**Audit Sécurité**

**Dirb**

DIRB v2.22

By The Dark Raver

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

START\_TIME: Thu Nov 9 05:29:47 2023

URL\_BASE: http://13.36.64.65:8080/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://13.36.64.65:8080/ ----

+ http://13.36.64.65:8080/css (CODE:302|SIZE:0)

+ http://13.36.64.65:8080/favicon.ico (CODE:200|SIZE:4286)

+ http://13.36.64.65:8080/fonts (CODE:302|SIZE:0)

+ http://13.36.64.65:8080/index (CODE:200|SIZE:1093)

+ http://13.36.64.65:8080/index.html (CODE:200|SIZE:1093)

+ http://13.36.64.65:8080/js (CODE:302|SIZE:0)

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

END\_TIME: Thu Nov 9 05:32:19 2023

DOWNLOADED: 4612 - FOUND: 6

dirb http://13.36.64.65:8080 /usr/share/dirb/wordlists/vulns/apache.txt

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

DIRB v2.22

By The Dark Raver

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

START\_TIME: Thu Nov 9 05:39:30 2023

URL\_BASE: http://13.36.64.65:8080/

WORDLIST\_FILES: /usr/share/dirb/wordlists/vulns/apache.txt

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

GENERATED WORDS: 30

---- Scanning URL: http://13.36.64.65:8080/ ----

+ http://13.36.64.65:8080/index.html (CODE:200|SIZE:1093)

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

END\_TIME: Thu Nov 9 05:39:31 2023

DOWNLOADED: 30 - FOUND: 1

Nmap

nmap -v -A -sV 13.36.64.65

Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-09 09:10 EST

NSE: Loaded 155 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 09:10

Completed NSE at 09:10, 0.00s elapsed

Initiating NSE at 09:10

Completed NSE at 09:10, 0.00s elapsed

Initiating NSE at 09:10

Completed NSE at 09:10, 0.00s elapsed

Initiating Ping Scan at 09:10

Scanning 13.36.64.65 [4 ports]

Completed Ping Scan at 09:10, 0.05s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 09:10

Completed Parallel DNS resolution of 1 host. at 09:10, 0.04s elapsed

Initiating SYN Stealth Scan at 09:10

Scanning ec2-13-36-64-65.eu-west-3.compute.amazonaws.com (13.36.64.65) [1000 ports]

Discovered open port 8080/tcp on 13.36.64.65

Discovered open port 80/tcp on 13.36.64.65

Discovered open port 22/tcp on 13.36.64.65

Discovered open port 4000/tcp on 13.36.64.65

Completed SYN Stealth Scan at 09:10, 23.05s elapsed (1000 total ports)

Initiating Service scan at 09:10

Scanning 4 services on ec2-13-36-64-65.eu-west-3.compute.amazonaws.com (13.36.64.65)

Completed Service scan at 09:10, 12.81s elapsed (4 services on 1 host)

Initiating OS detection (try #1) against ec2-13-36-64-65.eu-west-3.compute.amazonaws.com (13.36.64.65)

Initiating Traceroute at 09:10

Completed Traceroute at 09:10, 0.07s elapsed

Initiating Parallel DNS resolution of 1 host. at 09:10

Completed Parallel DNS resolution of 1 host. at 09:11, 13.00s elapsed

NSE: Script scanning 13.36.64.65.

Initiating NSE at 09:11

Completed NSE at 09:11, 17.72s elapsed

Initiating NSE at 09:11

Completed NSE at 09:11, 0.38s elapsed

Initiating NSE at 09:11

Completed NSE at 09:11, 0.00s elapsed

Nmap scan report for ec2-13-36-64-65.eu-west-3.compute.amazonaws.com (13.36.64.65)

Host is up (0.040s latency).

Not shown: 995 filtered tcp ports (no-response)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.4p1 Debian 5+deb11u2 (protocol 2.0)

| ssh-hostkey:

| 3072 7df25d04d96bef143c048a691ba090d8 (RSA)

| 256 9ea47f7d846c7854a84ead0d170ba45c (ECDSA)

|\_ 256 feb844d4db31578d5f29dacdb0a03f8b (ED25519)

80/tcp open http Apache httpd 2.4.56 ((Debian))

|\_http-server-header: Apache/2.4.56 (Debian)

| http-methods:

|\_ Supported Methods: HEAD POST OPTIONS

|\_http-title: Apache2 Debian Default Page: It works

443/tcp closed https

4000/tcp open http Cowboy httpd

|\_http-title: Site doesn't have a title (application/json; charset=utf-8).

| http-methods:

|\_ Supported Methods: HEAD POST OPTIONS

|\_http-server-header: Cowboy

8080/tcp open http-proxy

|\_http-title: app

| fingerprint-strings:

| DNSStatusRequestTCP, DNSVersionBindReqTCP, RPCCheck, Socks4, Socks5:

| HTTP/1.1 400 Bad Request

| Connection: close

| FourOhFourRequest:

| HTTP/1.1 404 Not Found

| accept-ranges: bytes

| Date: Thu, 09 Nov 2023 14:10:49 GMT

| Connection: close

| GetRequest:

| HTTP/1.1 200 OK

| accept-ranges: bytes

| cache-control: max-age=3600

| last-modified: Thu, 09 Nov 2023 14:00:06 GMT

| etag: W/"480643-1093-2023-11-09T14:00:06.028Z"

| content-length: 1093

| content-type: text/html; charset=UTF-8

| Date: Thu, 09 Nov 2023 14:10:48 GMT

| Connection: close

| <!doctype html><html lang=""><head><meta name="viewport" content="width=device-width,initial-scale=1,shrink-to-fit=no"><link href="https://cdn.jsdelivr.net/npm/bootstrap@5.1.3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1oBoqyl2QvZ6jIW3" crossorigin="anonymous"><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width,initial-scale=1"><link rel="icon" href="/time-manager/favicon.ico"><link rel="stylesheet" href="https://unpkg.com/primeicons@6.0.1/primeicons.css"><title>app</title

| HTTPOptions:

| HTTP/1.1 405 Method Not Allowed

| accept-ranges: bytes

| Date: Thu, 09 Nov 2023 14:10:48 GMT

| Connection: close

| RTSPRequest:

| HTTP/1.1 405 Method Not Allowed

| accept-ranges: bytes

| Date: Thu, 09 Nov 2023 14:10:49 GMT

|\_ Connection: close

|\_http-favicon: Unknown favicon MD5: 1BA2AE710D927F13D483FD5D1E548C9B

| http-methods:

|\_ Supported Methods: GET HEAD

|\_http-open-proxy: Proxy might be redirecting requests

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port8080-TCP:V=7.93%I=7%D=11/9%Time=654CE868%P=x86\_64-pc-linux-gnu%r(Ge

SF:tRequest,55F,"HTTP/1\.1\x20200\x20OK\r\naccept-ranges:\x20bytes\r\ncach

SF:e-control:\x20max-age=3600\r\nlast-modified:\x20Thu,\x2009\x20Nov\x2020

SF:23\x2014:00:06\x20GMT\r\netag:\x20W/\"480643-1093-2023-11-09T14:00:06\.

SF:028Z\"\r\ncontent-length:\x201093\r\ncontent-type:\x20text/html;\x20cha

SF:rset=UTF-8\r\nDate:\x20Thu,\x2009\x20Nov\x202023\x2014:10:48\x20GMT\r\n

SF:Connection:\x20close\r\n\r\n<!doctype\x20html><html\x20lang=\"\"><head>

SF:<meta\x20name=\"viewport\"\x20content=\"width=device-width,initial-scal

SF:e=1,shrink-to-fit=no\"><link\x20href=\"https://cdn\.jsdelivr\.net/npm/b

SF:ootstrap@5\.1\.3/dist/css/bootstrap\.min\.css\"\x20rel=\"stylesheet\"\x

SF:20integrity=\"sha384-1BmE4kWBq78iYhFldvKuhfTAU6auU8tT94WrHftjDbrCEXSU1o

SF:Boqyl2QvZ6jIW3\"\x20crossorigin=\"anonymous\"><meta\x20charset=\"utf-8\

SF:"><meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge\"><meta\

SF:x20name=\"viewport\"\x20content=\"width=device-width,initial-scale=1\">

SF:<link\x20rel=\"icon\"\x20href=\"/time-manager/favicon\.ico\"><link\x20r

SF:el=\"stylesheet\"\x20href=\"https://unpkg\.com/primeicons@6\.0\.1/prime

SF:icons\.css\"><title>app</title")%r(HTTPOptions,71,"HTTP/1\.1\x20405\x20

SF:Method\x20Not\x20Allowed\r\naccept-ranges:\x20bytes\r\nDate:\x20Thu,\x2

SF:009\x20Nov\x202023\x2014:10:48\x20GMT\r\nConnection:\x20close\r\n\r\n")

SF:%r(RTSPRequest,71,"HTTP/1\.1\x20405\x20Method\x20Not\x20Allowed\r\nacce

SF:pt-ranges:\x20bytes\r\nDate:\x20Thu,\x2009\x20Nov\x202023\x2014:10:49\x

SF:20GMT\r\nConnection:\x20close\r\n\r\n")%r(FourOhFourRequest,68,"HTTP/1\

SF:.1\x20404\x20Not\x20Found\r\naccept-ranges:\x20bytes\r\nDate:\x20Thu,\x

SF:2009\x20Nov\x202023\x2014:10:49\x20GMT\r\nConnection:\x20close\r\n\r\n"

SF:)%r(Socks5,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20clo

SF:se\r\n\r\n")%r(Socks4,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnect

SF:ion:\x20close\r\n\r\n")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20Bad\x20Reque

SF:st\r\nConnection:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\

SF:.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(DNSStat

SF:usRequestTCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20c

SF:lose\r\n\r\n");

Device type: general purpose

Running: Linux 2.4.X|3.X

OS CPE: cpe:/o:linux:linux\_kernel:2.4.37 cpe:/o:linux:linux\_kernel:3.2

OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=260 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 80/tcp)

HOP RTT ADDRESS

1 70.61 ms 192.168.163.2

2 64.15 ms ec2-13-36-64-65.eu-west-3.compute.amazonaws.com (13.36.64.65)

NSE: Script Post-scanning.

Initiating NSE at 09:11

Completed NSE at 09:11, 0.00s elapsed

Initiating NSE at 09:11

Completed NSE at 09:11, 0.00s elapsed

Initiating NSE at 09:11

Completed NSE at 09:11, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 70.64 seconds

Raw packets sent: 3049 (136.416KB) | Rcvd: 45 (1.896KB)

Nikto :

nikto -h http://13.36.64.65:8080/

- Nikto v2.1.6

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

+ Target IP: 13.36.64.65

+ Target Hostname: 13.36.64.65

+ Target Port: 8080

+ Start Time: 2023-11-12 05:34:45 (GMT-5)

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

+ Server: No banner retrieved

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ 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

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ OSVDB-3268: /css/: Directory indexing found.

+ OSVDB-3092: /css/: This might be interesting...

+ 7936 requests: 0 error(s) and 5 item(s) reported on remote host

+ End Time: 2023-11-12 05:36:33 (GMT-5) (108 seconds)

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

+ 1 host(s) tested

nikto -h 13.36.64.65:443

- Nikto v2.1.6

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

+ No web server found on 13.36.64.65:443

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

+ 0 host(s) tested

(CAR on est pas en https)