

Escanear puertos con nmap

Instalación de Nmap en Kali

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt-get install nmap  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-2+kali2+b1).  
nmap set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Saber cual es la dirección IP de la maquina Debian

```
deb@debian:~$ hostname -I  
192.168.1.69 2806:103e:2f:6d9f:2355:d887:dae0:5bc9 2806:103e:2f:6d9f:4664:34f6:2f6c:f457  
deb@debian:~$
```

Escaneo básico de un objetivo (El IP de la maquina debian <IP_debian>):

```
(kali@kali)-[~]  
$ nmap 192.168.1.69  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 22:56 EDT  
Nmap scan report for 192.168.1.69  
Host is up (0.0010s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   closed https  
  
Nmap done: 1 IP address (1 host up) scanned in 4.58 seconds
```

Después de realizar el escaneo, Nmap proporcionará una lista de puertos abiertos y los servicios que operan en esos puertos.

Escaneo de puertos y servicios:

```
(kali@kali)-[~]  
$ nmap -sV 192.168.1.69  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 22:58 EDT  
Nmap scan report for 192.168.1.69  
Host is up (0.0011s latency).  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  VERSION  
80/tcp    open  tcpwrapped  
443/tcp   closed https  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

Escaneo detallado y búsqueda de vulnerabilidades:

```
└─$ nmap -sV --script=vuln 192.168.1.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 22:59 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).
Stats: 0:01:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.64% done; ETC: 23:01 (0:00:01 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.82% done; ETC: 23:01 (0:00:00 remaining)
Stats: 0:01:37 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.82% done; ETC: 23:01 (0:00:00 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.82% done; ETC: 23:01 (0:00:00 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.82% done; ETC: 23:01 (0:00:00 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 81.82% done; ETC: 23:01 (0:00:00 remaining)
Nmap scan report for 192.168.1.69
Host is up (0.0011s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
443/tcp   closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.77 seconds
```

Documentar Vulnerabilidades Asociadas a los Servicios

http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)

Exploits CVE-2014-3704 también conocidos como 'Drupageddon' en Drupal. Se sabe que las versiones anteriores a la 7.32 del núcleo de Drupal están afectadas.

La vulnerabilidad permite a atacantes remotos realizar ataques de inyección SQL a través de una matriz que contiene claves creadas.

El script inyecta un nuevo usuario administrador de Drupal a través del formulario de inicio de sesión y luego intenta iniciar sesión como este usuario para determinar si el objetivo es vulnerable. Si ese es el caso, se realizan los siguientes pasos de explotación:

- Está habilitado el módulo de filtro PHP que permite evaluar fragmentos/código PHP incrustados.
- Se ha establecido el permiso para utilizar el código PHP para usuarios administradores.
- Se crea y se previsualiza un nuevo artículo que contiene la carga útil.

- limpieza: de forma predeterminada, se restauran todos los registros de la base de datos que fueron agregados o modificados por el script.

Vulnerabilidad descubierta originalmente por Stefan Horst de SektionEins.

La técnica de explotación utilizada para lograr RCE en el objetivo se basa en el módulo Metasploit `exploit/multi/http/drupal_drupageddon`.