

CURSO *ONLINE* DE CIBERSEGURIDAD__

Taller 2

Unidad 3. Aspectos avanzados de ciberseguridad



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

 **incibe**__

INSTITUTO NACIONAL DE CIBERSEGURIDAD



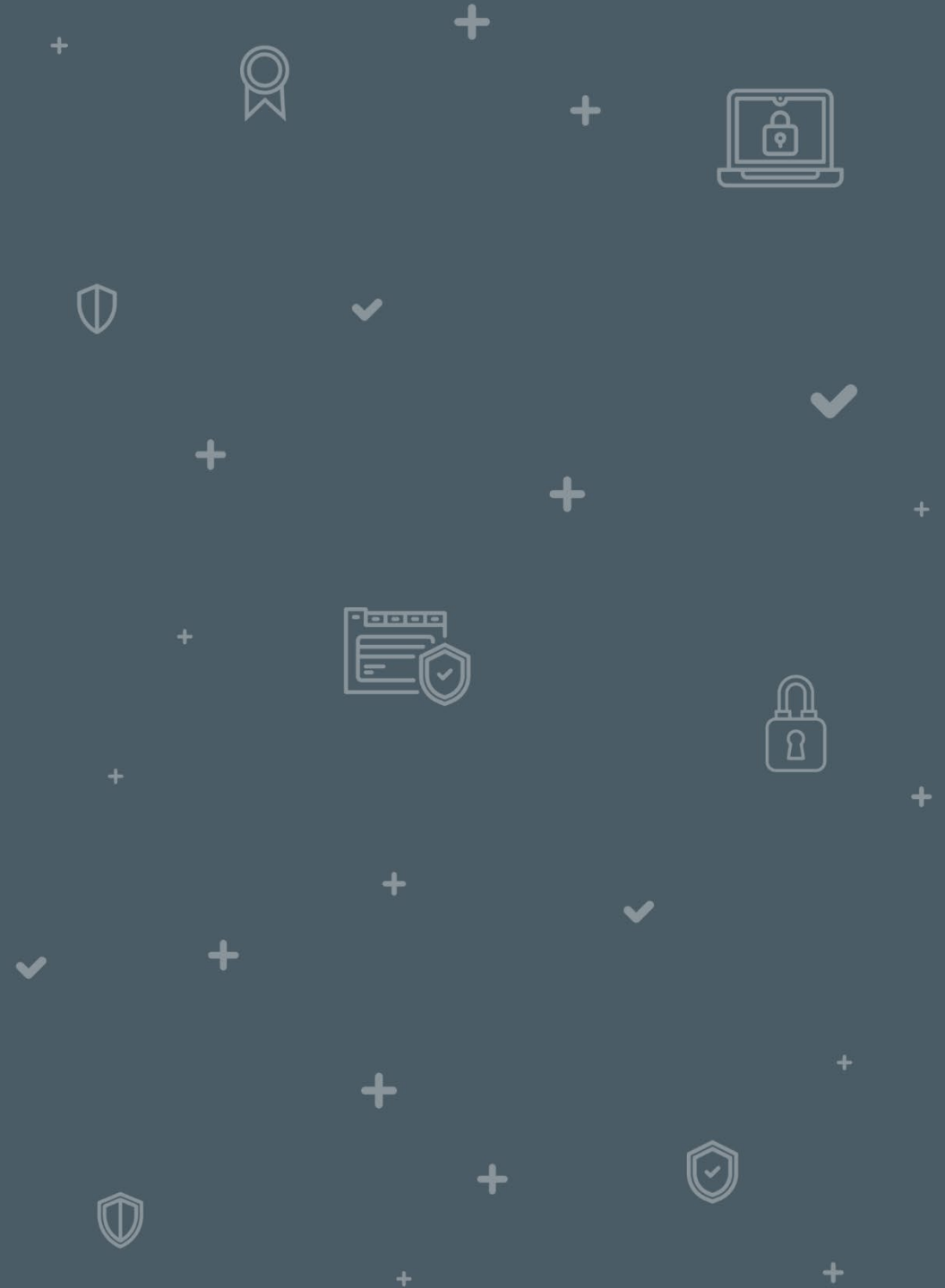
Contenidos

1	EL ESCANEO DE PUERTOS Y SERVICIOS	3
2	ESCANEO GLOBAL CON NMAP	5
3	ENUNCIADO EJERCICIO PRÁCTICO 1: ESCANEO DE PUERTOS Y SERVICIOS	15
4	SOLUCIÓN EJERCICIO PRÁCTICO 1: ESCANEO DE PUERTOS Y SERVICIOS	17
5	ENUNCIADO EJERCICIO PRÁCTICO 2: EL ESCANEO DE UN DETERMINADO PUERTO	19
6	ENUNCIADO EJERCICIO PRÁCTICO 2: EL ESCANEO DE UN DETERMINADO PUERTO	21

Duración total del taller: 20 minutos.

EL ESCANEEO DE PUERTOS Y SERVICIOS

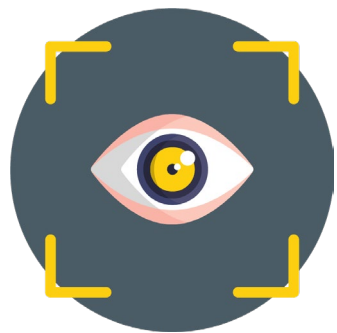
1





EL ESCANEO DE PUERTOS Y SERVICIOS

Realizarás un escaneo de puertos y servicios a través del uso de la herramienta Nmap y aprenderás a escanear, de manera global, la máquina víctima, identificando los puertos que alojan diferentes servicios y escaneando determinados puertos.



ESCANEEO GLOBAL CON NMAP

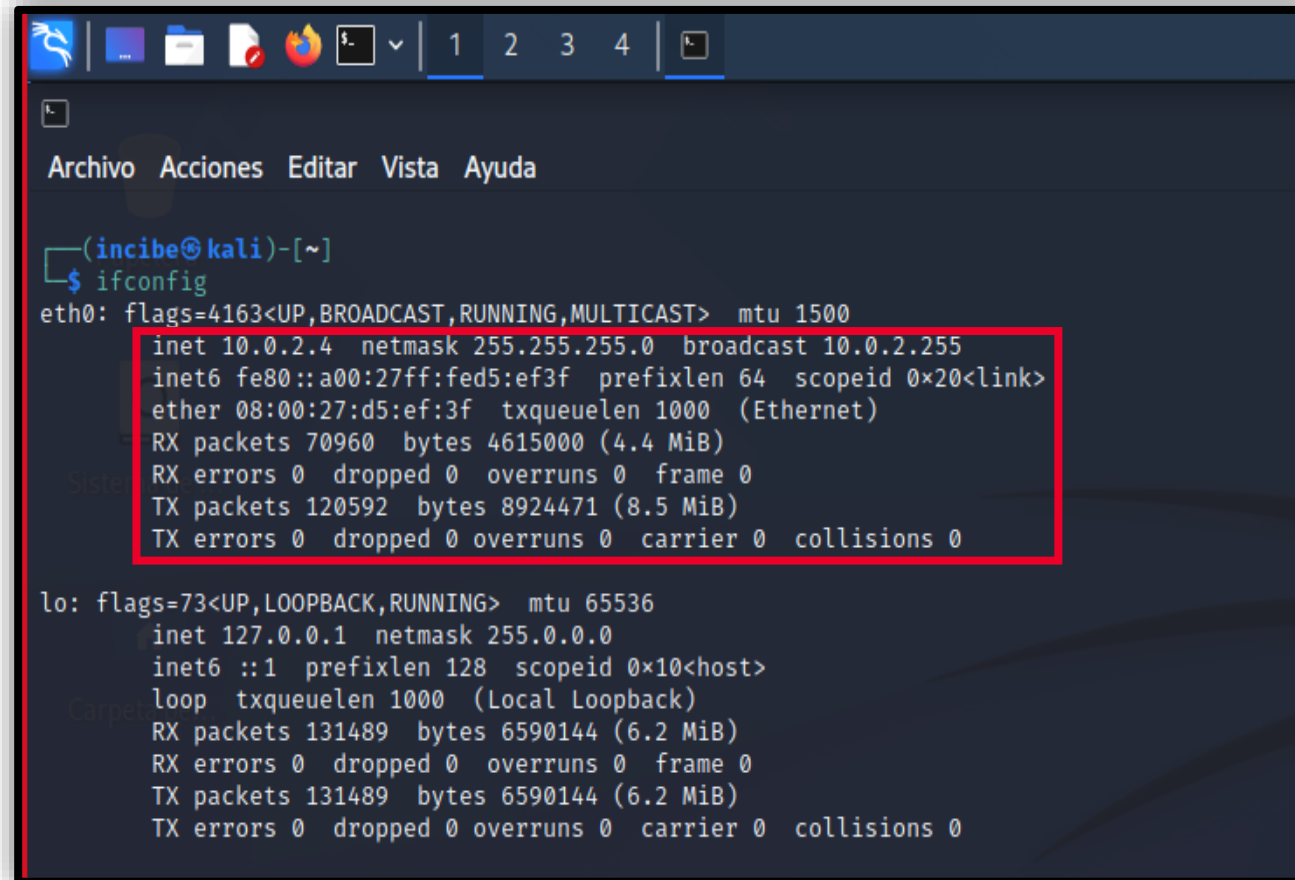
2 ESCANEO GLOBAL CON NMAP

Vas a realizar un escaneo global con Nmap. Para ello, se debe realizar el escaneo desde un ordenador y lanzarlo contra el sitio que se desea escanear. En esta práctica el ordenador que usarás para el escaneo será la máquina Kali Linux que instalaste en la Unidad 2 y el sitio de escaneo será la máquina virtual Metasploitable. Por este motivo es importante que tengas ambas máquinas virtuales abiertas en Virtual Box.

- En Kali Linux abre una terminal e introduce el comando «**ifconfig**». Este comando te mostrará la información de las interfaces de red. Lo que te servirá para averiguar la dirección IP de tu máquina virtual, es la que aparece después de la palabra «**inet**».

2

ESCANEEO GLOBAL CON NMAP



```
(incibe@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255  
    inet6 fe80::a00:27ff:fed5:ef3f prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:d5:ef:3f txqueuelen 1000 (Ethernet)  
    RX packets 70960 bytes 4615000 (4.4 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 120592 bytes 8924471 (8.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 131489 bytes 6590144 (6.2 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 131489 bytes 6590144 (6.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 1: Comando «ifconfig».

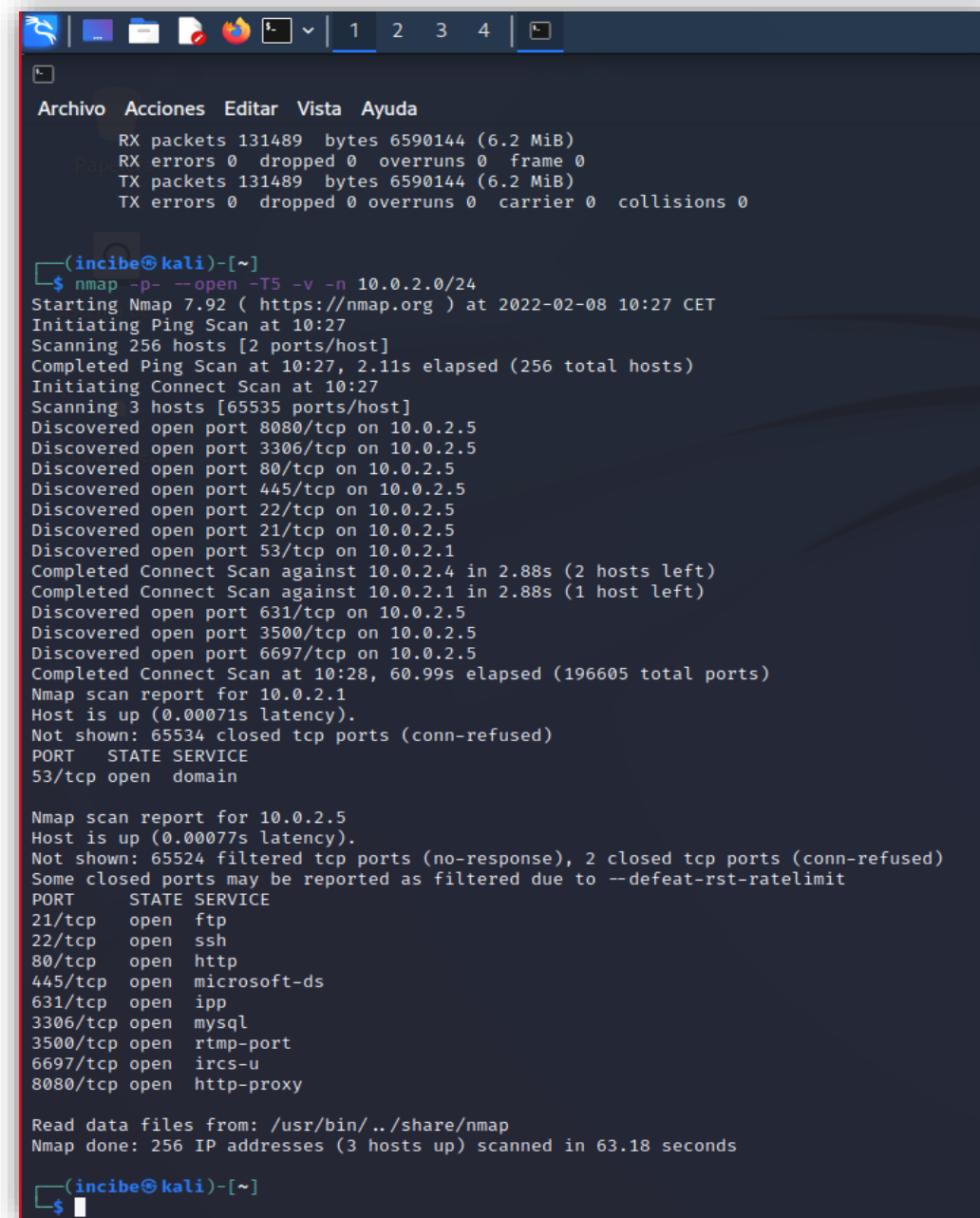
2 ESCANEEO GLOBAL CON NMAP

- Con el siguiente comando vamos a escanear todos los sistemas dentro de nuestro rango de red para poder encontrar la IP de nuestra máquina víctima: «**nmap -p- --open -T5 -v -n 10.0.2.0/24**».
- Estos son los principales parámetros que utilizaremos en este escaneo.
 - **Nmap**: es la herramienta que vas a utilizar para realizar el escaneo de puertos.
 - **-p-**: hace referencia a los puertos.
 - **--open**: sirve para seleccionar únicamente los puertos que están abiertos.
 - **-T5**: hace referencia al temporizador del escaneo. Puede ir de 0 a 5, donde 0 es menos agresivo y lento y 5 es más agresivo y rápido.
 - **10.0.2.0/24**: hace referencia al rango de IP de nuestra red, que será la que hayas averiguado en el paso anterior con el comando «**ifconfig**» y donde 24 indica el tamaño de nuestra máscara de red, en este caso 24 *bits*, lo que corresponde a los tres primeros números de la dirección IP, es decir, 10.0.2. Esto equivale a cómo está escrito en la imagen anterior 255.255.255.0. Si la dirección IP o la máscara de red que te salió en el paso anterior es otra, aquí deberás poner los datos que has obtenido.

2 ESCANEEO GLOBAL CON NMAP

- Como se puede observar existe una máquina con la IP 10.0.2.5 con múltiples puertos y servicios abiertos que escogeremos como máquina víctima.

Ilustración 2: Comando «nmap -p- --open -T5 -v -n 10.0.2.0/24».



```
(incibe@kali)-[~]
$ nmap -p- --open -T5 -v -n 10.0.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-08 10:27 CET
Initiating Ping Scan at 10:27
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 10:27, 2.11s elapsed (256 total hosts)
Initiating Connect Scan at 10:27
Scanning 3 hosts [65535 ports/host]
Discovered open port 8080/tcp on 10.0.2.5
Discovered open port 3306/tcp on 10.0.2.5
Discovered open port 80/tcp on 10.0.2.5
Discovered open port 445/tcp on 10.0.2.5
Discovered open port 22/tcp on 10.0.2.5
Discovered open port 21/tcp on 10.0.2.5
Discovered open port 53/tcp on 10.0.2.1
Completed Connect Scan against 10.0.2.4 in 2.88s (2 hosts left)
Completed Connect Scan against 10.0.2.1 in 2.88s (1 host left)
Discovered open port 631/tcp on 10.0.2.5
Discovered open port 3500/tcp on 10.0.2.5
Discovered open port 6697/tcp on 10.0.2.5
Completed Connect Scan at 10:28, 60.99s elapsed (196605 total ports)
Nmap scan report for 10.0.2.1
Host is up (0.00071s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.2.5
Host is up (0.00077s latency).
Not shown: 65524 filtered tcp ports (no-response), 2 closed tcp ports (conn-refused)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp   open  mysql
3500/tcp   open  rtmp-port
6697/tcp   open  ircs-u
8080/tcp   open  http-proxy

Read data files from: /usr/bin/./share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 63.18 seconds

(incibe@kali)-[~]
$
```

2

ESCANEO GLOBAL CON NMAP

- A continuación, escanearemos los servicios y puertos de la máquina víctima. Para ello, introduce el comando «**sudo nmap -p- --open -T5 -sS -Pn -A -sV -v -n 10.0.2.5 -oX Descargas/escaneo1.xml**». ¿Qué significa cada uno de estos comandos?
 - **sudo**: permite ejecutar comandos con privilegios de «super usuario».
 - **-sS**: realiza la comunicación a través del protocolo TCP más rápida.
 - **-Pn**: evita el descubrimiento de *host*, que puede ralentizar el análisis.
 - **-A**: detecta el sistema operativo y los servicios.
 - **-sV**: descubre las versiones de los servicios.
 - **-v**: aplica *verbose*, para ver los resultados según va escaneando.
 - **-n**: no aplica resolución DNS, lo que genera más ruido y ralentiza el escaneo.

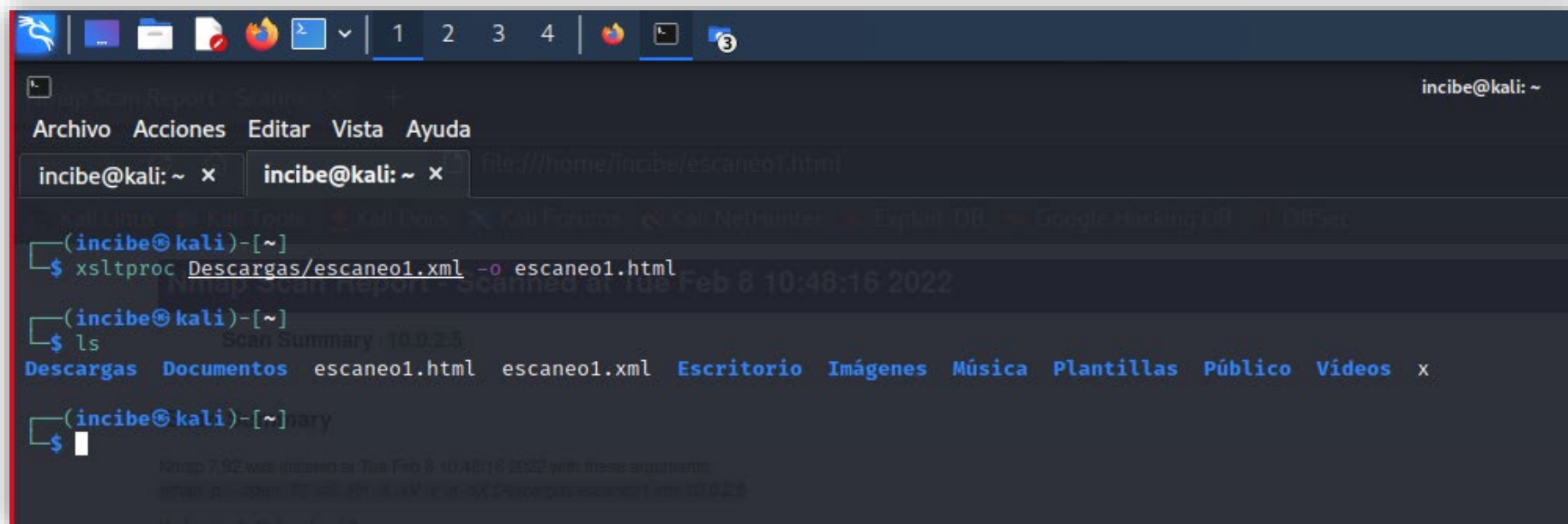


ESCANEO GLOBAL CON NMAP

- **10.0.2.5:** hace referencia a la dirección IP, que será la que hayas averiguado en el paso anterior con el comando «**ifconfig**». Si la dirección IP que te salió en el paso anterior es otra, aquí deberás poner la IP que has obtenido.
- **-oX Descargas/escaneo1.xml:** -oX se utiliza para exportar a un archivo y el resto del comando hace referencia a la ubicación en la que se va a descargar un archivo denominado «**escaneo1.xml**», donde se guardarán todos los puertos abiertos que ha encontrado el escaneo.
- Se debe tener en cuenta que en función del escaneo que se quiera realizar, no se tienen por qué utilizar todas las opciones y parámetros indicados anteriormente.

2 ESCANEO GLOBAL CON NMAP

- Una vez que se ha realizado el escaneo, convierte el archivo «**escaneo1.xml**» en formato «.html» para poder visualizarlo en el navegador. Para ello, introduce el comando «**xsltproc Descargas/escaneo1.xml -o escaneo1.html**».



```
incibe@kali: ~  
Archivo Acciones Editar Vista Ayuda  
incibe@kali: ~ x incibe@kali: ~ x file:///home/incibe/escaneo1.html  
(incibe@kali)-[~]  
$ xsltproc Descargas/escaneo1.xml -o escaneo1.html  
(incibe@kali)-[~]  
$ ls  
Descargas Documentos escaneo1.html escaneo1.xml Escritorio Imágenes Música Plantillas Público Videos x  
(incibe@kali)-[~]nary  
$
```

Ilustración 3: Comando «xsltproc Descargas/escaneo1.xml -o escaneo1.html».

2 ESCANEEO GLOBAL CON NMAP

- A continuación, dirígete donde hayas guardado tu nuevo archivo «.html». En este caso, en «Descargas». Haz doble clic para abrir el archivo en el navegador y visualizar los resultados del escaneo de puertos.

2

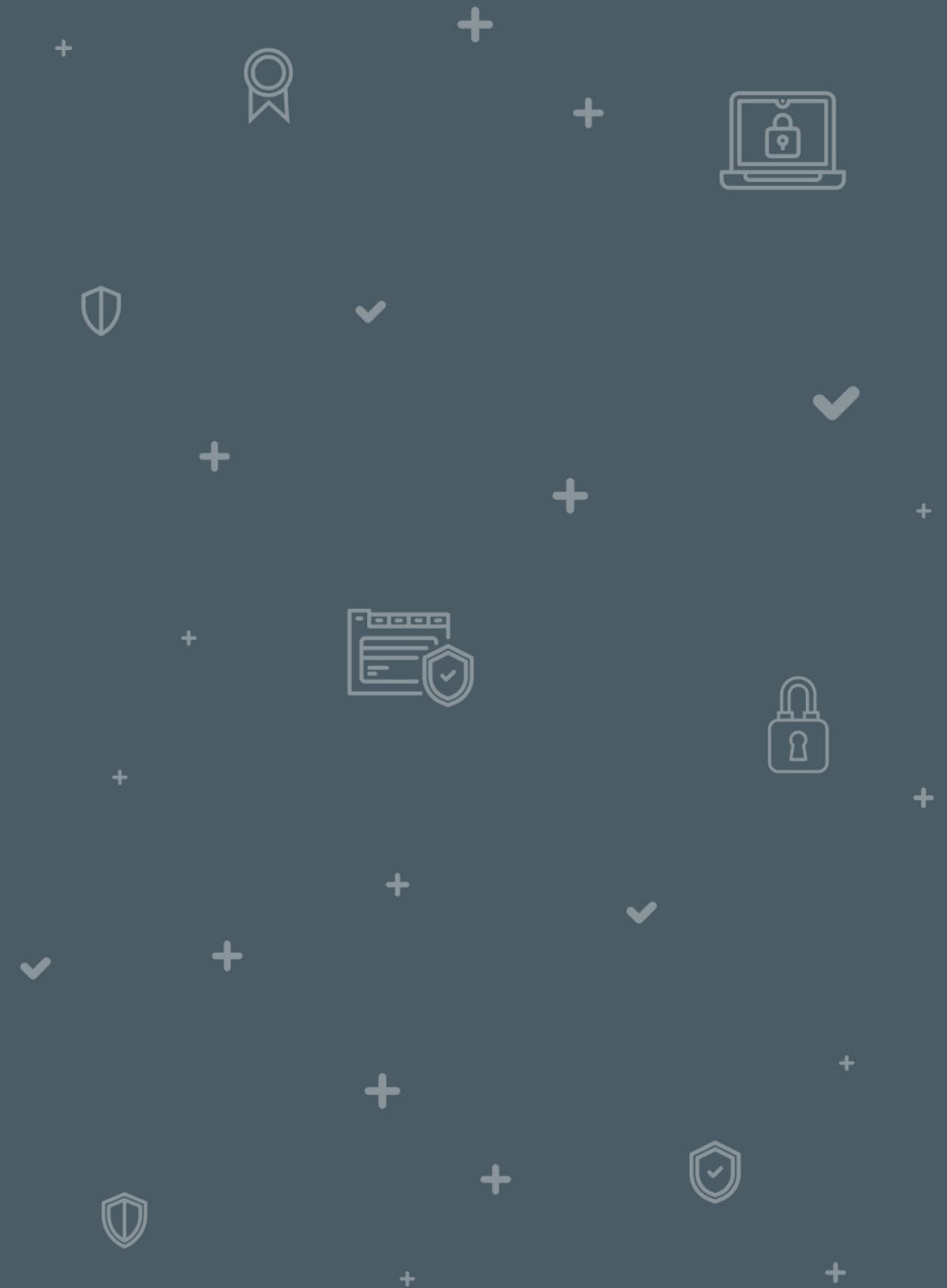
ESCANEEO GLOBAL CON NMAP

Nmap Scan Report - Scanned at Tue Feb 8 10:48:16 2022						
Scan Summary 10.0.2.5						
<p>Scan Summary</p> <p>Nmap 7.92 was initiated at Tue Feb 8 10:48:16 2022 with these arguments: <code>nmap -p- --open -T5 -sS -Pn -A -sV -v -n -oX Descargas/escaneo1.xml 10.0.2.5</code></p> <p>Verbosity: 1; Debug level 0</p> <p>Nmap done at Tue Feb 8 10:50:10 2022; 1 IP address (1 host up) scanned in 114.38 seconds</p>						
10.0.2.5						
<p>Address</p> <ul style="list-style-type: none"> 10.0.2.5 (ipv4) 08:00:27:42:51:79 - Oracle VirtualBox virtual NIC (mac) 						
<p>Ports</p> <p>The 65524 ports scanned but not shown below are in state: filtered</p> <ul style="list-style-type: none"> 65524 ports replied with: no-response <p>The 2 ports scanned but not shown below are in state: closed</p> <ul style="list-style-type: none"> 2 ports replied with: reset 						
Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	ProFTPD	1.3.5
22	tcp	open	ssh	syn-ack	OpenSSH	6.6.1p1 Ubuntu 2ubuntu2.13
	ssh-hostkey	1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA) 2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA) 256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA) 256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)				
80	tcp	open	http	syn-ack	Apache httpd	2.4.7
	http-is	Volume / SIZE TIME FILENAME - 2020-10-29 19:37 chat/ - 2011-07-27 20:17 drupal/ 1.7K 2020-10-29 19:37 payroll_app.php - 2013-04-08 12:06 phpmyadmin/				
	http-server-header	Apache/2.4.7 (Ubuntu)				
	http-title	Index of /				

Ilustración 4: Resultados del escaneo de puertos.

3

ENUNCIADO EJERCICIO PRÁCTICO 1: ESCANEEO DE PUERTOS Y SERVICIOS



3 ENUNCIADO EJERCICIO PRÁCTICO 1: ESCANEADO DE PUERTOS Y SERVICIOS

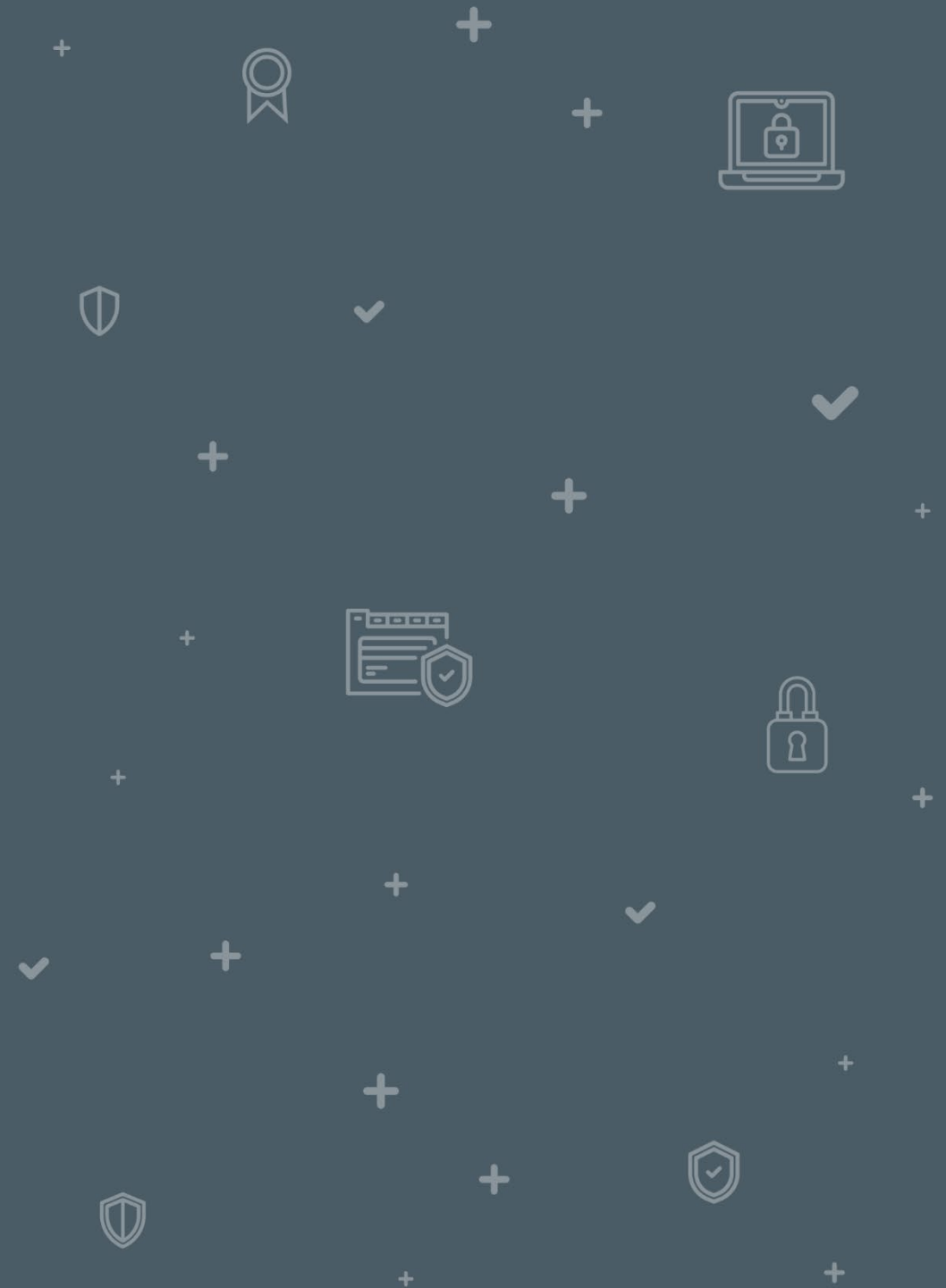


Con el archivo que has descargado de los puertos y servicios abiertos escaneados con Nmap:

- Identifica el puerto que sirve el SSH.
- Identifica el puerto que aloja el servicio SMB.

4

SOLUCIONARIO EJERCICIO PRÁCTICO 1: ESCANEEO DE PUERTOS Y SERVICIOS



4 SOLUCIONARIO EJERCICIO PRÁCTICO 1: ESCANEOS DE PUERTOS Y SERVICIOS

Con el archivo que has descargado de los puertos y servicios abiertos escaneados con Nmap:

- Identifica el puerto que sirve el SSH.

22	tcp	open	ssh	syn-ack	OpenSSH	6.6.1p1 Ubuntu 2ubuntu2.13	Ubuntu Linux; protocol 2.0
	ssh-hostkey						

Ilustración 5: Servicio SSH.

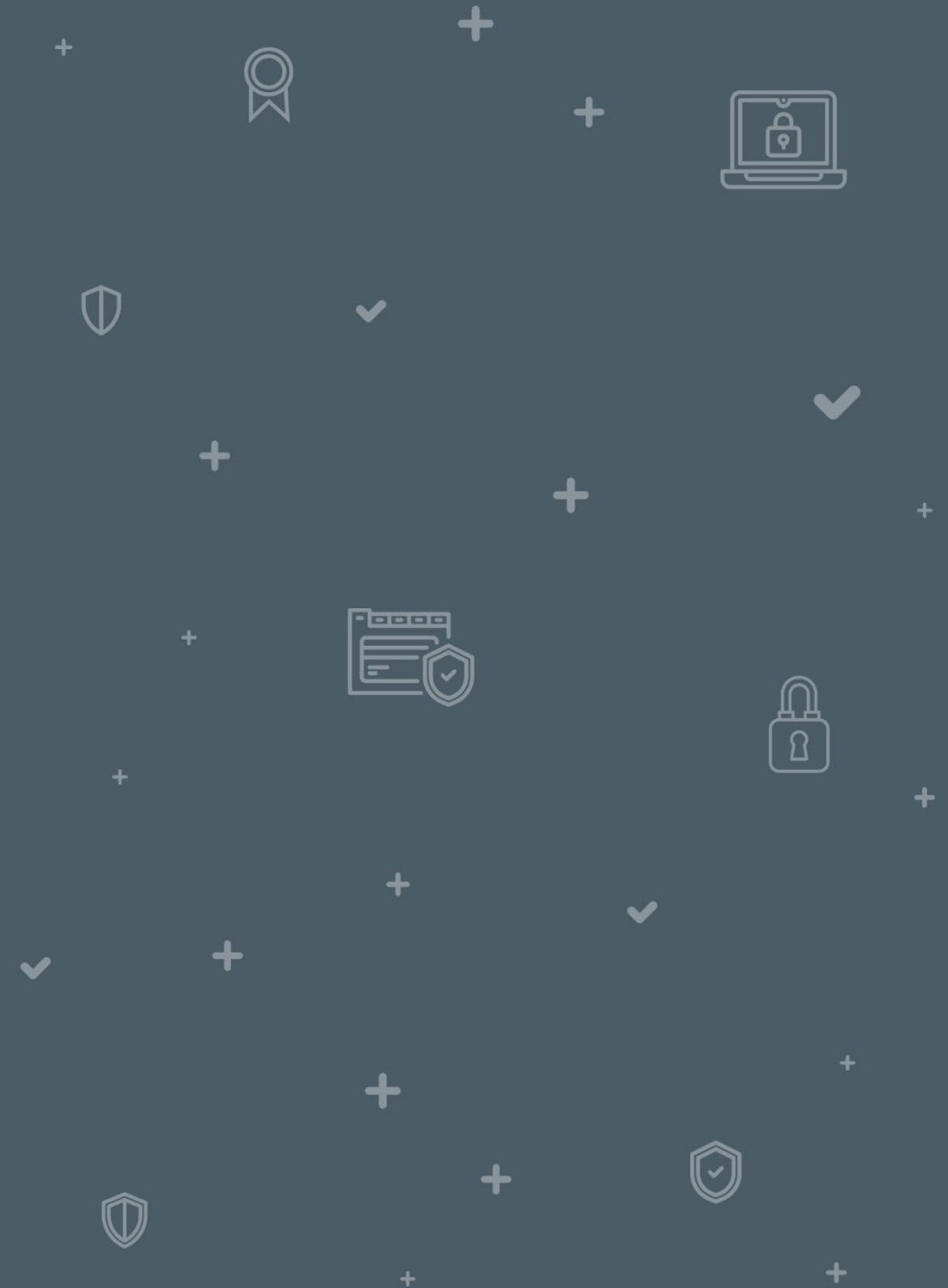
- Identifica el puerto que aloja el servicio SMB.

445	tcp	open	netbios-ssn	syn-ack	Samba smbd	4.3.11-Ubuntu	workgroup: WORKGROUP
-----	-----	------	-------------	---------	------------	---------------	----------------------

Ilustración 6: Servicio SMB.

5

ENUNCIADO EJERCICIO PRÁCTICO 2: EL ESCANEEO DE UN DETERMINADO PUERTO





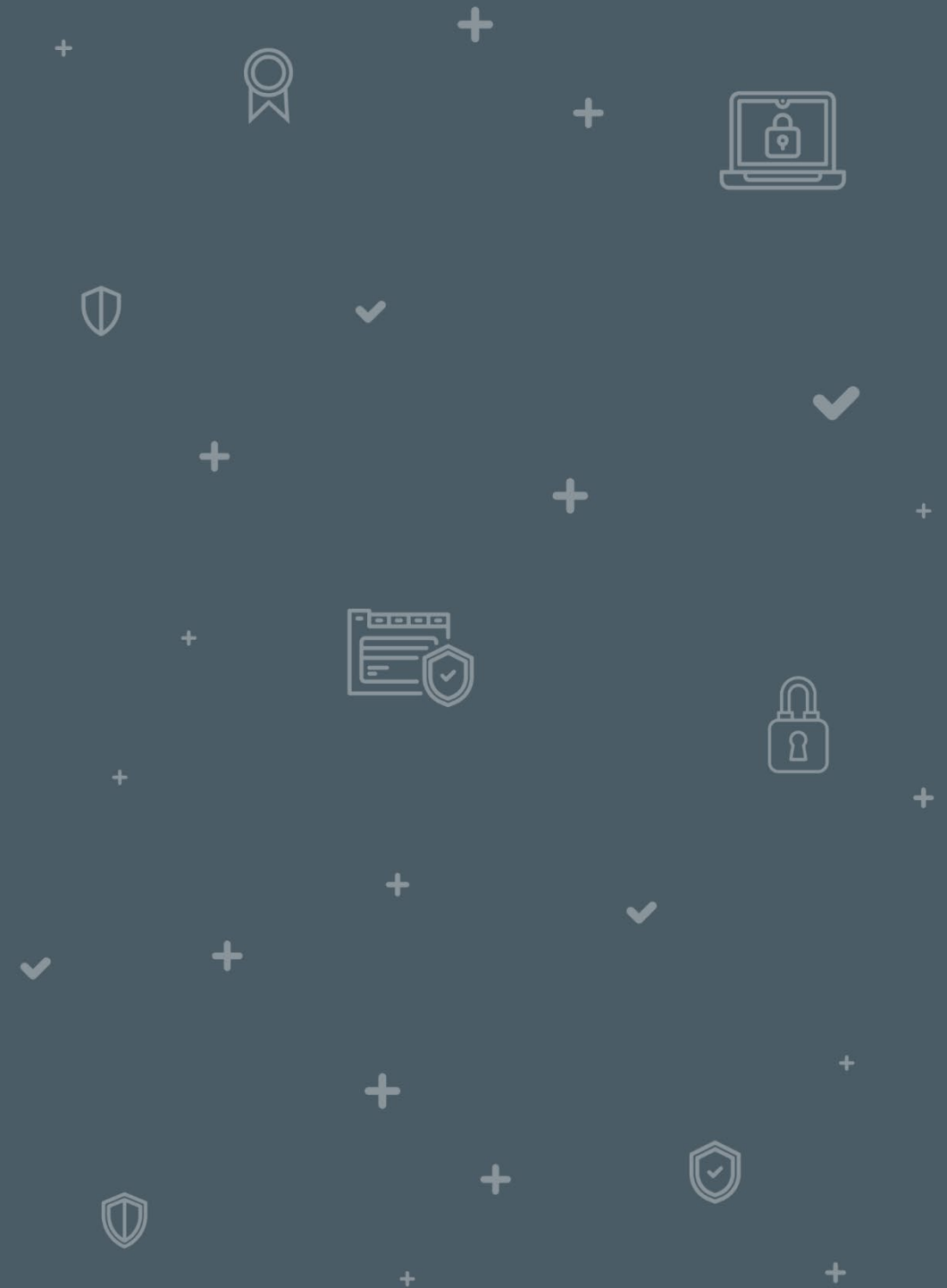
ENUNCIADO EJERCICIO PRÁCTICO 2: EL ESCANEO DE UN DETERMINADO PUERTO



A continuación, con lo que has aprendido, trata de realizar un escaneo del puerto 80 de la máquina víctima.

6

SOLUCIONARIO EJERCICIO PRÁCTICO 2: EL ESCANEEO DE UN DETERMINADO PUERTO





SOLUCIONARIO EJERCICIO PRÁCTICO 2: EL ESCANEO DE UN DETERMINADO PUERTO

A continuación, con lo que has aprendido, trata de realizar un escaneo del puerto 80 de la máquina víctima.

- Utiliza el comando «**sudo nmap -p 80 -T5 -sS -Pn -A -sV -v -n 10.0.2.5 -oX Descargas/escaneo_puerto80.xml**».
- Si hubieras indicado el comando «**sudo nmap -p 80 -T5 -sS -Pn -A -sV -v -n 10.0.2.5**», también sería una solución correcta, ya que no es obligatorio exportar los resultados en un archivo «.xml».

6 SOLUCIONARIO EJERCICIO PRÁCTICO 2: EL ESCANEO DE UN DETERMINADO PUERTO

```
Archivo Acciones Editar Vista Ayuda
(incibe@kali)-[~]
$ sudo nmap -p 80 -T5 -sS -Pn -A -sV -v -n 10.0.2.5 -oX Descargas/escaneo_puerto80.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-28 14:01 CEST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating ARP Ping Scan at 14:01
Scanning 10.0.2.5 [1 port]
Completed ARP Ping Scan at 14:01, 0.05s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 14:01
Scanning 10.0.2.5 [1 port]
Discovered open port 80/tcp on 10.0.2.5
Completed SYN Stealth Scan at 14:01, 0.04s elapsed (1 total ports)
Initiating Service scan at 14:01
Scanning 1 service on 10.0.2.5
Completed Service scan at 14:01, 6.01s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.0.2.5
NSE: Script scanning 10.0.2.5.
Initiating NSE at 14:01
Completed NSE at 14:01, 0.15s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Nmap scan report for 10.0.2.5
Host is up (0.00071s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7
|_ http_title: Index of /


```

Ilustración 7: Comando «sudo nmap -p 80 -T5 -sS -Pn -A -sV -v -n 10.0.2.5 -oX Descargas/escaneo_puerto80.xml».

¡GRACIAS!



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

