

Monitored(放棄)

NMAP

```
└─# nmap -sCV 10.10.11.248
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 61:e2:e7:b4:1b:5d:46:dc:3b:2f:91:38:e6:6d:c5:ff (RSA)
|   256 29:73:c5:a5:8d:aa:3f:60:a9:4a:a3:e5:9f:67:5c:93 (ECDSA)
|_  256 6d:7a:f9:eb:8e:45:c2:02:6a:d5:8d:4d:b3:a3:37:6f (ED25519)
80/tcp    open  http      Apache httpd 2.4.56
|_http-title: Did not follow redirect to https://nagios.monitored.htb/
|_http-server-header: Apache/2.4.56 (Debian)
389/tcp   open  ldap      OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http  Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=nagios.monitored.htb/organizationName=Monitored/stateOrProvinceName=Dorset/
countryName=UK
| Not valid before: 2023-11-11T21:46:55
|_Not valid after:  2297-08-25T21:46:55
| tls-alpn:
|_  http/1.1
|_http-title: Nagios XI
Service Info: Host: nagios.monitored.htb; 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 30.16 seconds
```

whatweb

```
—(root@kali)-[~]
└─# whatweb https://nagios.monitored.htb/
https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f [200
OK] Apache[2.4.56], Bootstrap, Cookies[nagiosxi], Country[RESERVED][ZZ],
Email[sales@nagios.com], HTML5, HTTPServer[Debian Linux][Apache/2.4.56 (Debian)],
HttpOnly[nagiosxi], IP[10.10.11.248], JQuery[3.6.0], PasswordField[password],
PoweredBy[the], Script[text/javascript], Title[Login & middot; Nagios XI],
UncommonHeaders[content-security-policy], X-Frame-Options[SAMEORIGIN], X-UA-
```

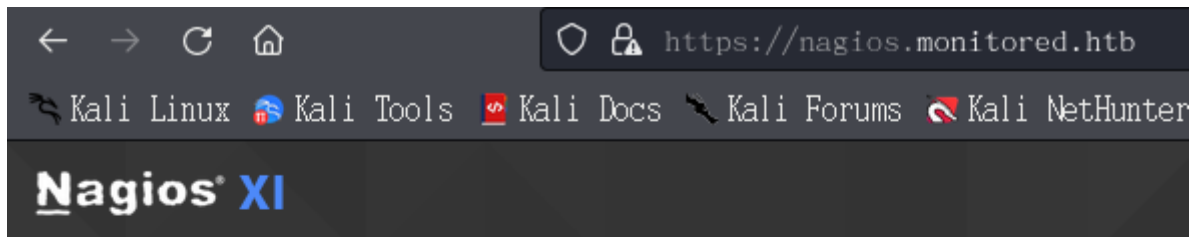
Compatible[IE=Edge]

[1] + done whatweb

https://nagios.monitored.htb/ [200 OK] Apache[2.4.56], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.56 (Debian)], IP[10.10.11.248], JQuery[3.6.0], Script[text/javascript], Title[Nagios XI]

- WEB 443Port

共3頁



Welcome

Click the link below to get started using Nagios XI.

[Access Nagios XI](#)

Check for tutorials and updates by visiting the Nagios Library at library.nagios.com.

Problems, comments, etc, should be directed to our support forum at support.nagios.com/forum/.

目錄報破，有兩個，java異常，另一個有出現登入畫面

```
[02:47:46] 301 - 335B - /javascript → https://nagios.monitored.htb/javascript/  
[02:48:03] 401 - 468B - /nagios  
[02:48:03] 401 - 468B - /nagios/
```



再繼續爆破

```
(root@kali) [~]
# ffuf -u "https://nagios.monitored.htb/nagiosxi/FUZZ" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -r

v2.1.0-dev
nagios.monitored.htb Port 443

:: Method      : GET
:: URL         : https://nagios.monitored.htb/nagiosxi/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : true
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

images [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 289ms]
# This work is licensed under the Creative Commons [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 322ms]
about [Status: 200, Size: 18495, Words: 3095, Lines: 310, Duration: 326ms]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 346ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 349ms]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 379ms]
# [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 427ms]
# [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 425ms]
# [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 442ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 375ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 365ms]
# [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 416ms]
# [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 405ms]
# Copyright 2007 James Fisher [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 404ms]
# on at least 2 different hosts [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 392ms]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 408ms]
help [Status: 200, Size: 26749, Words: 5495, Lines: 468, Duration: 306ms]
tools [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 323ms]
mobile [Status: 200, Size: 15978, Words: 2562, Lines: 225, Duration: 312ms]
admin [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 317ms]
reports [Status: 200, Size: 26755, Words: 5495, Lines: 468, Duration: 326ms]

account [Status: 200, Size: 26755, Words: 5495, Lines: 468, Duration: 309ms]
includes [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 292ms]
backend [Status: 200, Size: 108, Words: 4, Lines: 5, Duration: 309ms]
db [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 278ms]
api [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 282ms]
config [Status: 200, Size: 26753, Words: 5495, Lines: 468, Duration: 333ms]
views [Status: 200, Size: 26751, Words: 5495, Lines: 468, Duration: 310ms]
sounds [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 279ms]
terminal [Status: 200, Size: 5215, Words: 1247, Lines: 124, Duration: 348ms]
[Status: 200, Size: 26737, Words: 5495, Lines: 468, Duration: 345ms]

v1 [Status: 200, Size: 32, Words: 4, Lines: 2, Duration: 324ms]
:: Progress: [41899/220560] :: Job [1/1] :: 146 req/sec :: Duration: [0:06:33] :: Errors: 0 ::
```

ffuf -u "https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ" -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Method: GET
URL: https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ
Wordlist: FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Follow redirects: false
Calibration: false
Timeout: 10
Threads: 40
Matcher: Response status: 200-299,301,302,307,401,403,405,500
Filter: Response size: 32

license [Status: 200, Size: 34, Words: 3, Lines: 2, Duration: 1870ms]
%20 [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 305ms]
video games [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 306ms]
authenticate [Status: 200, Size: 53, Words: 7, Lines: 2, Duration: 2167ms]
spyware doctor [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 289ms]
4%20Color%2099%20IT2 [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 268ms]
nero 7 [Status: 403, Size: 286, Words: 20, Lines: 10, Duration: 313ms]

https://nagios.monitored.htb/nagiosxi/api/v1/license

error: "Unknown API endpoint."

https://nagios.monitored.htb/nagiosxi/api/v1/authenticate

Request: POST /nagiosxi/api/v1/authenticate HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=kfiq7688kv5003pmegg9po3jq2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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: zh-TW
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Content-Length: 46

Response: HTTP/1.1 200 OK
Date: Sun, 18 Feb 2024 11:41:17 GMT
Server: Apache/2.4.56 (Debian)
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Content-Length: 49
Connection: close
Content-Type: application/json
{"error": "Must be valid username and password."}

TCP找不到相關資訊，掃描UDP看看

—# bash incursore.sh 10.10.11.248 -t udp

@wirzka

Launching a udp scan on 10.10.11.248

Host is likely running Linux

[*] UDP port scan launched

PORT	STATE	SERVICE
123/udp	open	ntp
161/udp	open	snmp

Making a script scan on UDP ports: 123, 161

PORT	STATE	SERVICE	VERSION
123/udp	open	ntp	NTP v4 (unsynchronized)
161/udp	open	snmp	SNMPv1 server; net-snmp SNMPv3 server (public)

| snmp-info:

| enterprise: net-snmp

| engineIDFormat: unknown

| engineIDData: 6f3fa7421af94c6500000000

| snmpEngineBoots: 35

|_ snmpEngineTime: 1h27m16s

Service Info: Host: monitored

161 UDP

參考URL : <https://book.hacktricks.xyz/network-services-pentesting/pentesting-snmp>

```
(root@kali)-[~/hackthebox/Monitored/161]
# snmpbulkwalk -c public -v2c nagios.monitored.htb > out.txt

(root@kali)-[~/hackthebox/Monitored/161]
# cat out.txt | grep check
iso.3.6.1.2.1.25.4.2.1.4.921 = STRING: "postgres: 13/main: checkpointer "
iso.3.6.1.2.1.25.4.2.1.5.597 = STRING: "-c sleep 30; sudo -u svc /bin/bash -c /opt/scripts/check_host.sh svc XjH7VCe
howpR1xZB "
iso.3.6.1.2.1.25.4.2.1.5.1391 = STRING: "-u svc /bin/bash -c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
iso.3.6.1.2.1.25.4.2.1.5.1392 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
```

猜測是WEB的帳密(猜測失敗)、22也失敗

user : svc

passwd : XjH7VCehowpR1xZB

使用先前爆破的<https://nagios.monitored.htb/nagios/>

可登入

Browser address bar: <https://nagios.monitored.htb/nagios/>

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | DuckDuckGo | 保有隱... | JSQ

Nagios®

General

Home
Documentation

Current Status


Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Problems
Services (Unhandled)
Hosts (Unhandled)
Network Outages

Quick Search:

Reports

Availability
Trends (Legacy)
Alerts
History
Summary
Histogram (Legacy)
Notifications
Event Log

System



✓ Daemon running with PID 25455

Nagios® Core™
Version 4.4.13 in Nagios XI

[Back to Nagios XI](#)

Quick Links

- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

找到版本CVE漏洞

<https://github.com/jakgibb/nagiosxi-root-rce-exploit> [錯誤，並無上傳漏洞]

<https://medium.com/@n1ghtcr4wl3r/nagios-xi-vulnerability-cve-2023-40931-sql-injection-in-banner-ace8258c5567> [找到此漏洞，但需要其他要素。。。]

因找到帳密，使用之前找到需要帳密的WEB。但登入失敗

<https://nagios.monitored.htb/nagiosxi/api/v1/authenticate>

Send

Cancel

< >

Request

Response

Pretty Raw Hex

1 POST /nagiosxi/api/v1/authenticate HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=kfiq7688kv5003pmegg9po3jq2
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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: zh-TW
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15 Content-Length: 40
16
17 username=svc&password=XjH7VCehowpR1xZB
18

Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Sun, 18 Feb 2024 12:10:46 GMT
3 Server: Apache/2.4.56 (Debian)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
6 Content-Length: 49
7 Connection: close
8 Content-Type: application/json
9
10 {
11 "error": "Must be valid username and password."
12 }
13

但使用<https://nagios.monitored.htb/nagiosxi/login.php> 用Burp
更改成

1 x 2 x +

Send Cancel < >

Request

Pretty Raw Hex

```
1 POST /nagiosxi/api/v1/authenticate HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=kfiq7688kv5003pmegg9po3jq2
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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: zh-TW
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f%noauth=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 38
11 Origin: https://nagios.monitored.htb
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18 Connection: close
19
20 username=svc&password=XjH7VCehowpR1xZB
```

Response

Pretty Raw Hex Bender

```
1 HTTP/1.1 200 OK
2 Date: Sun, 18 Feb 2024 12:10:28 GMT
3 Server: Apache/2.4.56 (Debian)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
6 Content-Length: 151
7 Connection: close
8 Content-Type: application/json
9
10 {
  "username": "svc",
  "user_id": "2",
  "auth_token": "978caa0bee677ea65530bd7ddd3613d7489f8b1b",
  "valid_min": 5,
  "valid_until": "Sun, 18 Feb 2024 07:15:30 -0500"
}
11
```

auth_token : 978caa0bee677ea65530bd7ddd3613d7489f8b1b

找到模擬nagiosls

<http://nagiosls.demos.nagios.com/nagioslogserver/help/api>