Troll 2

❯ sudo nmap -F 192.168.56.0/24

Nuestra maquina objetivo:

Nmap scan report for 192.168.56.109

Host is up (0.00073s latency).

Not shown: 97 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

80/tcp open http

MAC Address: 08:00:27:C1:C9:1F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Abro otra terminal y con gobuster busco las url del http

gobuster dir -u http://192.168.56.109 -w /usr/share/wordlists/dirb/common.txt -x .php,.html,.txt

gobuster dir -u http://192.168.56.109 -w /usr/share/wordlists/dirb/common.txt -x .php,.html,.txt

===============================================================

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

===============================================================

[+] Url: http://192.168.56.109

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirb/common.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Extensions: php,html,txt

[+] Timeout: 10s

===============================================================

Starting gobuster in directory enumeration mode

===============================================================

/.html (Status: 403) [Size: 287]

/.hta.php (Status: 403) [Size: 290]

/.hta.txt (Status: 403) [Size: 290]

/.htaccess.php (Status: 403) [Size: 295]

/.htaccess (Status: 403) [Size: 291]

/.hta (Status: 403) [Size: 286]

/.hta.html (Status: 403) [Size: 291]

/.htpasswd.txt (Status: 403) [Size: 295]

/.htpasswd.html (Status: 403) [Size: 296]

/.htpasswd (Status: 403) [Size: 291]

/.htaccess.txt (Status: 403) [Size: 295]

/.htaccess.html (Status: 403) [Size: 296]

/.htpasswd.php (Status: 403) [Size: 295]

/cgi-bin/.html (Status: 403) [Size: 295]

/cgi-bin/ (Status: 403) [Size: 290]

/index (Status: 200) [Size: 110]

/index.html (Status: 200) [Size: 110]

/index.html (Status: 200) [Size: 110]

/robots (Status: 200) [Size: 346]

/robots.txt (Status: 200) [Size: 346]

/robots.txt (Status: 200) [Size: 346]

/server-status (Status: 403) [Size: 295]

Progress: 18456 / 18460 (99.98%)

===============================================================

Finished

no encontramos nada mas que troleos pero si la versión de Apache/2.2.22 (Ubuntu) Server at 192.168.56.109 Port 80

nikto -h http://192.168.56.109

- Nikto v2.5.0

---------------------------------------------------------------------------

+ Target IP: 192.168.56.109

+ Target Hostname: 192.168.56.109

+ Target Port: 80

+ Start Time: 2025-04-28 22:16:20 (GMT-4)

---------------------------------------------------------------------------

+ Server: Apache/2.2.22 (Ubuntu)

+ /: Server may leak inodes via ETags, header found with file /, inode: 13079, size: 110, mtime: Tue Oct 14 22:05:15 2014. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ /index: Uncommon header 'tcn' found, with contents: list.

+ /index: Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275

+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

+ OPTIONS: Allowed HTTP Methods: OPTIONS, GET, HEAD, POST .

+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/

+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.

+ 8909 requests: 0 error(s) and 9 item(s) reported on remote host

+ End Time: 2025-04-28 22:16:45 (GMT-4) (25 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested