

Scanning

Ejercicio 5

Contents

1	Nmap	2
1.1	Metasploitable 1	3
1.2	Metasploitable 2	4
1.3	Scripts	7
2	wafw00f	8
3	Whatweb	9

1 Nmap

Con la herramienta Nmap se puede llevar a cabo un escaneo de puertos de forma activa. Nmap realiza una serie de escaneos enviando paquetes en crudo compatibles con protocolos TCP, UDP, ICMP, entre otros.

Queremos realizar los principales escaneos de puertos disponibles en nmap. Debido a que es una operación algo mecánica, vamos a automatizar el proceso con el siguiente script.

```
1 import subprocess
2 import os
3
4 ip = input("IP del objetivo: ")
5 argumentos = ["-sS", "-sT", "-sY", "-sN", "-sF", "-sX", "-sA", "-sW", "-sM", "-sZ"] # Lista de argumentos de nmap
6
7 conf = input("¿Guardar los resultados?(y/n): ") # Preguntamos si queremos escribir un output
8
9 if conf == "y":
10     name = input("Nombre del archivo: ") # Nombre del archivo
11     name = name + ".txt"
12     if os.path.isfile(name): # Comprobamos que el archivo existe en dicho absolute path
13         a = input("El archivo ya existe, quiere reescribirlo?(y/n): ")
14
15         if a == "n":
16             raise Exception("Operación cancelada")
17
18     with open(name, "w") as archivo: # Creamos el archivo para escribir o lo reescribimos si ya existe
19
20         for argumento in argumentos:
21             print("\n\n") # Ejecuta todos los comando de nmap de la lista de argumentos y escribe
22             print(f"nmap {argumento} -vv -p- {ip}") # el output del comando en el archivo
23             output = subprocess.run(["sudo", "nmap", argumento, "-vv", "-p-", ip], capture_output = True, text = True)
24             print(output.stdout)
25             archivo.write(f"nmap {argumento} -vv -p- {ip}" + output.stdout + "\n\n\n")
26
27
28
29
30 else:
31
32     for argumento in argumentos:
33         print("\n\n") # Ejecuta todos los comando de nmap de la lista de argumentos
34         print(f"nmap {argumento} -vv -p- {ip}")
35         print("\n")
36         subprocess.call(["sudo", "nmap", argumento, "-vv", "-p-", ip])
37
```

El programa ha de ser ejecutado en el shell con permisos de root

```
(kali@kali)-[~/Desktop/ej4/nmap]
$ sudo python3 nmap_auto.py
IP del objetivo: 192.168.1.153
¿Guardar los resultados?(y/n): y
Nombre del archivo: out
El archivo ya existe, quiere reescribirlo?(y/n): y

nmap -sS -vv -p- 192.168.1.153
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 17:22 EDT
Initiating ARP Ping Scan at 17:22
Scanning 192.168.1.153 [1 port]
Completed ARP Ping Scan at 17:22, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:22
Completed Parallel DNS resolution of 1 host. at 17:22, 0.01s elapsed
Initiating SYN Stealth Scan at 17:22
Scanning 192.168.1.153 (192.168.1.153) [65535 ports]
Discovered open port 80/tcp on 192.168.1.153
Discovered open port 445/tcp on 192.168.1.153
Discovered open port 139/tcp on 192.168.1.153
Discovered open port 5900/tcp on 192.168.1.153
Discovered open port 3306/tcp on 192.168.1.153
Discovered open port 23/tcp on 192.168.1.153
Discovered open port 53/tcp on 192.168.1.153
Discovered open port 21/tcp on 192.168.1.153
Discovered open port 111/tcp on 192.168.1.153
Discovered open port 22/tcp on 192.168.1.153
```

Además, todo el output de nmap que es imprimido en el shell se guarda en un fichero de texto.

1.1 Metasploitable 1

Se va a representar en una tabla los resultados de los escaneos de la máquina Metasploitable 1 describiendo los servicios descubiertos:

PUERTO	ESTADO	SERVICIO	DESCRIPCIÓN
21/tcp	open	ftp	Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP
22/tcp	open	ssh	Su principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además, permite copiar datos de forma segura
23/tcp	open	telnet	Protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella
25/tcp	open	smtp	Protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos
53/tcp	open	domain	Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
80/tcp	open	http	Es el protocolo de comunicación que permite las transferencias de información a través de archivos (XML, HTML...)
139/tcp	open	netbios-ssn	Es una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico
445/tcp	open	netbios-ssn	
3306/tcp	open	mysql	Es un sistema de gestión de bases de datos relacional desarrollado bajo licencia dual
3632/tcp	open	distccd	Software diseñado para distribuir tareas de compilación a través de la red hacia máquinas participantes.
5432/tcp	open	postgresql	Es un sistema de gestión de bases de datos relacional orientado a objetos
8009/tcp	open	ajp13	Protocolo binario que permite enviar solicitudes desde un servidor web a un servidor de aplicaciones que se encuentra detrás del servidor web. También permite monitoreo dado que el servidor web puede enviar un ping al servidor de aplicación.
8180/tcp	open	http	

Se va a representar en una tabla los resultados de los escaneos de la máquina Metasploitable 1 junto con las versiones de los servicios descubiertos:

PUERTO	ESTADO	SERVICIO	VERSIÓN
21/tcp	open	ftp	ProFTPD 1.3.1
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8
139/tcp	open	netbios-ssn	netbios-ssn Samba smbd 3.X - 4.X
445/tcp	open	netbios-ssn	netbios-ssn Samba smbd 3.0.20-Debian
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

El sistema operativo de metasploitable 1 es linux 2.6.9 - 2.6.33.

1.2 Metasploitable 2

Se va a representar en una tabla los resultados de los escaneos de la máquina Metasploitable 2 describiendo los servicios descubiertos:

PUERTO	ESTADO	SERVICIO	VERSIÓN
21/tcp	open	ftp	Protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP
22/tcp	open	ssh	Su principal función es el acceso remoto a un servidor por medio de un canal seguro en el que toda la información está cifrada. Además, permite copiar datos de forma segura
23/tcp	open	telnet	Protocolo de red que nos permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella
25/tcp	open	smtp	Protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos
53/tcp	open	domain	Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
80/tcp	open	http	Es el protocolo de comunicación que permite las transferencias de información a través de archivos (XML, HTML...)
111/tcp	open	rpcbind	Convierte RPC Program Number en direcciones universales.
139/tcp	open	netbios-ssn	Es una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico
445/tcp	open	netbios-ssn	
512/tcp	open	exec	
513/tcp	open	login	Aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host. El anfitrión remoto debe hacer funcionar un servicio de Rlogind (o demonio) para que el Rlogin conecte con el anfitrión.
514/tcp	open	shell	
1099/tcp	open	rmiregistry	Servidor que permite a una aplicación buscar objetos que están siendo exportados para su uso mediante llamadas a métodos remotos.
1524/tcp	open	ingreslock	Backdoor
2049/tcp	open	nfs	Posibilita que distintos sistemas conectados a una misma red accedan a ficheros remotos como si se tratara de locales.
2121/tcp	open	ccproxy-ftp	Servidor proxy fácil de usar. Soporta conexiones de banda ancha, DSL, fibra óptica, satelital, entre otras; y actúa como servidor proxy para protocolos de correo, noticias, HTTP, HTTPS, FTP, SOCKS, TELNET. También, permite construir un servidor proxy y compartir Internet dentro de una LAN (Red de Área Local) de forma fácil y eficiente
3306/tcp	open	mysql	Es un sistema de gestión de bases de datos relacional desarrollado bajo licencia dual
3632/tcp	open	distccd	Software diseñado para distribuir tareas de compilación a través de la red hacia máquinas participantes.
5432/tcp	open	postgresql	Es un sistema de gestión de bases de datos relacional orientado a objetos

5900/tcp	open	vnc	VNC es un programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente
6000/tcp	open	X11	Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para este.
6667/tcp	open	irc	Protocolo de comunicación en tiempo real basado en texto. Se diferencia de la mensajería instantánea en que los usuarios no deben acceder a establecer la comunicación de antemano, de tal forma que todos los usuarios que se encuentran en un canal pueden comunicarse entre sí, aunque no hayan tenido ningún contacto anterior
6697/tcp	open	ircs-u	
8009/tcp	open	ajp13	Protocolo binario que permite enviar solicitudes desde un servidor web a un servidor de aplicaciones que se encuentra detrás del servidor web. También permite monitoreo dado que el servidor web puede enviar un ping al servidor de plicación.
8180/tcp	open	http	
8787/tcp	open	drb	Permite comunicación interna entre programas basados en Ruby de forma remota
44354/tcp	open	mountd	The mountd daemon is a Remote Procedure Call (RPC) that answers a client request to mount a file system. The mountd daemon finds out which file systems are available by reading the /etc/xtab file.
46344/tcp	open	status	
47474/tcp	open	java-rmi	Mecanismo ofrecido por Java para invocar un método de manera remota
58360/tcp	open	nlockmgr	Server that processes file locking requests from local kernel or from other remote lock daemon

Se va a representar en una tabla los resultados de los escaneos de la máquina Metasploitable 2 junto con las versiones de los servicios descubiertos:

PUERTO	ESTADO	SERVICIO	VERSIÓN
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	netbios-ssn Samba smbd 3.X - 4.X
445/tcp	open	microsoft-ds	netbios-ssn Samba smbd 3.0.20-Debian
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	
514/tcp	open	shell	
1099/tcp	open	rmiregistry	GNU Classpath grmiregistry
1524/tcp	open	ingreslock	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ccproxy-ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	
6667/tcp	open	irc	UnrealIRCd
6697/tcp	open	ircs-u	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
8787/tcp	open	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
44354/tcp	open	mountd	1-3 (RPC #100005)
46344/tcp	open	status	1 (RPC #100024)
47474/tcp	open	java-rmi	GNU Classpath grmiregistry
58360/tcp	open	nlockmgr	1-4 (RPC #100021)

El sistema operativo de metasploitable 2 es linux 2.6.9 - 2.6.33.

1.3 Scripts

En nmap también puede hacerse uso de scripts para obtener resultados que un escaneo corriente no podría obtener:

```
(kali@kali)-[~/Desktop/ej4/nmap]
$ sudo nmap --script ftp-anon --script-args ftp-anon.maxlist=-1 192.168.1.160 -p 21,2121
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 21:03 EDT
Nmap scan report for 192.168.1.160 (192.168.1.160)
Host is up (0.00061s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
2121/tcp  open  ccproxy-ftp
MAC Address: 08:00:27:F1:6B:BB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
```

Este script nos permite saber si un servicio ftp permite logueo anónimo.

```
(kali@kali)-[~/Desktop/ej4/nmap]
$ sudo nmap --script http-default-accounts 192.168.1.160 -p 80,8180
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 21:23 EDT
Nmap scan report for 192.168.1.160 (192.168.1.160)
Host is up (0.00092s latency).

PORT      STATE SERVICE
80/tcp    open  http
8180/tcp  open  unknown
|_ http-default-accounts:
|   [Apache Tomcat] at /manager/html/
|   tomcat:tomcat
|   [Apache Tomcat Host Manager] at /host-manager/html/
|   tomcat:tomcat
|_
MAC Address: 08:00:27:F1:6B:BB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

Este script prueba las credenciales por defecto en un servicio http.

3 Whatweb

Whatweb reconoce tecnología web incluido los sistemas de gestión de contenido (CMS), paquetes de estadística y analítica, librerías JavaScript, servidores web y embedded devices. También identifica versiones, direcciones, cuentas, módulos de frameworks, errores SQL y más.

```
(kali@kali)~$ sudo whatweb -a 4 -v 192.168.1.151 192.168.1.152
[sudo] contraseña para kali:
WhatWeb report for http://192.168.1.152
Status      : 200 OK
Title       : <None>
IP          : 192.168.1.152
Country     : RESERVED, ZZ

Summary     : Apache[2.2.8][Default], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch], Matomo, PHP[5.2.4-2ubuntu5.10][Suhosin-Patch]

Detected Plugins:
[ Apache ]
  The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

  String      : Default
  Version     : 2.2.8 (from HTTP Server Header)
  Google Dorks: (3)
  Website     : http://httpd.apache.org/

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.

  OS          : Ubuntu Linux
  String      : Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch (from server string)
```

```
[ Matomo ]
  Matomo is the leading open alternative to Google Analytics that gives you full control over your data. Matomo lets you easily collect data from websites, apps & the IoT and visualise this data and extract insights. Privacy is built-in. Matomo was formerly known as Piwik, and is developed in PHP.

  Aggressive function available (check plugin file or details).
  Google Dorks: (1)
  Website      : https://matomo.org

[ PHP ]
  PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present.

  Version      : 5.2.4-2ubuntu5.10
  Module       : Suhosin-Patch
  Google Dorks: (2)
  Website      : http://www.php.net/

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Sat, 16 Jul 2022 15:10:17 GMT
  Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
  Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
  ETag: "107f7-2d-481ffa5ca8840"
  Accept-Ranges: bytes
  Content-Length: 45
```

```
WhatWeb report for http://192.168.1.151
Status      : 200 OK
Title       : Metasploitable2 - Linux
IP          : 192.168.1.151
Country     : RESERVED, ZZ

Summary     : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], Matomo, PHP[5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

Detected Plugins:
[ Apache ]
  The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

  Version      : 2.2.8 (from HTTP Server Header)
  Google Dorks: (3)
  Website      : http://httpd.apache.org/

[ HTTPServer ]
  HTTP server header string. This plugin also attempts to identify the operating system from the server header.
```

```

OS      : Ubuntu Linux
String  : Apache/2.2.8 (Ubuntu) DAV/2 (from server string)

[ Matomo ]
Matomo is the leading open alternative to Google Analytics
that gives you full control over your data. Matomo lets you
easily collect data from websites, apps & the IoT and
visualise this data and extract insights. Privacy is
built-in. Matomo was formerly known as Piwik, and is
developed in PHP.

Aggressive function available (check plugin file or details).
Google Dorks: (1)
Website   : https://matomo.org

[ PHP ]
PHP is a widely-used general-purpose scripting language
that is especially suited for Web development and can be
embedded into HTML. This plugin identifies PHP errors,
modules and versions and extracts the local file path and
username if present.

Version    : 5.2.4-2ubuntu5.10
Version    : 5
Google Dorks: (2)
Website    : http://www.php.net/

[ WebDAV ]
Web-based Distributed Authoring and Versioning (WebDAV) is
a set of methods based on the Hypertext Transfer Protocol
(HTTP) that facilitates collaboration between users in

```

```

editing and managing documents and files stored on World
Wide Web servers. - More Info:
http://en.wikipedia.org/wiki/WebDAV

Version      : 2

[ X-Powered-By ]
X-Powered-By HTTP header

String       : PHP/5.2.4-2ubuntu5.10 (from x-powered-by string)

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Sat, 16 Jul 2022 15:10:18 GMT
  Server: Apache/2.2.8 (Ubuntu) DAV/2
  X-Powered-By: PHP/5.2.4-2ubuntu5.10
  Connection: close
  Transfer-Encoding: chunked
  Content-Type: text/html

(kali@kali)~$ sudo whatweb -a 4 -v -u msfadmin:msfadmin 192.168.1.151 192.168.1.152
WhatWeb report for http://192.168.1.151
Status      : 200 OK
Title       : Metasploitable2 - Linux
IP          : 192.168.1.151
Country     : RESERVED, ZZ

Summary     : Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], Matomo, PHP[5.2.4-2ubuntu5.10], WebDAV[2], X-Powered-By[PHP/5.2.4-2
ubuntu5.10]

```

```

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Sat, 16 Jul 2022 15:22:19 GMT
  Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
  Last-Modified: Wed, 17 Mar 2010 14:08:25 GMT
  ETag: "107f7-2d-481ffa5ca8840"
  Accept-Ranges: bytes
  Content-Length: 45
  Connection: close
  Content-Type: text/html

(kali@kali)~$
(kali@kali)~$
(kali@kali)~$ sudo whatweb -a 4 192.168.1.151 192.168.1.152
[sudo] contraseña para kali:
http://192.168.1.152 [200 OK] Apache[2.2.8][default], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with
Suhosin-Patch], IP[192.168.1.152], Matomo, PHP[5.2.4-2ubuntu5.10][Suhosin-Patch]
http://192.168.1.151 [200 OK] Apache[2.2.8], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.2.8 (Ubuntu) DAV/2], IP[192.168.1.151], Matomo, P
HP[5.2.4-2ubuntu5.10], Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-By[PHP/5.2.4-2ubuntu5.10]

```