:05
Completed NSE at 12:05, 4.17s elapsed
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.074s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_ 2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
25/tcp    closed smtp
```



- ```

root@kali: ~/Desktop/joomla/joomscan
File Actions Edit View Help

  ( _ ) ( _ ) ( _ ) ( v ) / _ ) / _ ) / \ ( \ )
  .- ) ( ) ( ) ( ) ( ) ( \ ) \ ( \ ) ( \ )
  \ _ ) ( _ ) ( _ ) ( / \ \ ) ( _ ) / \ ) \ )
                                     (1337.today)

--=[OWASP JoomScan
+---+---=[Version : 0.0.7
+---+---=[Update Date : [2018/09/23]
+---+---=[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP

Usage:
joomscan.pl <target>
joomscan.pl -u http://target.com/joomla
joomscan.pl -m targets.txt

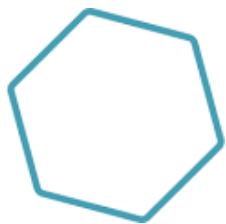
```



# W P S C A N

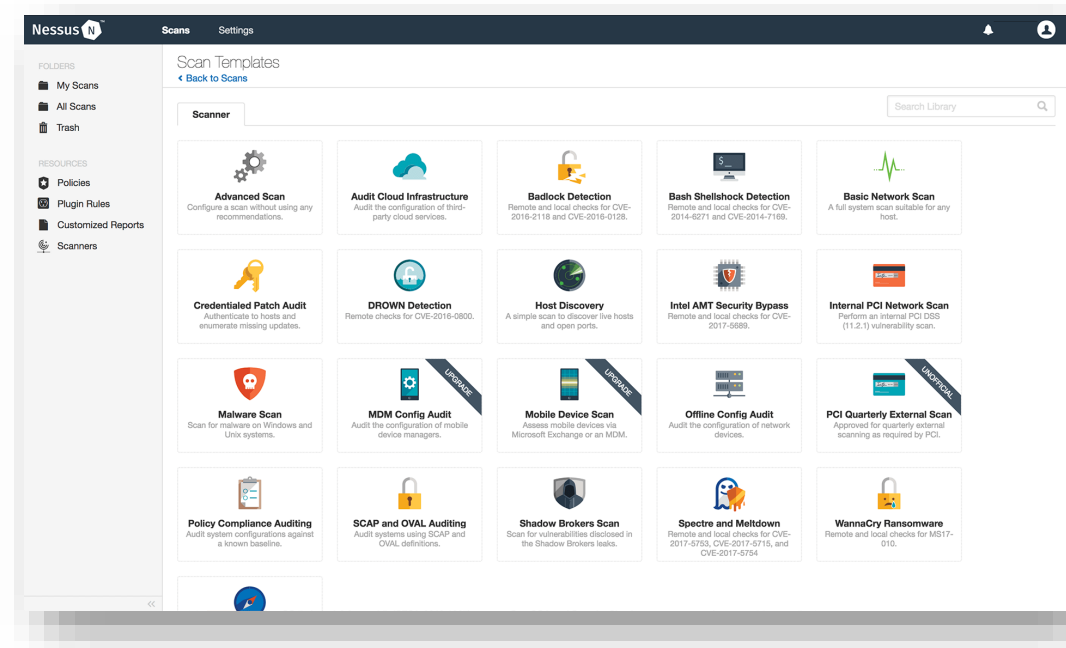
- WPScan es otra herramienta de seguridad de código abierto, pero está diseñada específicamente para el escaneo de seguridad de sitios web contruidos en el sistema de gestión de contenidos WordPress.
- Al igual que Nmap y Joomscan, WPScan se utiliza para identificar vulnerabilidades y debilidades en sitios web WordPress con el objetivo de mejorar su seguridad.

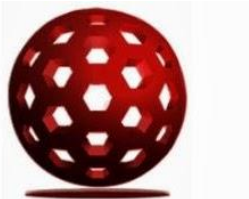
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# script Desktop/wp.log  
Script started, file is Desktop/wp.log  
root@kali:~# wpscan --url 192.168.234.1:8080/wordpress --enumerate u  
  
-----  
W P S C A N ®  
WordPress Security Scanner by the WPScan Team  
Version 2.9.3  
Sponsored by Sucuri - https://sucuri.net  
@_WPScan_, @ethicalhack3r, @erwan_lr, pvdL, @FireFart_  
-----  
[+] URL: http://192.168.234.1:8080/wordpress/  
[+] Started: Tue Dec 26 18:24:09 2017  
  
[!] The WordPress 'http://192.168.234.1:8080/wordpress/readme.html' file exists  
exposing a version number  
[!] Full Path Disclosure (FPD) in 'http://192.168.234.1:8080/wordpress/wp-includ  
es/rss-functions.php':
```



# NESSUS ESSENTIALS

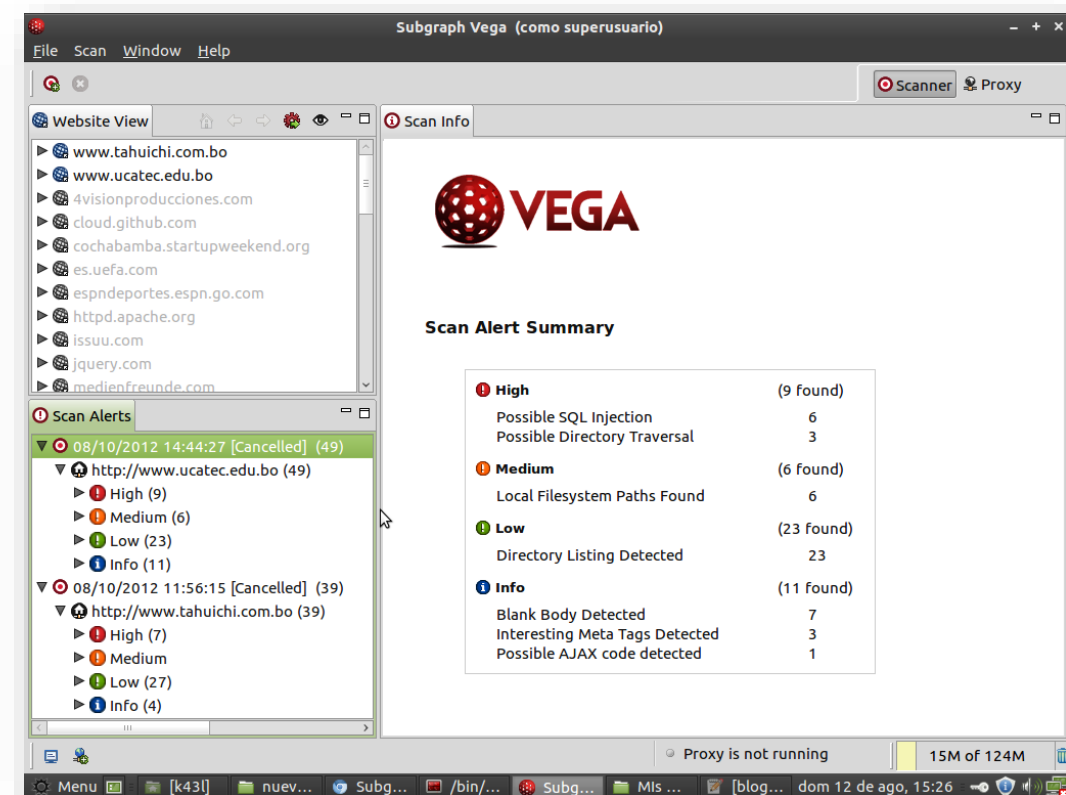
- Nessus Essentials es una versión gratuita y limitada del software de evaluación de vulnerabilidades Nessus, desarrollado por Tenable.
- Nessus es una herramienta de seguridad ampliamente utilizada para identificar vulnerabilidades en sistemas informáticos, redes y aplicaciones. Proporciona un escaneo exhaustivo y automatizado de activos y recursos en busca de debilidades que podrían ser aprovechadas por atacantes.





VEGA

- Vega es otra herramienta de seguridad de código abierto diseñada para la exploración y evaluación de vulnerabilidades en aplicaciones web.
- A diferencia de Nessus, que se enfoca en la evaluación de vulnerabilidades en sistemas y redes, Vega se centra en identificar debilidades específicas en aplicaciones web, incluidos problemas de seguridad en el código, configuraciones incorrectas y posibles riesgos de seguridad.





EL USO DE ESTAS HERRAMIENTAS DEBE SER PARTE DE UNA ESTRATEGIA GENERAL DE SEGURIDAD CIBERNÉTICA Y PRUEBAS DE PENETRACIÓN, Y SE DEBE COMBINAR CON BUENAS PRÁCTICAS DE DESARROLLO SEGURO Y ADMINISTRACIÓN DE SISTEMAS PARA GARANTIZAR LA PROTECCIÓN EFECTIVA DE LAS APLICACIONES Y SISTEMAS.

