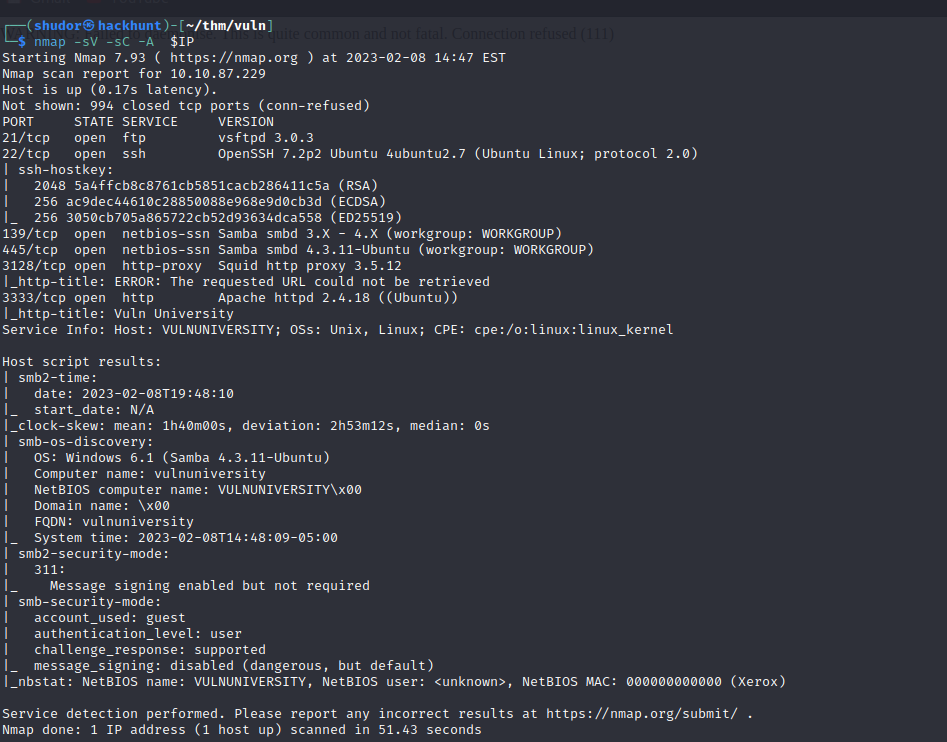
**Reconnaissance**

Nmap Scan



Scan the box, how many ports are open?

6

With the help of above image we can say that there is 6 port open

What version of the squid proxy is running on the machine?



3.5.12

How many ports will nmap scan if the flag -p-400 was used?

All port from 1 to 400 so it will be 400 ports

<https://nmap.org/book/port-scanning-options.html>

Using the nmap flag -n what will it not resolve?

DNS

<https://nmap.org/book/man-briefoptions.html>

What is the most likely operating system this machine is running?

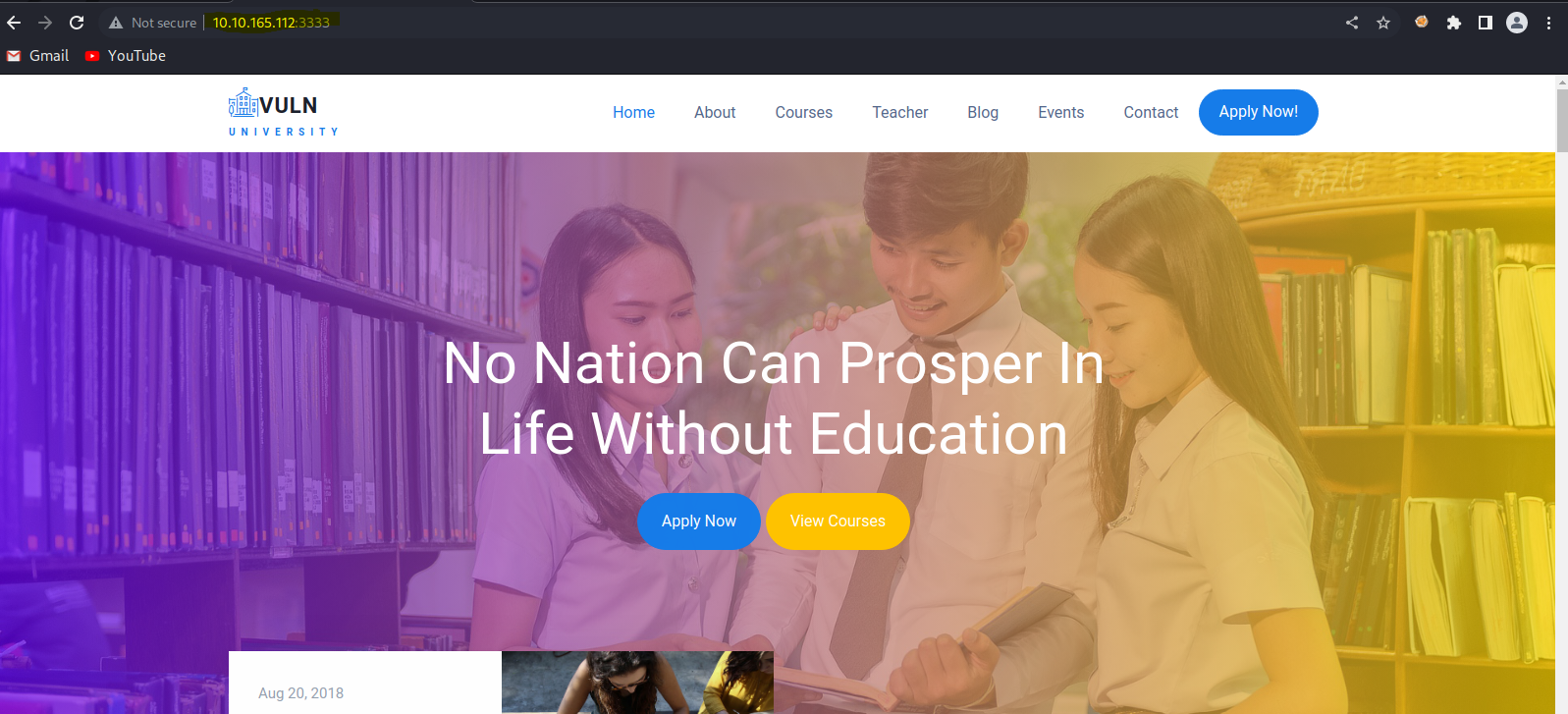
Ubuntu

Text

Description automatically generated

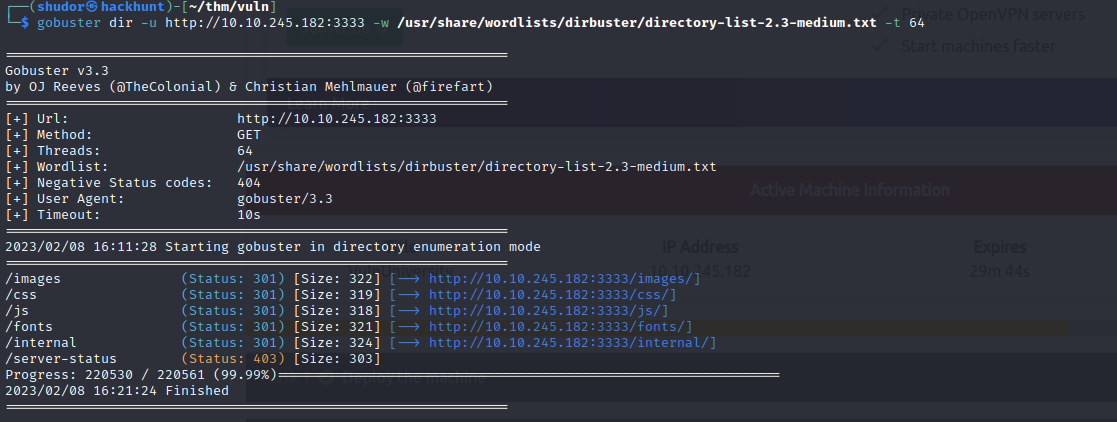
What port is the web server running on?

3333



**Locating Directories using gobuster**

Gobuster Scan



What is the directory that has an upload form page?

/internal

Graphical user interface, application

Description automatically generated

**Compromise the web server**

What common file type, which you'd want to upload to exploit the server, is blocked? Try a couple to find out.

Php

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, website

Description automatically generated

Text

Description automatically generated

What is the name of the user who manages the webserver?

bill

Graphical user interface

Description automatically generated

What is the user flag?

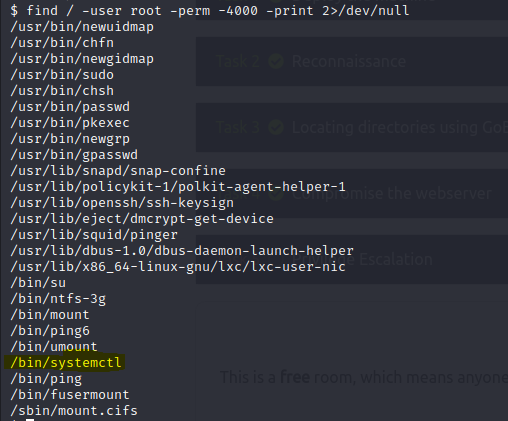
Text

Description automatically generated

8bd7992fbe8a6ad22a63361004cfcedb

**Privilege Escalation**

On the system, search for all SUID files. What file stands out?



Become root and get the last flag (/root/root.txt)

Text

Description automatically generated