Proyecto de Reconocimiento en Pentesting de Vulnerabilidades

28 de Abril del 2025

VISIÓN GENERAL

En este proyecto haremos una serie de pruebas para encontrar posibles vulnerabilidades así como acciones recomendadas para reforzar la seguridad informática de la empresa.

ESPECIFICACIONES

Haremos pruebas a través de Kali linux, para encontrar vulnerabilidades utilizando la herramienta NMAPS.

Escaneo y sus resultados.

utilizando las lineas de comando:

1. Ping y descubrimiento de puertos: nmap -sP <direccion ip>
2. Escaneo de servicios y versiones: nmap -sV <direccion ip>
3. Para enumerar los puertos vulnerables y servicios: sudo nmap -p- <direccion ip>
4. Para detección de vulnerabilidades: sudo nmap –script=vuln <direccion ip>

Imágenes de los escaneos

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -p- 10.0.0.160
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 19:55 EDT
Nmap scan report for 10.0.0.160
Host is up (0.00051s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 0A:00:27:00:00:10 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 32.30 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sP 10.0.0.160
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 19:57 EDT
Nmap scan report for 10.0.0.160
Host is up (0.00085s latency).
MAC Address: 0A:00:27:00:00:10 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sV 10.0.0.160
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 19:58 EDT
Nmap scan report for 10.0.0.160
Host is up (0.00062s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE   VERSION
22/tcp  open  ssh       OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
80/tcp  open  http      Apache httpd 2.4.62 ((Debian))
443/tcp open  ssl/https Apache/2.4.62 (Debian)
MAC Address: 0A:00:27:00:00:10 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.37 seconds
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -script=vuln 10.0.0.160
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 19:59 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.0.0.160
Host is up (0.00063s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|_  /wordpress/wp-login.php: Wordpress login page.
443/tcp open  https
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 0A:00:27:00:00:10 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 71.05 seconds
```

Puerto	Servicio	versión	vulnerabilidades	descripcion
22	SSH	OpenSSH 9.2p1 Debian 2+deb12u5	Fuerza bruta / Diccionario, Credenciales por defecto o conocidas, Usuarios con shells válidas + sudo sin contraseña, Exposición de claves privadas, Forwarding mal configurado	Intentos de login por hydra, medusa, o ncrack. Especialmente efectivo si el sistema tiene contraseñas débiles. Si existen usuarios con contraseñas simples (root:toor, admin:admin). Si encuentras un usuario SSH, podrías escalar privilegios si tiene sudo mal configurado.
80	HTTP	Apache httpd 2.4.62 (Debian)	WordPress detectado lo que puede dar paso a CVE-2024-27316 (mod_rewrite buffer overflow) y Directory Listing / Server Info	En algunas configuraciones específicas, el módulo mod_rewrite puede provocar una corrupción de memoria. Requiere condiciones específicas. Si no está deshabilitado, el listado de directorios o server-status puede revelar información sensible.

443	HTTPS (SSL/TLS)	Apache/2.4.62 (Debian)	CVE-2007-6750 - Slowloris	El servidor es probablemente vulnerable a Slowloris, un ataque DoS que mantiene múltiples conexiones abiertas y agota los recursos del servidor web.

Conclusiones:

El host 10.0.0.160 presenta varios servicios expuestos que, si bien están en versiones recientes y relativamente seguras, aún pueden ser explotables bajo ciertas condiciones:

- El servidor web Apache (puerto 80/443) no muestra vulnerabilidades críticas a primera vista, pero es vulnerable a un ataque de denegación de servicio (DoS) mediante Slowloris (CVE-2007-6750).
- El sitio web contiene una instancia de WordPress, lo que introduce un amplio espectro de posibles vulnerabilidades dependiendo de la versión y los plugins instalados.
- SSH está expuesto públicamente (puerto 22), lo que lo hace susceptible a ataques de fuerza bruta, especialmente si hay contraseñas débiles o configuraciones inseguras.
- No se detectaron vulnerabilidades activas en el servicio SSH, pero la exposición de servicios críticos sin control de acceso adecuado representa un riesgo potencial.