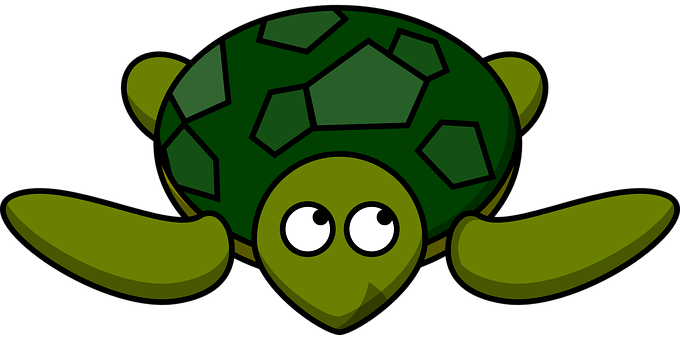
# TRYHACKME | 0DAY CTF Report

## Kənan Rəsulov Date: 17.02.2025

**Task:** As a part of my internship in Intern Intelligence, my first task is is to exploit a web application and gain access to a machine and perform privilege escalation. To achieve this I completed **0day** CTF in Tryhackme platform.



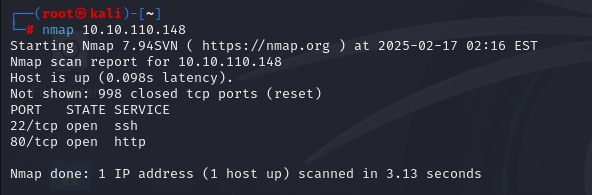
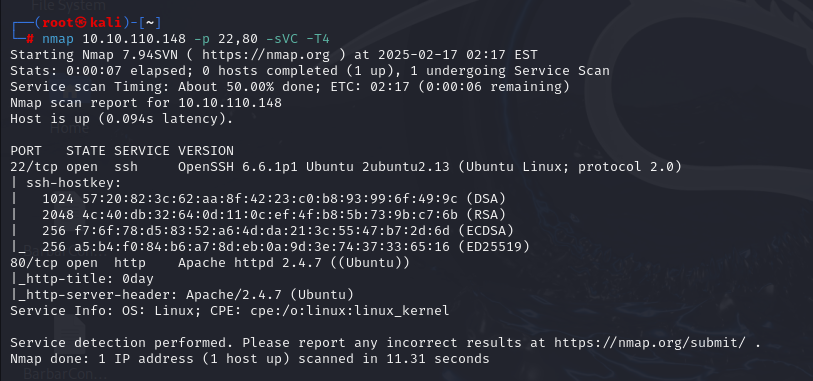
Credits to creators of this room [MuirlandOracle](https://tryhackme.com/p/MuirlandOracle) & [0day](https://tryhackme.com/p/0day)

### Table of contents

* Reconnaissance
* Gain initial access
* Privilege escalation

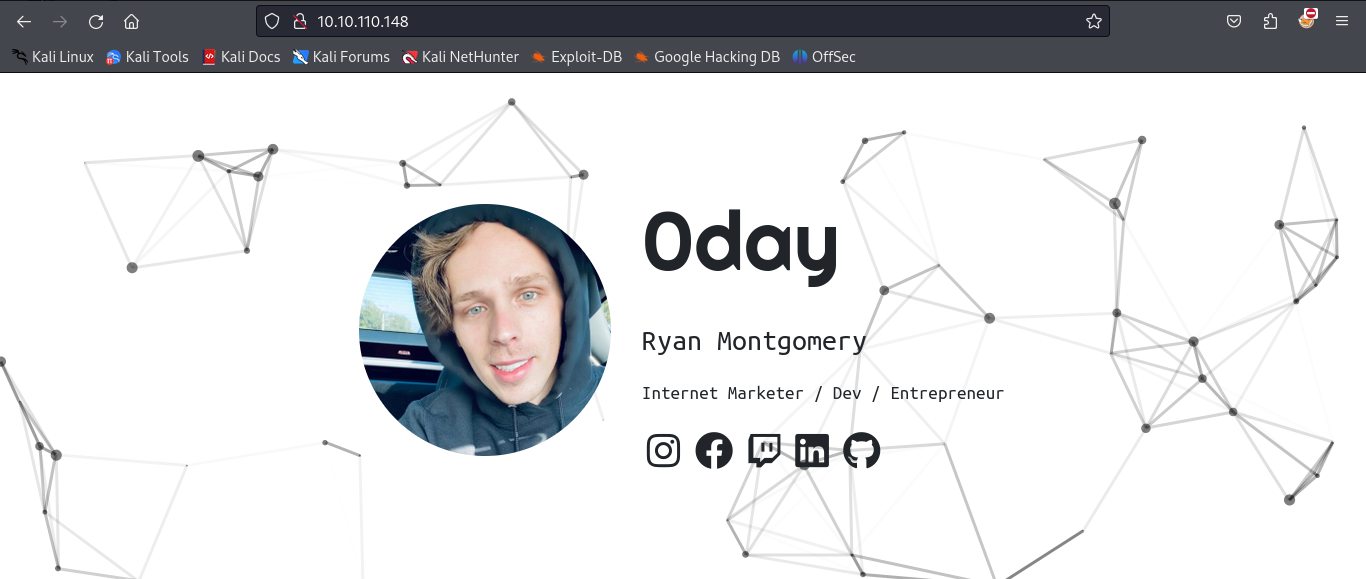
# Reconnaissance

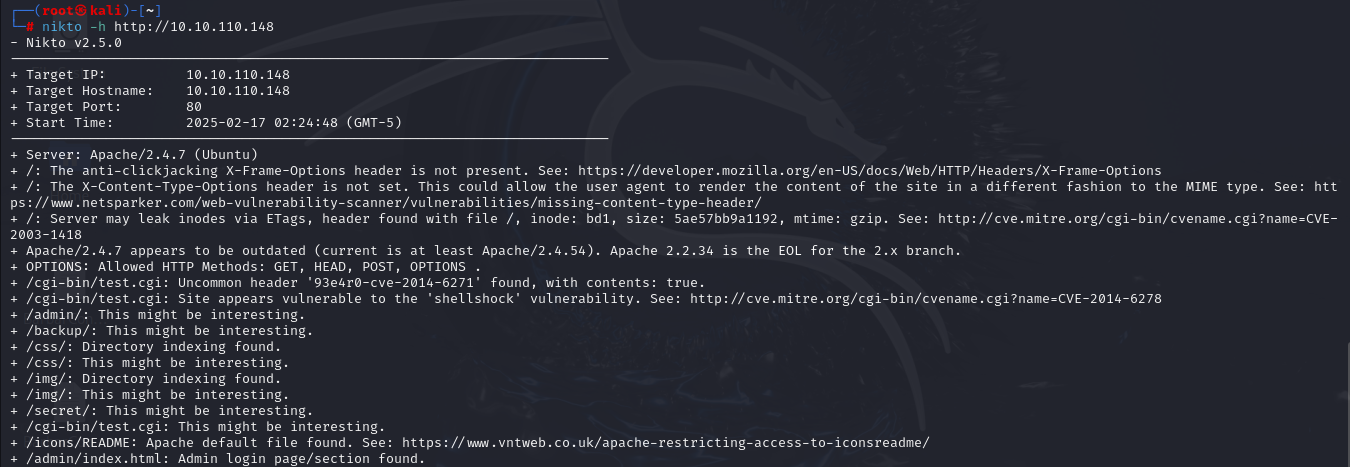
First of all we begin with port scanning with the tool *nmap*. Lets explore the open ports and display some information about them with relevant flags.



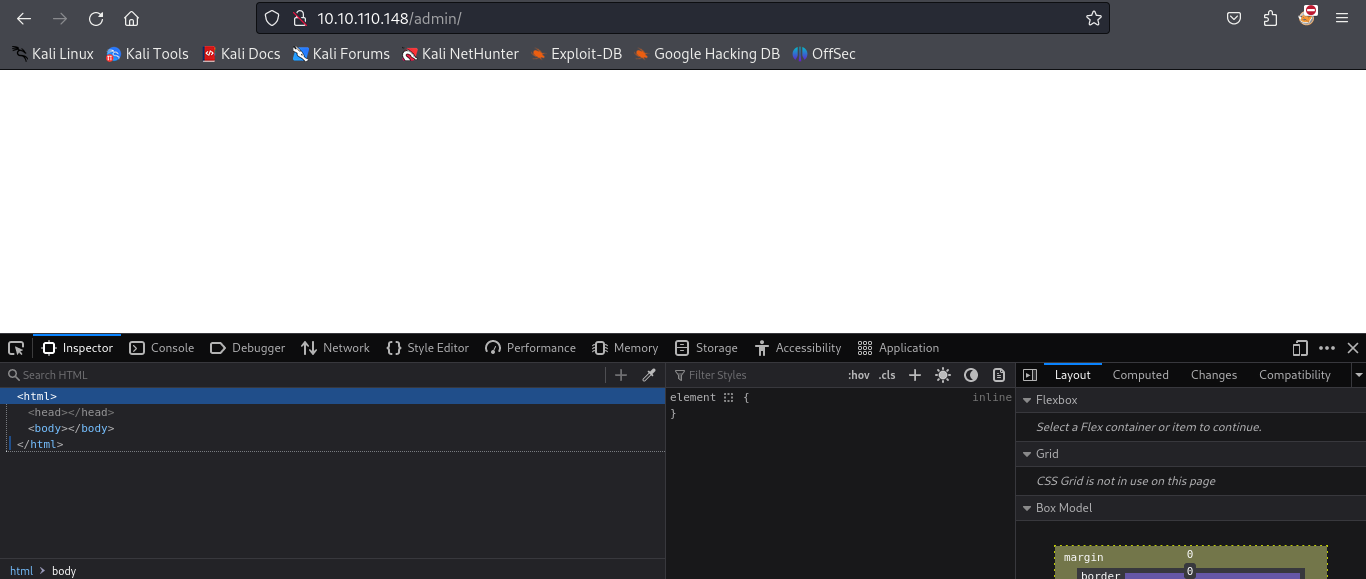
Let’s see... We have port 22 (ssh) and 80 (http) open. Before going further, we should check the website or anything located in that IP address. To do that, we simply paste the IP address to the browser’s URL input.

So after going to the adress we face a promotional webpage which shows a person named *“Ryan Montgomery”* and links to his social media accounts.

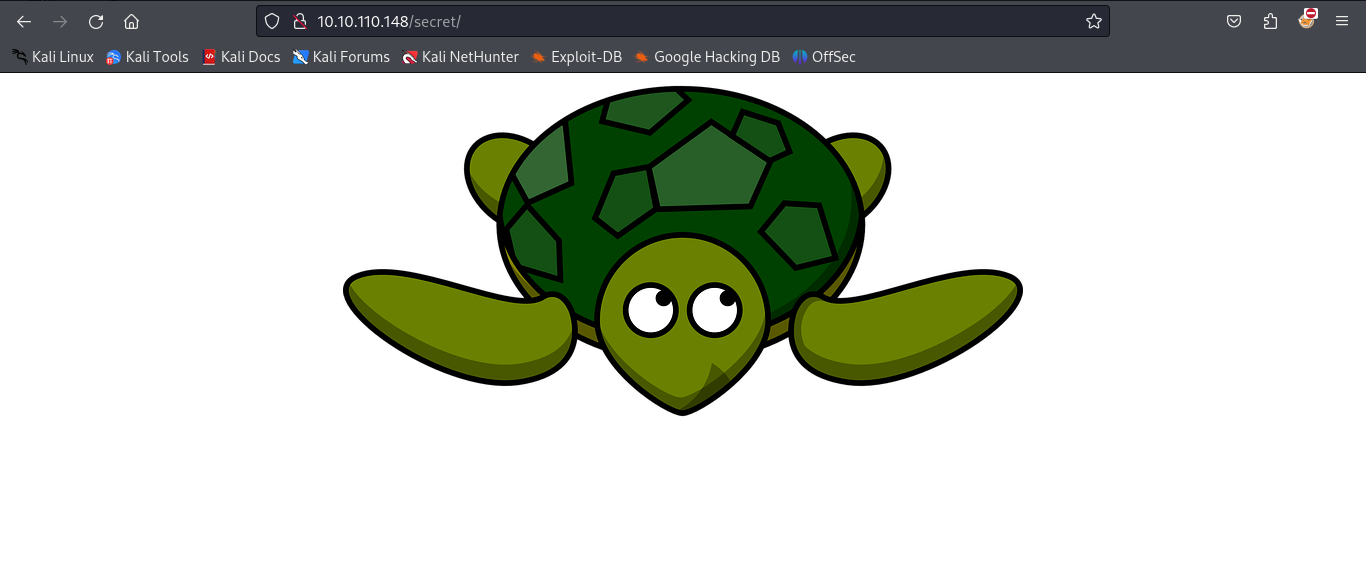


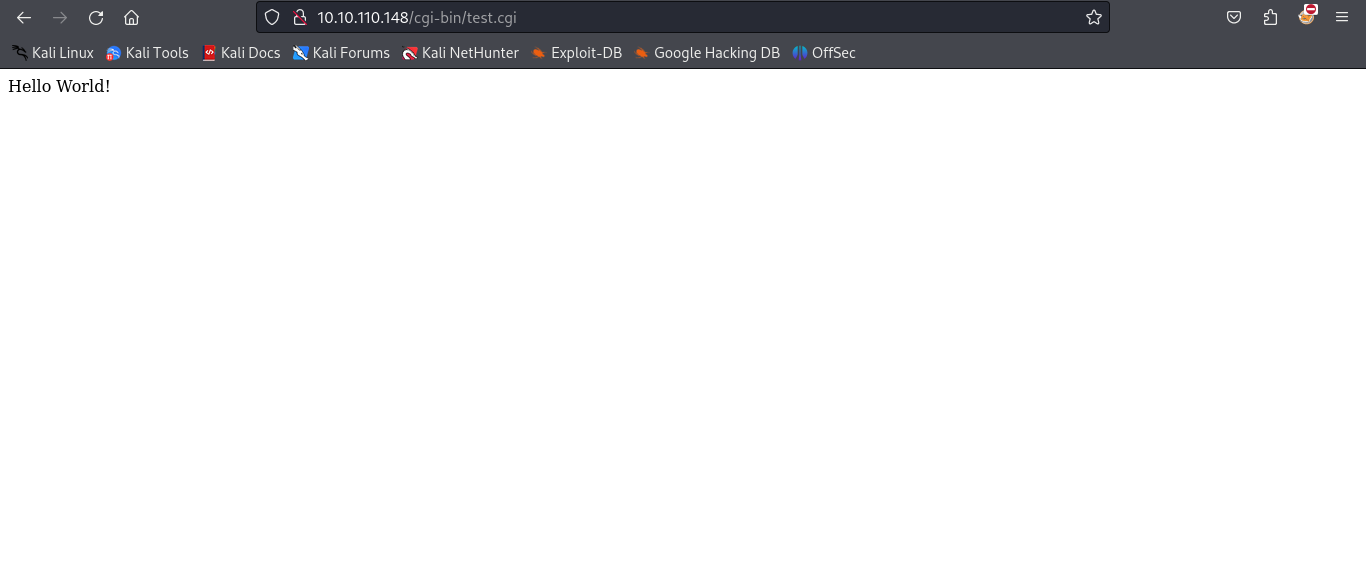
There is nothing interesting in this page, so we continue our exploration with the tool called *nikto* for enumeration.

We find out some interesting directories called; ‘secret’, ‘admin’, ‘cgi-bin’. And also a file named ‘test.cgi’ in the cgi-bin directory. There is also a vulnerability (CVE-2014-6278 Shellshock). But before let’s explore the interesting directories.

In the *admin* directory, there is nothing to see actually, though we inspect the HTML code of it.

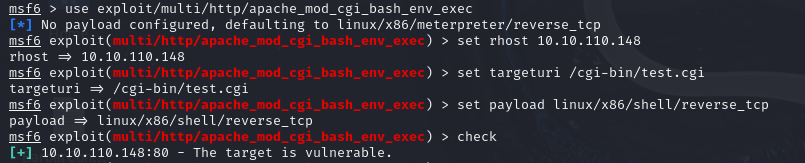
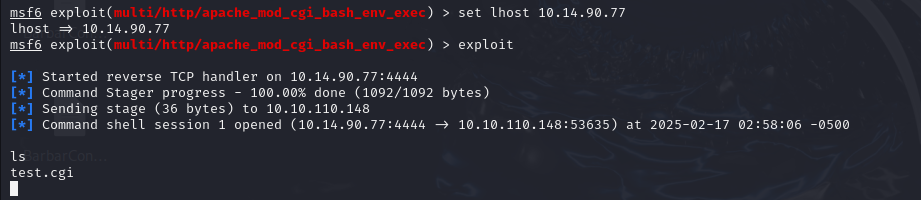
In the *secret* directory there is just a turtle image and nothing else.



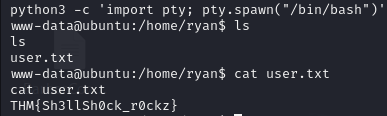
These directories all are rabbit hole, so let’s skip to the exploitation part. Our *shellshock* vulnerability is related with “/cgi-bin/test.cgi” path. After visiting this path, we encounter a page displaying “Hello World!” on the screen.

# Gain initial access

So something happening behind the curtains. We should go back to Shellshock vulnerability. After some research I found out that, Shellshock is a GNU Bash vulnerability that was discovered in 2014. The Shellshock vulnerabililty can affect numerous systems and attack vectors. GNU Bash through version 4.3 processes trailing strings after function definitions in environment variable values. This allows attackers to execute arbitrary code by using those external variables. In our situation, we can get a reverse shell using *meterpreter*.



We got our shell! First we upgrade our shell with python and, then go to the home directory and get our user flag from a user named *ryan*.

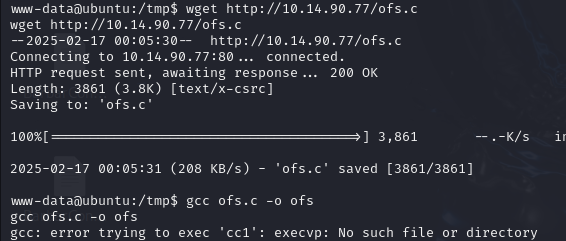


# Privilege escalation

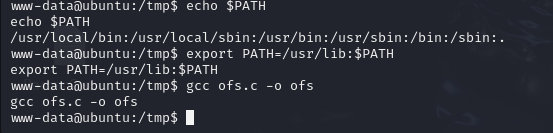
When I want to do privilege escalation I always check the kernel version first, because it is so simple to avoid it. Fortunately, our Ubuntu version is outdated and vulnerable.



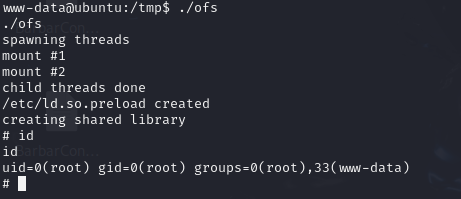
Doing some research, I find out CVE-2015-1328 for Linux kernel 3.13.0 < 3.19 exploit. So for the escalation, there is a **C** code and we must compile it in the target machine and execute it. To do this we write our payload to a **C** file and start a http server in our machine. Then from the target machine we use *wget* to download the file to compile it with *gcc*.



So we got an error called “error trying to exec ‘cc1’”. I surfed in the internet and discovered that, cc1 is the internal command which takes preprocessed C-language files and converts them to assembly. It's the actual part that compiles C. So gcc either gcc can’t find cc1 or it does not exist. I checked the **PATH** if it goes to the default path of cc1 in */usr/lib* and identified it does not check this path. So I edited the variable to visit that location first and compiled the file again.



And lastly there is one thing to do; executing the binary.



Now we are root user and can access to the root flag. And root.txt is:

THM{g00d\_j0b\_0day\_is\_Pleased}