NMAP

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia
Javier Holgado Durán
Jaime Junquera Melendez
Jose Carlos Abollo Palacios

16 de abril de 2018

¿Qué es NMAP?

Definición

Es un software libre con paradigma de auditoría cuya función es el escaneo de puertos y host de una red. Se puede usar desde consola o desde interfaz gráfica.

Características y scripts

Características

- Escaneo de puertos.
- Descubrimiento de servidores.
- Determinación del sistema operativo de un host.
- Mapeo de redes.
- Debugeo de interfaces y rutas.

Scripts

Gracias al uso de scripts puede comrpobar algunas de las siguientes vulnerabiliades.

- **Malware:** Revisa si hay conexiones abiertas por códigos maliciosos.
- **Vuln:** Descubre las vulnerabilidades más conocidas.
- **Discovery:** Recupera información después de un ataque.
- **All:** Ejecuta todas las anteriores.

Ejemplos

nmap -p 1-65535 -sV -sS -T4 target

Obtiene la versión de todos los puertos del objetivo.

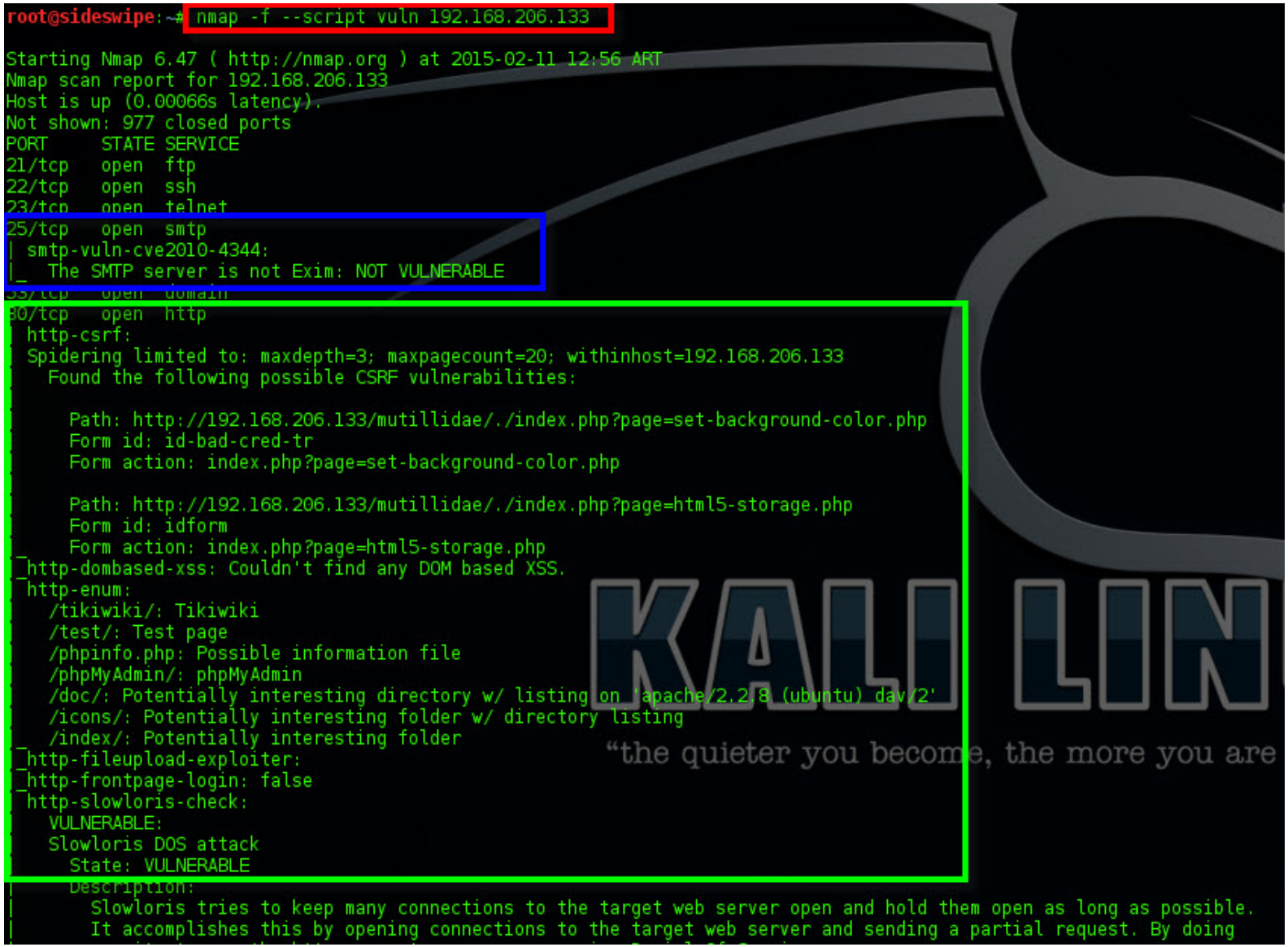
nmap -v -sV -O -sS -T5 target

Escaneo sigiloso de sistema opeativo y salida verbosa.

nmap –iflist

Debugeo de interfaces y rutas.

Ejemplos


root@sideswipe:~# nmap -f --script vuln 192.168.206.133
Starting Nmap 6.47 (http://nmap.org) at 2015-02-11 12:56 ART
Nmap scan report for 192.168.206.133
Host is up (0.00066s latency).
Not shown: 977 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
80/tcp open http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.206.133
| Found the following possible CSRF vulnerabilities:
| Path: http://192.168.206.133/mutillidae/./index.php?page=set-background-color.php
| Form id: id-bad-cred-tr
| Form action: index.php?page=set-background-color.php
| Path: http://192.168.206.133/mutillidae/./index.php?page=html5-storage.php
| Form id: idform
| Form action: index.php?page=html5-storage.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /tikiwiki/: Tikiwiki
| /test/: Test page
| /phpinfo.php: Possible information file
| /phpMyAdmin/: phpMyAdmin
| /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
| /icons/: Potentially interesting folder w/ directory listing
|_ /index/: Potentially interesting folder
|_http-fileupload-exploiter:
|_http-frontpage-login: false
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: VULNERABLE
| Description:
| 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
KALI LIN
"the quieter you become, the more you are

Bibliografía

https://es.wikipedia.org/wiki/Nmap
https://nmap.org/nsedoc/
https://www.cyberciti.biz/security/nmap-command-examples-tutorials/