# Taller 2.3 - Monitoreo y cierre de puertos abiertos

Ismael Macareno Chouikh

2025-01-10

## Índice

## 1. Escaneo básico de puertos abiertos

Primero usamos `nmap` para realizar un escaneo básico de los puertos abiertos en el servidor objetivo

- `nmap DIRECCIONIPVICTIMA`

Este comando realiza un escaneo rápido sobre los 1000 puertos más comunes en el servidor con la IP que decidamos, en mi caso la dirección que probaré es la 172.26.0.101.

```
maka@magi:~$ nmap 172.26.0.101
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-10 10:22 CET
Nmap scan report for 172.26.0.101
Host is up (0.00065s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
143/tcp open  imap

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

Como se puede apreciar en el bloque de código `BASH` de arriba, se puede ver que mi máquina víctima con Ubuntu 14.04 tiene puertos abiertos relacionados con `ftp`, `ssh`, `smtp`, `telnet`, `http`, etc.

## 2. Escaneo con detección de versiones de servicios

A continuación, realizamos un escaneo más detallado para identificar las versiones de los servicios que están corriendo en estos puertos, lo que nos ayudará a saber si están actualizados o si presentan vulnerabilidades conocidas:

- `nmap -sV DIRECCIONIPVICTIMA`

```
maka@magi:~$ maka@magi:~$ nmap -sV 172.26.0.101
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-10 10:28 CET
Nmap scan report for 172.26.0.101
Host is up (0.00064s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.2
22/tcp  open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet  Linux telnetd
25/tcp  open  smtp    Postfix smtpd
53/tcp  open  domain  ISC BIND 9.9.5-3ubuntu0.19 (Ubuntu Linux)
80/tcp  open  http    Apache httpd 2.4.7 ((Ubuntu))
143/tcp open  imap    Courier Imapd (released 2011)
Service Info: Host:  ubuntu1.myguest.virtualbox.org; OSs: Unix, 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 7.11 seconds
```

`nmap` ha identificado:

- `vsftpd` está en la versión 3.0.2
- `OpenSSH` está en la versión 6.6.1p1
- `BIND` está en la versión 9.9.5
- `apache` está en la versión 2.4.7

## 3. Escaneo de vulnerabilidades conocidas

Para buscar posibles vulnerabilidades en estos servicios, utilizamos el script `vuln` de `nmap`, que ejecuta un análisis más profundo:

```
maka@magi:~$ nmap --script vuln 172.26.0.101
Starting Nmap 7.92 ( https://nmap.org ) at 2025-01-10 10:33 CET
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 172.26.0.101
Host is up (0.00051s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
25/tcp  open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
| ssl-dh-params:
|   VULNERABLE:
```

```
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable to active man-in-the-middle attacks
|       which could completely compromise the confidentiality and integrity
|       of any data exchanged over the resulting session.
|     Check results:
|       ANONYMOUS DH GROUP 1
|             Cipher Suite: TLS_DH_anon_WITH_DES_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1016
|     References:
|       https://www.ietf.org/rfc/rfc2246.txt
|
|   Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MitM (Logjam)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       The Transport Layer Security (TLS) protocol contains a flaw that is
|       triggered when handling Diffie-Hellman key exchanges defined with
|       the DHE_EXPORT cipher. This may allow a man-in-the-middle attacker
|       to downgrade the security of a TLS session to 512-bit export-grade
|       cryptography, which is significantly weaker, allowing the attacker
|       to more easily break the encryption and monitor or tamper with
|       the encrypted stream.
|     Disclosure date: 2015-5-19
|     Check results:
|       EXPORT-GRADE DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 512
|             Generator Length: 8
|             Public Key Length: 512
|     References:
|       https://weakdh.org
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_DES_CBC_SHA
```

```
|             Modulus Type: Safe prime
|             Modulus Source: postfix builtin
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp  open  domain
80/tcp  open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| 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-enum:
|_  /webmail/: Mail folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
143/tcp open  imap

Nmap done: 1 IP address (1 host up) scanned in 346.66 seconds
```

## 4. Medidas Correctivas

- Actualizar servicios
- Deshabilitar protocolos inseguros