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:

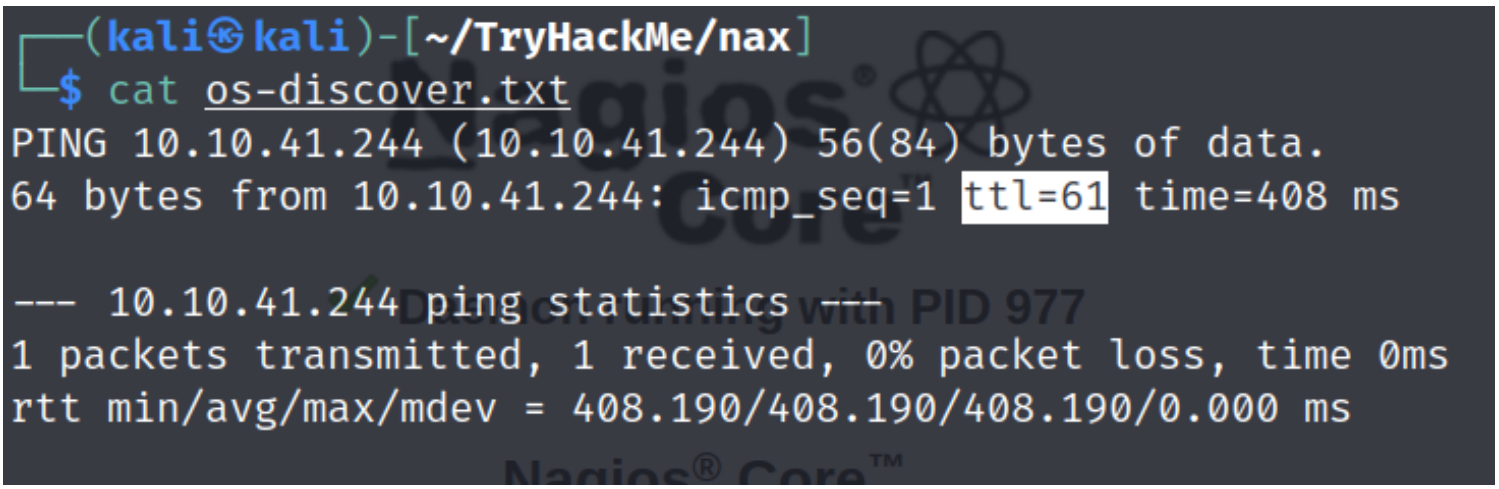
In this machine we have to solve a series of challenges with the clues that the creator has not given, look for credentials and find an exploit for the running version and look for the exploits.

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.

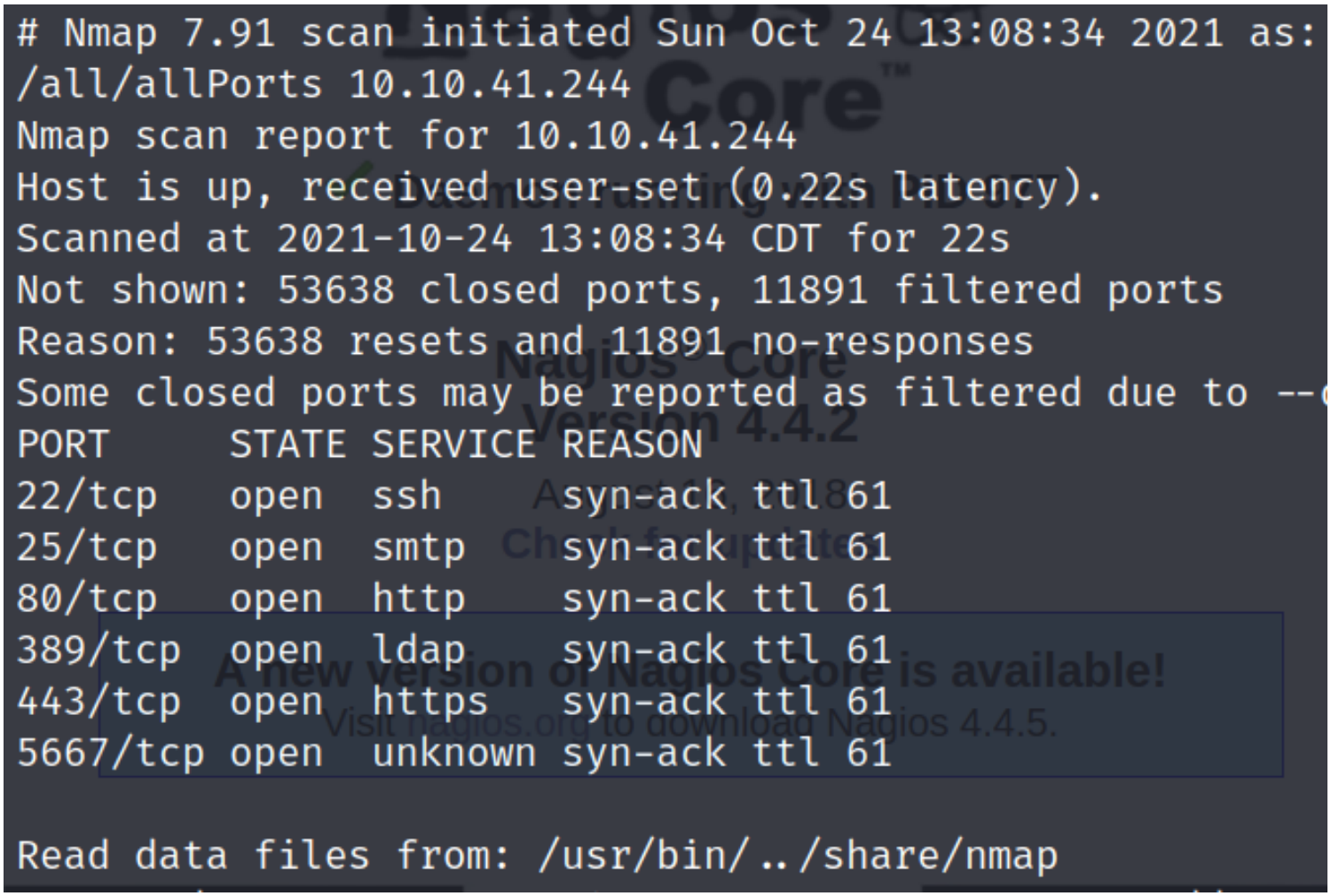


Now that I know better what I'm up against, I have to list the passes and I like to divide this into two stages:

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

All Ports

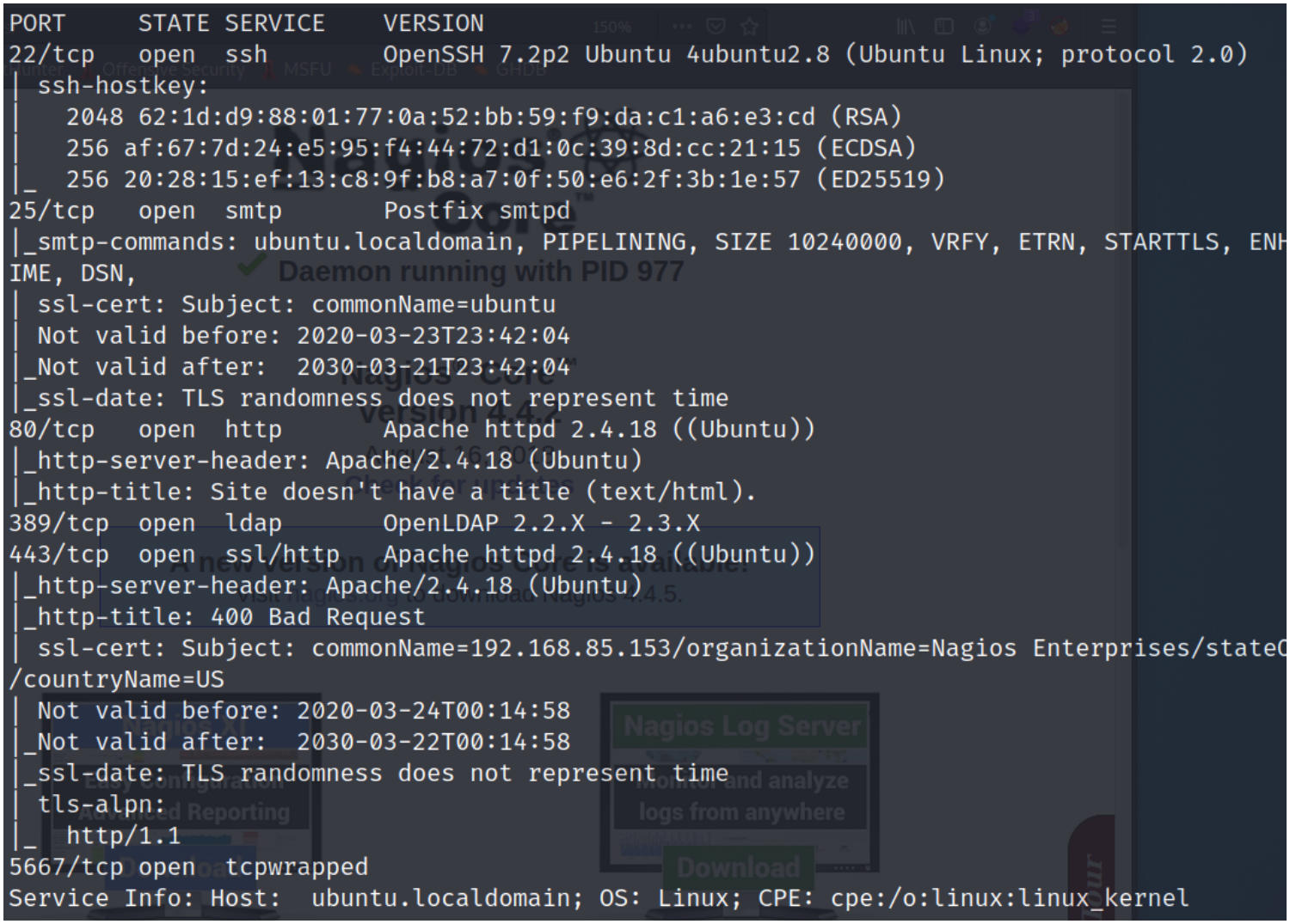
nmap -sS --min-rate 5000 -Pn -n 10.10.41.244 -p- --open -vvv -oA nmap/all/allPorts



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

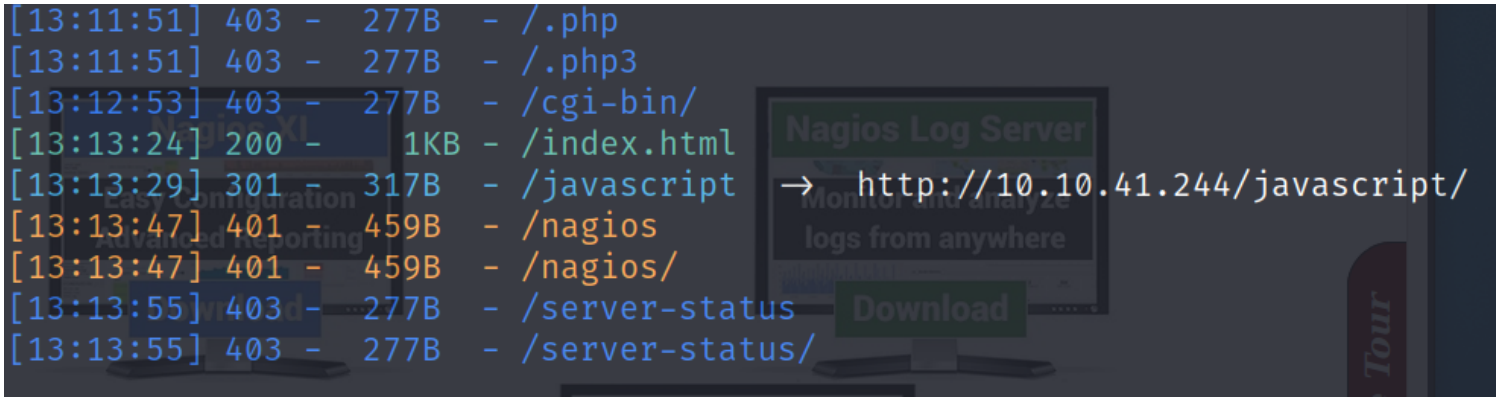
Deep Scan

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

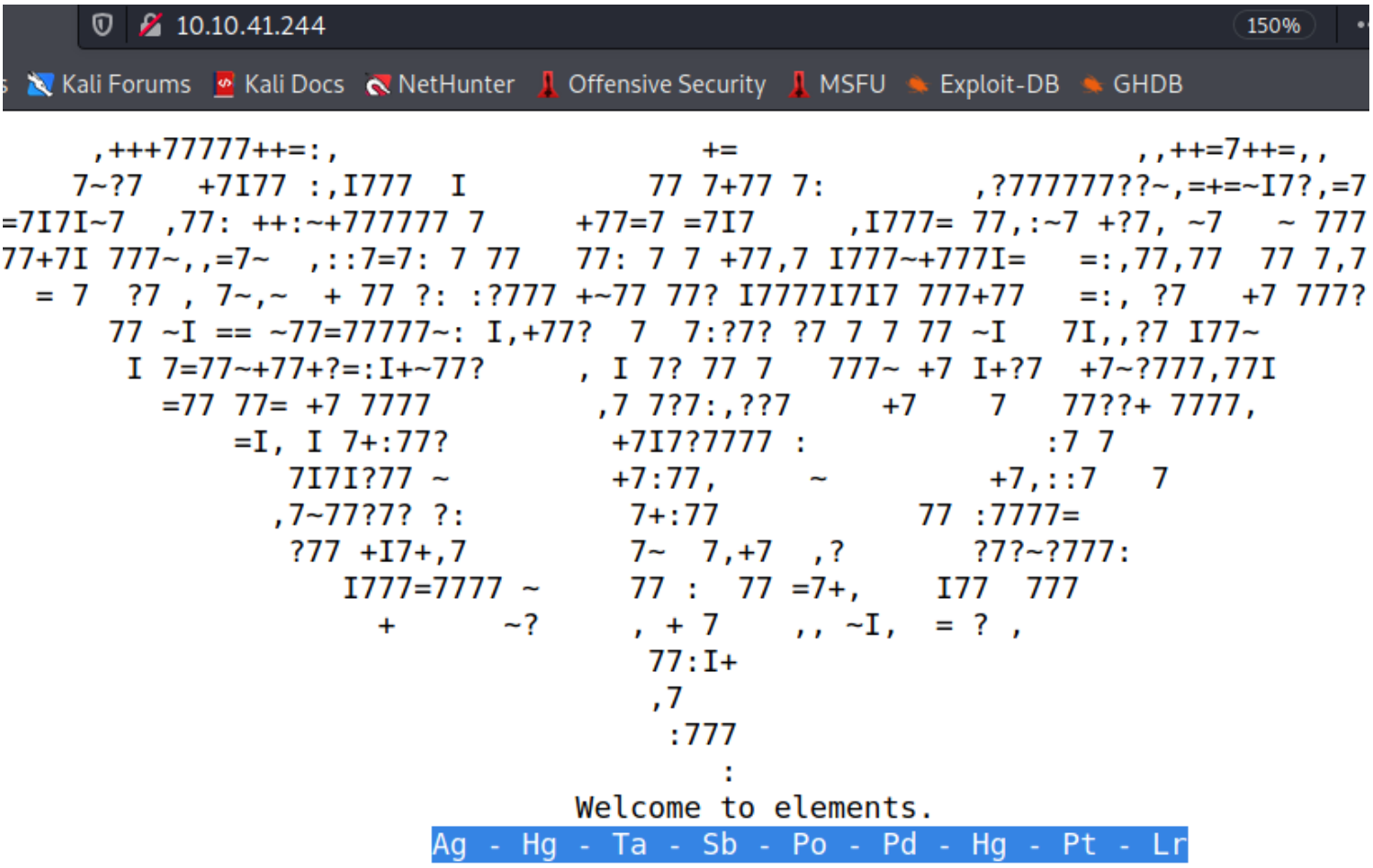


While reviewing the page I ran a directory search:

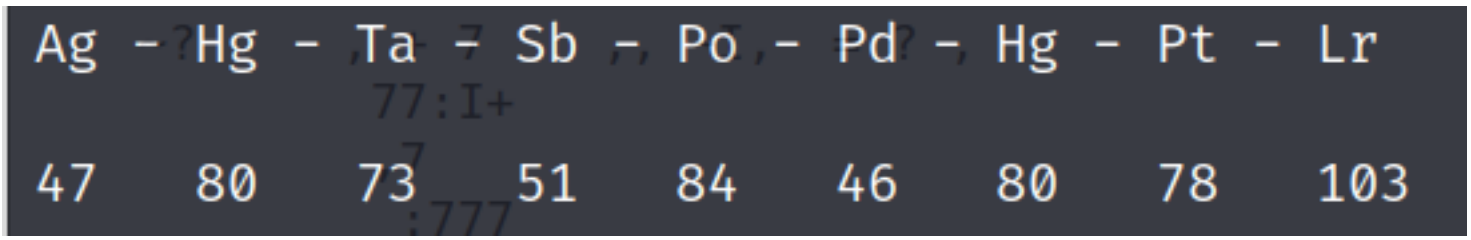
dirsearch -u http://10.10.41.244



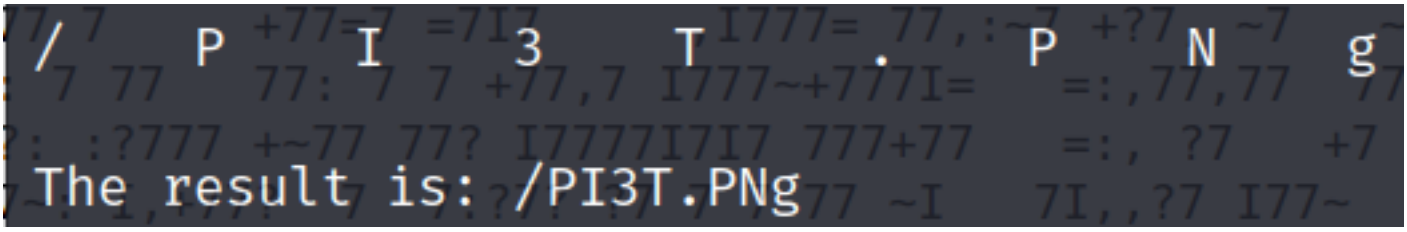
The nagios directory caught my attention but in order to access it I needed some credentials.



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/npiet/npiet-execute.php

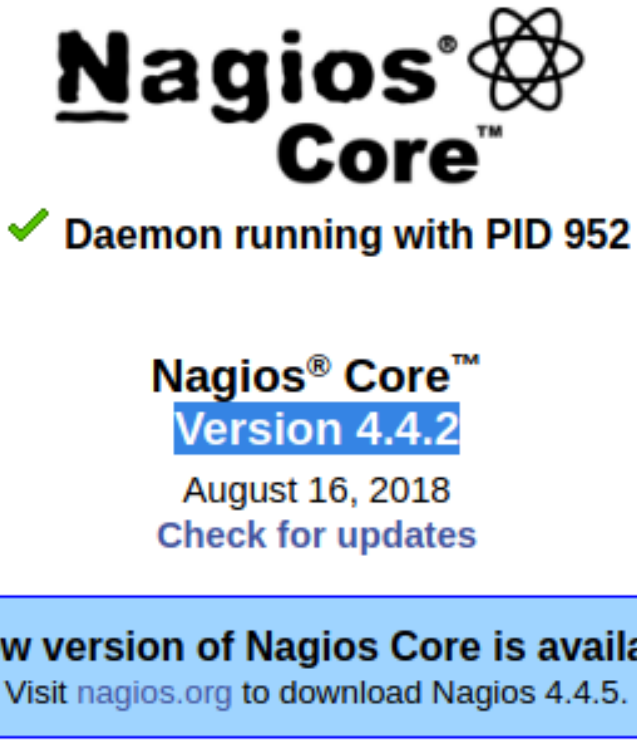
> Hi,
>
> Welcome to **npiet online** !
>
> Info: upload status: Ok
> Info: **Oops - no suitable picture found: no useful image format...**
> Info: Trying to execute anyway...
>
> Info: executing: npiet -w -e 220000 PI3T.PNg
>
> ---
>
> **libpng warning: Extra compressed data.**
> **libpng warning: Extra compression data.**
> **nagiosadmin%n3p3UQ&9BjLp4$7uhWdYnagiosadmin%n3p3UQ&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!



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.