

Nax

Nax is a vulnerable machine of the tryhackme platform.

Link: <https://tryhackme.com/room/nax>

Goal: Find the user and root flags.

Report by: Martin Martinez

Intro:

In this machine we have to solve a series of challenges with the clues that the creator has not given, look for credentials and find an exploit for the running version and look for the exploits.

Enumeration

As always before listing the available ports on the machine I like to know what system I am dealing with, so to find out the operating system send an ICMP packet and based on the TTL get the operating system.

ping -c 1 10.10.41.244 > os-discover.txt

The TTL is equal to 61 **so it is a machine with some Linux distribution**, the TTL decreases because the connection goes through some intermediaries before reaching the IP object.

```
(kali@kali)-[~/TryHackMe/nax]
$ cat os-discover.txt
PING 10.10.41.244 (10.10.41.244) 56(84) bytes of data.
64 bytes from 10.10.41.244: icmp_seq=1 ttl=61 time=408 ms

--- 10.10.41.244 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 408.190/408.190/408.190/0.000 ms
```

Now that I know better what I'm up against, I have to list the passes and I like to divide this into two stages:

- One to get only the ports open as quickly as possible.
- Another to focus on those ports and get more information.

All Ports

nmap -sS --min-rate 5000 -Pn -n 10.10.41.244 -p- --open -vvv -oA nmap/all/allPorts

```
# Nmap 7.91 scan initiated Sun Oct 24 13:08:34 2021 as:
/all/allPorts 10.10.41.244
Nmap scan report for 10.10.41.244
Host is up, received user-set (0.22s latency).
Scanned at 2021-10-24 13:08:34 CDT for 22s
Not shown: 53638 closed ports, 11891 filtered ports
Reason: 53638 resets and 11891 no-responses
Some closed ports may be reported as filtered due to --c
PORT      STATE SERVICE REASON
22/tcp    open  ssh     Asyn-ack, ttl 61
25/tcp    open  smtp    syn-ack, ttl 61
80/tcp    open  http    syn-ack, ttl 61
389/tcp   open  ldap    syn-ack, ttl 61
443/tcp   open  https   syn-ack, ttl 61
5667/tcp  open  unknown syn-ack, ttl 61

Read data files from: /usr/bin/../../share/nmap
```

Thanks to this super fast scan I can now focus only on the open ports and get much more information:

Deep Scan

nmap -sC -sV -p 22,80,389,443,5667 -Pn -n 10.10.41.244 -oA nmap/deep/deepScan

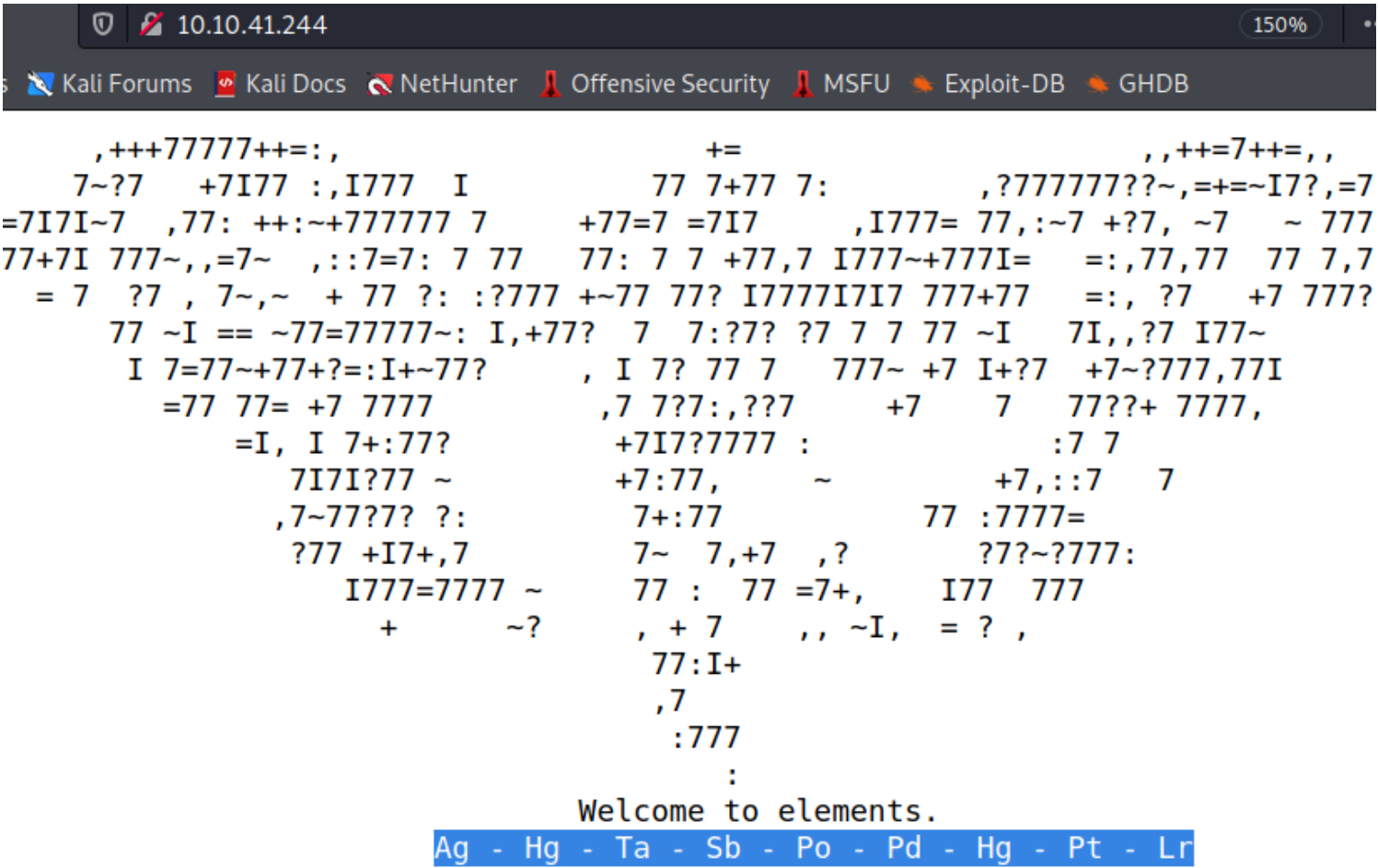
```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 62:1d:d9:88:01:77:0a:52:bb:59:f9:da:c1:a6:e3:cd (RSA)
|_   256 af:67:7d:24:e5:95:f4:44:72:d1:0c:39:8d:cc:21:15 (ECDSA)
|_   256 20:28:15:ef:13:c8:9f:b8:a7:0f:50:e6:2f:3b:1e:57 (ED25519)
25/tcp    open  smtp         Postfix smtpd
|_ _smtp-commands: ubuntu.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSNOTIFICATIONS, DSN,
|_ _ssl-cert: Subject: commonName=ubuntu
|_   Not valid before: 2020-03-23T23:42:04
|_   Not valid after:  2030-03-21T23:42:04
|_ _ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: Site doesn't have a title (text/html).
389/tcp   open  ldap         OpenLDAP 2.2.X - 2.3.X
443/tcp   open  ssl/http     Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: 400 Bad Request
|_ _ssl-cert: Subject: commonName=192.168.85.153/organizationName=Nagios Enterprises/stateOrProvinceName=US
|_   Not valid before: 2020-03-24T00:14:58
|_   Not valid after:  2030-03-22T00:14:58
|_ _ssl-date: TLS randomness does not represent time
|_   tls-alpn:
|_     http/1.1
5667/tcp  open  tcpwrapped
Service Info: Host: ubuntu.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

While reviewing the page I ran a directory search:

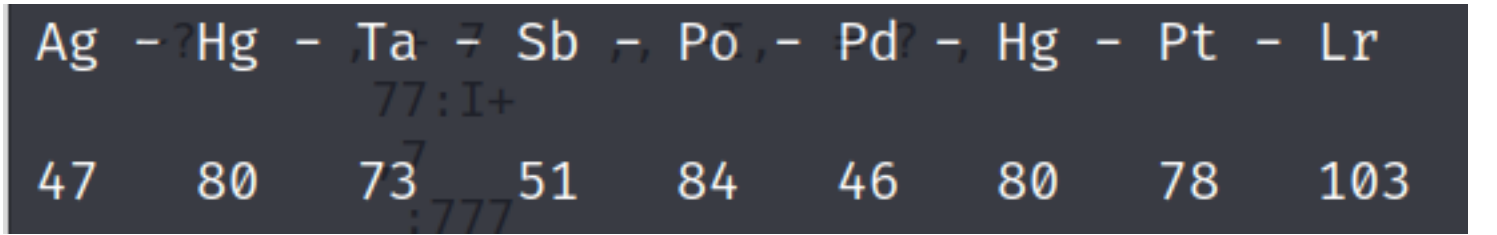
dirsearch -u <http://10.10.41.244>

```
[13:11:51] 403 - 277B - /.php
[13:11:51] 403 - 277B - /.php3
[13:12:53] 403 - 277B - /cgi-bin/
[13:13:24] 200 - 1KB - /index.html
[13:13:29] 301 - 317B - /javascript → http://10.10.41.244/javascript/
[13:13:47] 401 - 459B - /nagios
[13:13:47] 401 - 459B - /nagios/
[13:13:55] 403 - 277B - /server-status
[13:13:55] 403 - 277B - /server-status/
```

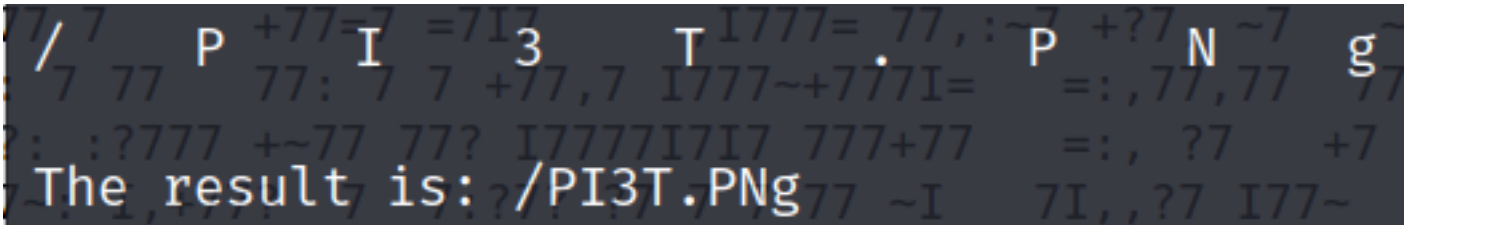
The nagios directory caught my attention but in order to access it I needed some credentials.



When entering the web page I find something quite strange, below there are some letters but in reality they are the symbols of some chemical elements when I obtained their number I got the following:



These numbers allowed me to obtain a secret directory, since when converting its ASCII value to text you get the following:



This allowed me to download a rather strange image that made no sense to me, but when I searched for "piet decoder", I found a page that allowed me to upload similar images and maybe I could get something and so I did!

<https://www.bertnase.de/npviet/npviet-execute.php>

Hi,

Welcome to [npviet online](#) !

Info: upload status: Ok

Info: **Oops - no suitable picture found: no useful image format...**

Info: Trying to execute anyway...

Info: executing: npviet -w -e 220000 PI3T.PNG

libpng warning: Extra compressed data.

libpng warning: Extra compression data.

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

There are the credentials, so now I have access to the nagios directory!

user: nagiosadmin

password: n3p3UQ&9BjLp4\$7uhWdY

FootHold

When you enter the website you can see the version of nagios running as well as a warning that it needs to be updated, this is very good as we can check for vulnerabilities!



✓ Daemon running with PID 952

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.

To search for vulnerabilities you need to look a little further than the version, I recommend you the following link:

<https://www.nagios.com/products/security/>

CVE-2019-15949

Remote command execution as root
vulnerability in Nagios XI's getprofile.sh script. The script runs when profiles are created via the profile component. User must have access to edit plugins or access to the nagios user on the server.

CVE-2019-15949

🚧 CVE-2019-15949 Detail

Current Description

Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios user, or access as the admin user via the web interface. The getprofile.sh script, invoked by downloading a system profile (profile.php?cmd=download), is executed as root via a passwordless sudo entry; the script executes check_plugin, which is owned by the nagios user. A user logged into Nagios XI with permissions to modify plugins, or the nagios user on the server, can modify the check_plugin executable and insert malicious commands to execute as root.

Exploit

In order to exploit this vulnerability we need to have some credentials, when searching for exploits I realized that there is one quite simple to use in metasploit, you just need to configure some parameters to exploit it.

The best thing is that we are the root user directly so we don't have to worry about escalating privileges.

```
meterpreter > cat user.txt
THM{84b17add1d72a9f2e99c33bc568ae0f1}
meterpreter > cat /root/root.txt
THM{c89b2e39c83067503a6508b21ed6e962}
meterpreter > |
```