Perfection walkthrough

Index

List of pictures

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
└─# nmap -sT -Pn -p- -sV -sC -O -A 10.10.11.253 -oA perfection
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 15:49 AEDT
Nmap scan report for 10.10.11.253
Host is up (0.022s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
|_  256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (ED25519)
80/tcp open  http    nginx
|_http-title: Weighted Grade Calculator
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=4/4%OT=22%CT=1%CU=40758%PV=Y%DS=2%DC=T%G=Y%TM=660E3
OS:19F%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)S
OS:EQ(SP=104%GCD=2%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST
OS:11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=F
OS:E88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M
OS:53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T
OS:4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
OS:%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y
OS:%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%
OS:RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   29.84 ms 10.10.14.1
2   30.00 ms 10.10.11.253

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.60 seconds
```

Figure 1 - nMap scan results

Ports open are 22 and 80. So, this machine has SSH enabled on port 22 and a web service running on port 80. Also, nMap has recognized Linux as operative system.

Initial foothold

I started the web application analysis running *gobuster*, *dirsearch* and *nikto* tools, but any of these tools provided useful information. So, I tried to interact to the web application via browser. Its home page is:

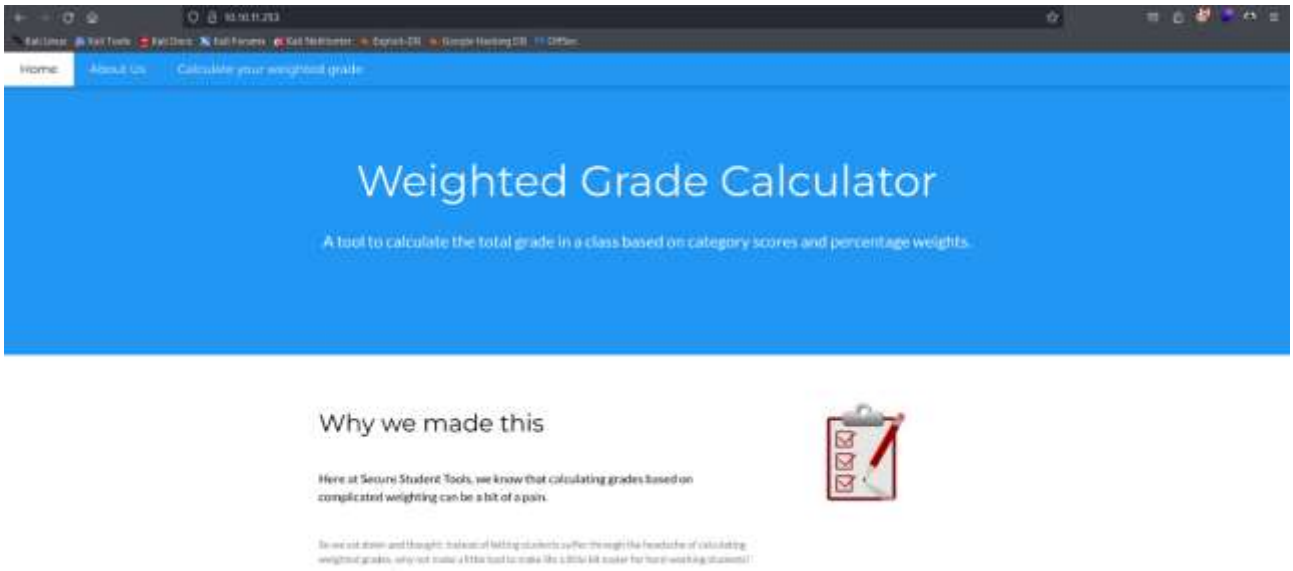

Figure 2 - Web application home page

This application provides a grade calculator with the following interface:

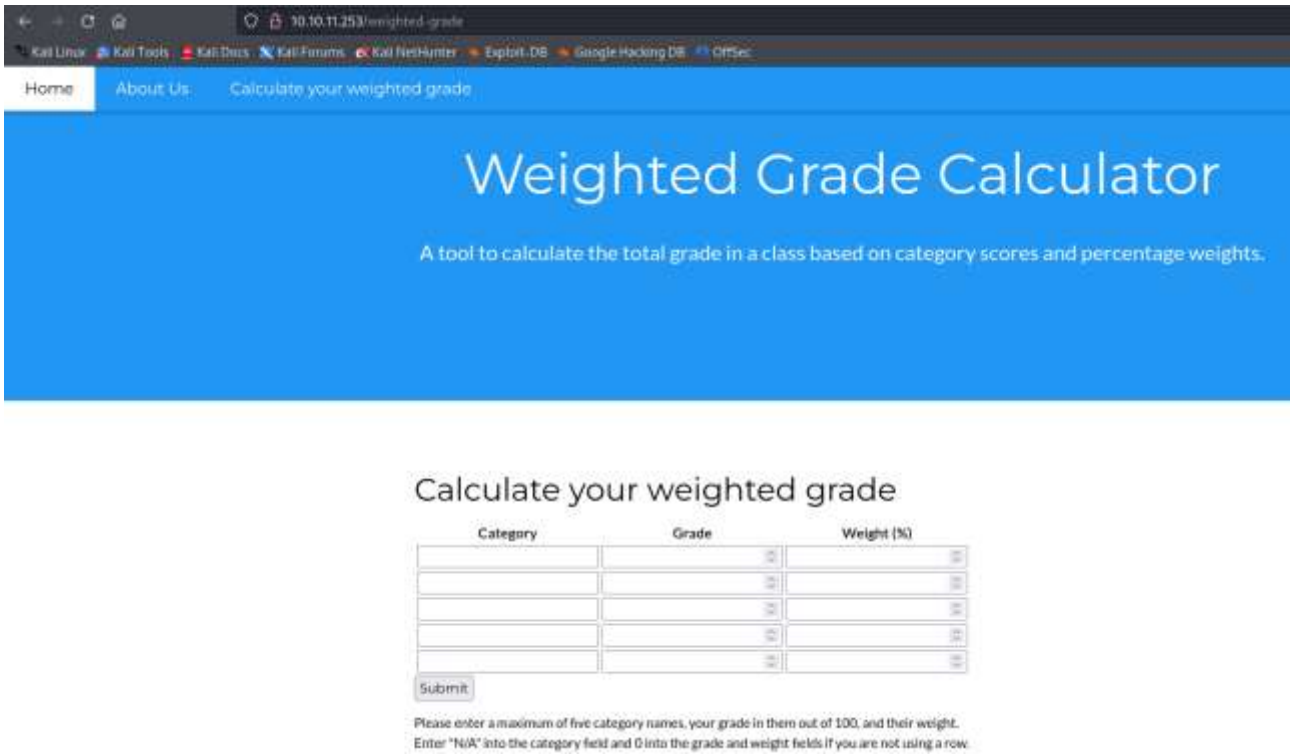

Figure 3 - Grade calculator interface

Also, I grabbed the following information using Wappalyzer:

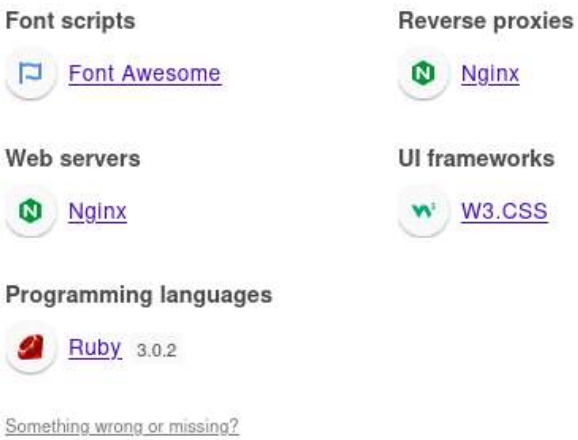

Figure 4 - Wappalyzer analysis

User flag

Classic XSS and SQL injection payload didn't work in the grade calculator form. However, while I tried some payload, I found out a way to broke the input validation, as shown in the following picture:

Figure 5 - Input validation broken

Another kind of attack I tried on this input file was Server-Side Template Injection (SSTI). Luckly, this kind of attack worked. So, I was able to execute commands. Of course, command syntax must match Ruby syntax, because server execute Ruby. Using the command in the following image, I obtained a shell:

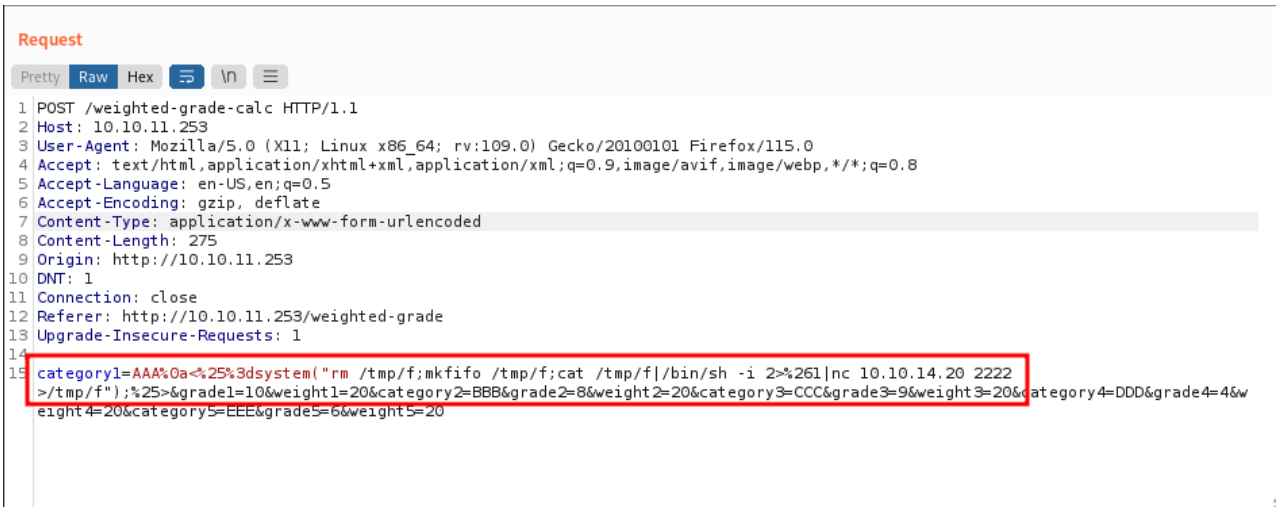

Figure 6 - Command to obtain a shell

Obviously, I need a listener on my attacker machine. I obtained this shell with ***susan*** user:

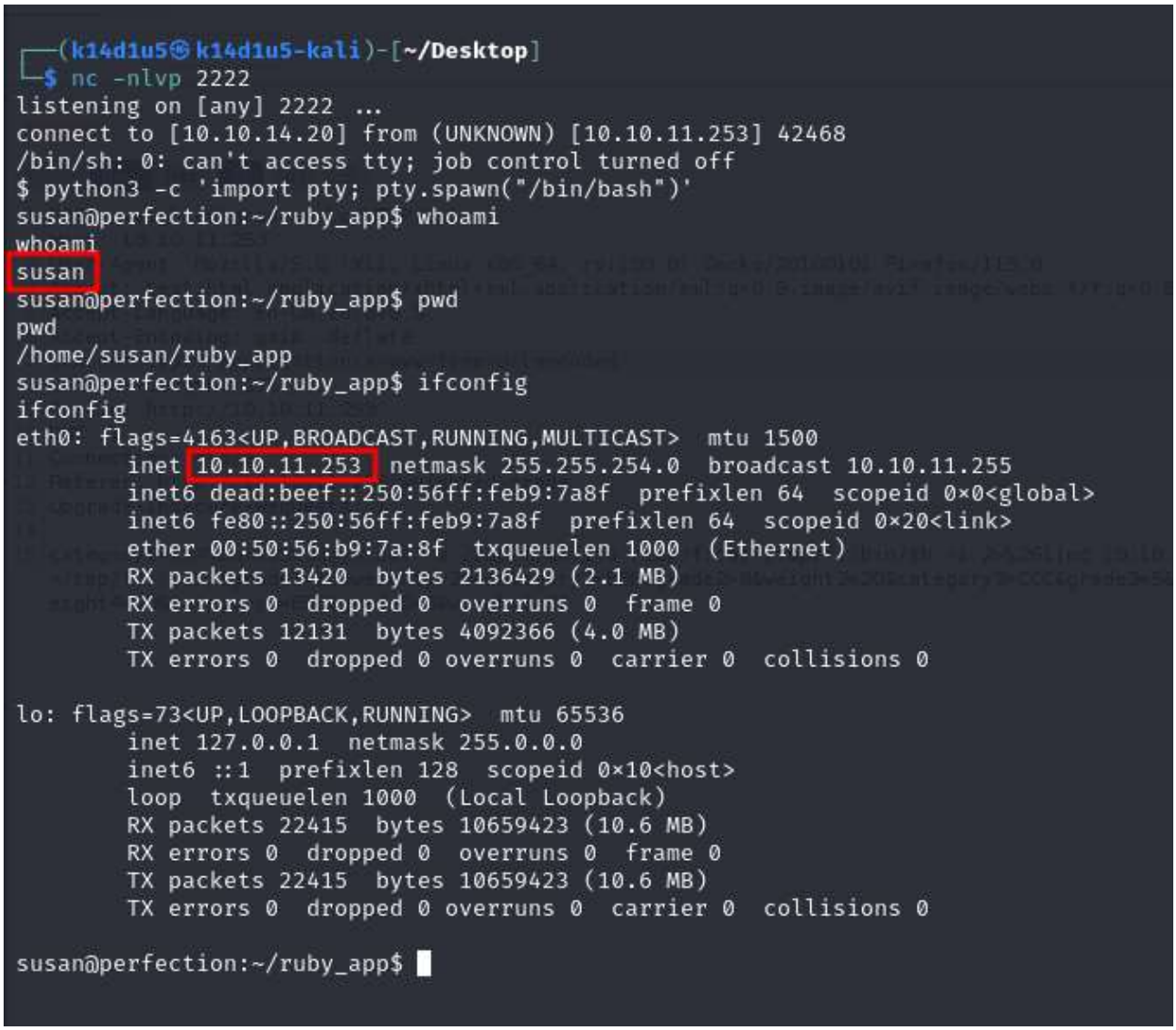

Figure 7 - User shell

At this point, I simply needed to retrieve the user flag (I forgot the screenshot).

Privilege escalation

To escalate my privileges, I found a very interesting file in a subdirectory of Susan's home directory:

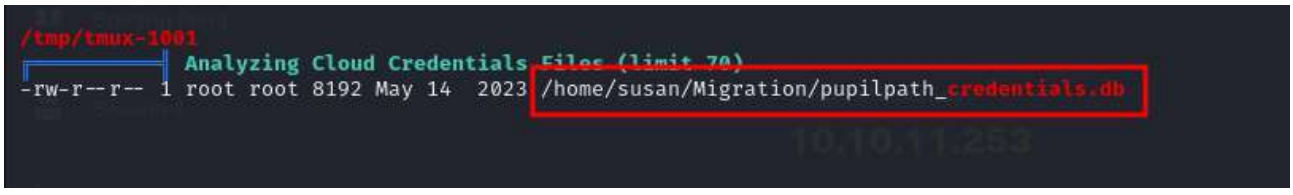

Figure 8 - Interesting credentials file

I was able to read the content of this file using ***strings*** command:

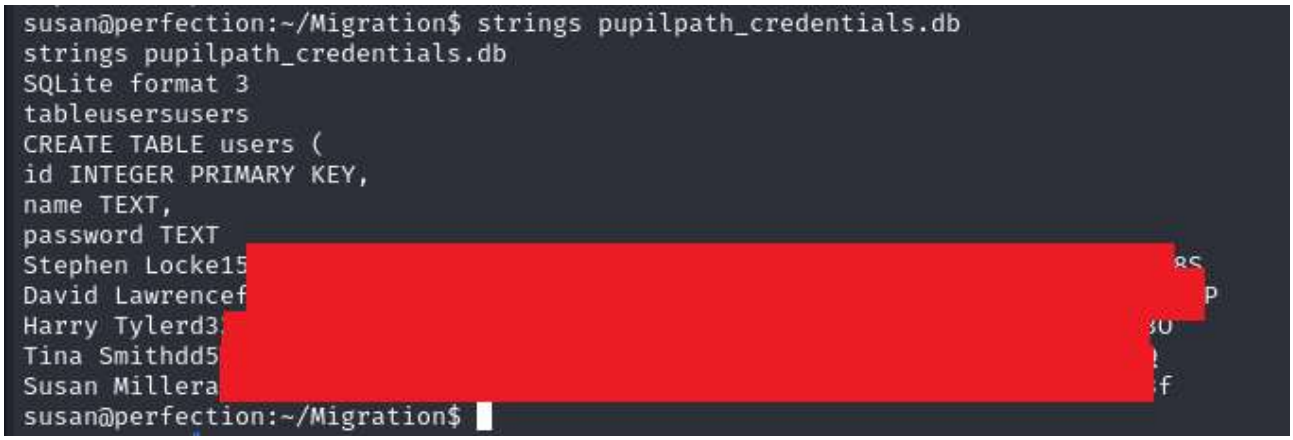

Figure 9 - Credentials file content

I tried very hard to crack Susan hash password, but I failed. So, I tried to crack other hashes too, but I failed too. I was sure this could be the correct path, but I miss some information. I started to search some other useful information. After I spent a lot of time, I found another interesting file:

Figure 10 - Password pattern

I was very relieved. With these new information I was able to crack the password:

Figure 11 - Password cracked

The command I used to crack the password is the same shown in the previous image without the ***–show*** option. At this point, I just needed to run ***sudo su*** command and retrieve the root flag:

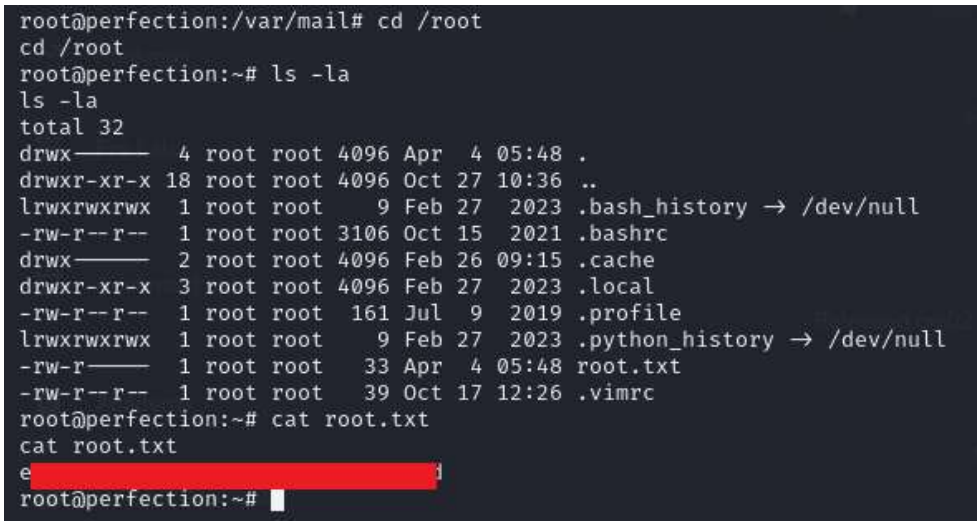

Figure 12 - Root flag