Defending Against Brute Force Attacks: Strategies and Prevention Techniques

KUKUTLA TEJONATH REDDY,
International Center for AI and Cyber Security Research and Innovations (CCRI),
Asia University, Taiwan, tejonath45@gmail.com

ABSTRACT

Brute force attack is the most recognized and common threat in this digital world. Brute force attack is one of the hacking methods which involves trying all the possibilities to crack the correct passwords or encrypted keys. Brute force attack is used by hackers to gain access and collect data from individual persons or an organization. Brute-force attacks are common cases that are getting harder to detect successfully on a network level due to increasing volume and encryption of network traffic and growing ubiquity of high-speed networks. Although research in this field has advanced considerably, there still remain classes of attacks that are undetectable. Since their no security measure can guarantee that an attacker will not succeed eventually, intrusion detection techniques should be applied to detect anomalous behavior early and minimize its impacts on network performance caused by the intruders. This article discusses what is a brute force attack, how brute force attack works, types of brute force attack, how to defend against brute force attack.

KEYWORDS: Brute Force Attack, Password Cracking, Unauthorized Access, Hacking Methods

I. INTRODUCTION

In this world of cybersecurity, brute force attack is one of the threats for an individual person or an organization. Brute force attack is one of the hacking methods where a hacker will try all the possible combinations and patterns until he cracks the correct password. Nowadays, they are focusing on cracking encryption keys, security tokens and other forms of authentications. The name "Brute force" comes from a hacker who will forcefully try a number of attempts to get access to user accounts. Hackers will use brute force attacks to gain unauthorized access to personal data or sensitive information of an individual or an organization. They will try a number of usernames and passwords to crack the password. Hackers will use brute force attacks for several purposes like identity theft, financial fraud, and for political or ideological motives. They will often use automated tools and botnets to launch brute force attacks. This article provides an overview of brute force attack, how brute force attack works, types of brute force attacks, how to mitigate brute force attack.

A. What is a Brute Force Attack?

Brute Force attack is a method that is used by hackers to get access to unauthorized information by trying every possible combination and pattern of passwords or encryption keys until they find the correct password or encryption key. Brute force attack is a trial-and-error approach.

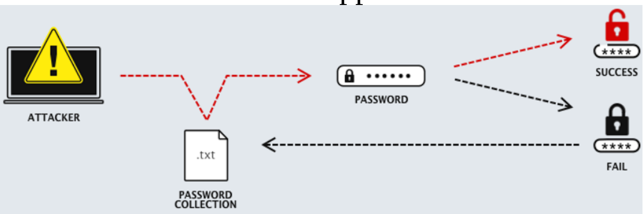


Fig.no:1 (how brute force attack works)

B. How Does a Brute Force Attack Work?

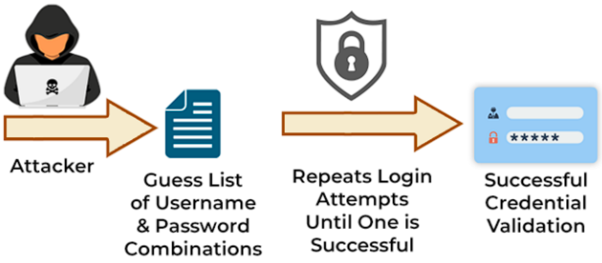

Attacker
Guess List of Username & Password Combinations
Repeats Login Attempts Until One is Successful
*****
Successful Credential Validation

Fig.no:2 (working of brute force attack)

Selecting the target: Attacker will select a specific target to attack such as a user account, website and encrypted files which ever they want to access

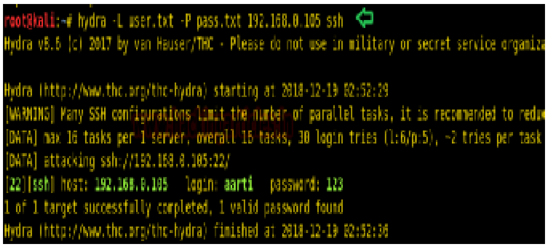
Generating Passwords: Hackers will start to create a list of all the possible passwords to try. List includes commonly used passwords, dictionary words, or a random combination of characters.

Automated Trial and Error: Using automated software or script, to try to check all the possible passwords in the list. This process will continue until attacker gets the password or all the combinations exhausted

Success or failure: If the attacker got the correct password from automated trial and error, they can gain access to the website or target machine and they can steal the sensitive information or financial data from that. If all the combinations are tried without success, the attack fails. The attacker will come up with a new combination of lists.

II. RELATED WORKS

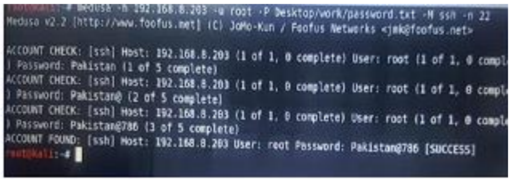
Brute Force is the most commonly used technique to crack server passwords. There are many methods to do brute force attacks like Hydra, Ncrack and Medusa. In these methods the attacks work by trying all possible combinations until correct passwords comes or all the possible combinations in list completed.



```
root@kali:~# hydra -L user.txt -P pass.txt 192.168.0.105 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organiza

Hydra (http://www.thc.org/thc-hydra) starting at 2018-12-19 02:52:29
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to redu
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:6/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.0.105:22/
[22][ssh] host: 192.168.0.105   login: aarti   password: 123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-12-19 02:52:36
```

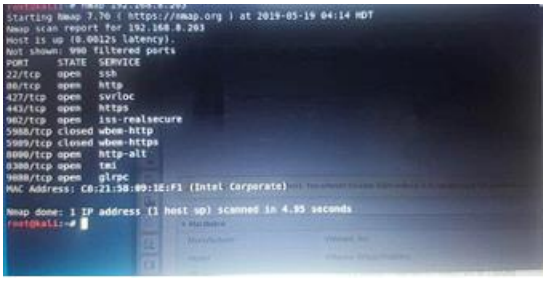
Fig.3: Brute force using Hydra



```
root@kali:~# medusa -h 192.168.8.203 -u root -P Desktop/work/password.txt -M ssh -n 22
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.8.203 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
) Password: Pakistan (1 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.8.203 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
) Password: Pakistan@ (2 of 5 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.8.203 (1 of 1, 0 complete) User: root (1 of 1, 0 compl
) Password: Pakistan@786 (3 of 5 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.8.203 User: root Password: Pakistan@786 [SUCCESS]
root@kali:~#
```

Fig.4: Brute force using Medusa



```
root@kali:~# nmap 192.168.8.203
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-19 04:14 MDT
Nmap scan report for 192.168.8.203
Host is up (0.0012s latency).
Not shown: 990 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
427/tcp   open   svrloc
443/tcp   open   https
902/tcp   open   iss-realsecure
5988/tcp  closed wbem-http
5989/tcp  closed wbem-https
8000/tcp  open   http-alt
8300/tcp  open   tmi
9080/tcp  open   glrpc
MAC Address: C8:21:58:09:1E:F1 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 4.95 seconds
root@kali:~#
```

Fig.5: Brute force using Ncrack

III. Types of Brute Force attack

Simple Brute Force Attack: This is a basic form of brute force attack. This attacker will try all the possible combinations of characters until one is found. It is a time-consuming method, but it will work effectively.

Dictionary Attacks: Dictionary attack is a one of the types of brute force attack it involves predefined list of common words in the victim life like common names, date of birth,"123456789", etc. using automated software's attacker will try all the dictionary list until the correct password found or tried all the dictionary list completes.

Credential Stuffing: In this type of brute force attack, cybercriminals will use automated software tools to try a large number of usernames and password combinations obtained from previous data. If users reuse passwords in multiple accounts, attackers can get access from various platforms.

Hybrid Brute Force Attacks: In this attack, attackers will combine dictionary attacks and simple brute force attacks to make them faster and more adaptable. In this, the attacker will use a permutations method to crack passwords.

Reverse Brute Force Attack: In this type of brute force attack in which an attacker will use common passwords for multiple usernames in an attempt to gain access.

SSH Brute Force: Attackers will target Secure Shell (SSH) servers, trying to gain access to system by guessing the SSH credentials

IV. Preventions

The good news is that with the right security measures we can secure our data or information from brute force attacks.

Strong Password Policies: Users need to create complex passwords for their systems or websites. The password needs to be mixed with uppercase and lowercase letters, numbers, and special characters. And we need to change our passwords regularly.

Multi-Factor Authentication (MFA): Multi-Factor Authentication will add an extra security layer for a website or several applications by providing multiple forms of identifications, such as a password and a verification code sent to their mobile device. Even if an attacker finds out passwords still, they need to give second factor code to gain access.

Regular Software Updates: We need to keep up-to-date our system or software to patch the vulnerabilities. By that we can escape from attackers. That patch will be a way to attack, so we need to cover up that patch by regular software updates.

Web Application Firewalls (WAFs): Web application firewalls will monitor and filter HTTP traffic between web applications and the internet. Web application firewalls will detect and mitigate brute force attacks by blocking malicious IP addresses.

Account Lockout Policies: We need to set-up account lockout policies for a certain number of failed login attempts. This will prevent us from attackers, from making multiple login attempts

Monitoring and Logging: We need to monitor login activities and we need to maintain detailed logs

V. CONCLUSIONS

In this ever-expanding digital world, Understanding and defending against brute force attacks has been important for both individuals and organizations. Brute force attack will remain a determined and important threat in cybersecurity. Brute force attacks are flexible and can target a wide range of target systems, websites, and email accounts. So, we need to educate and bring awareness to users about brute force attacks and about how to take precautions from this type of attack. In this article we explained about what is brute force attack, how brute force attack, types of brute force attack, and preventions of brute force attack.

VI. References

[1] S. Zhang, X. Xie and Y. Xu, "A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity," in IEEE Access, vol. 8, pp. 128250-128263, 2020

[2] Grover, Varsha and Gagandeep, An Efficient Brute Force Attack Handling Techniques for Server Virtualization (March 30, 2020). Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020

[3] Verma, R., Dhanda, N., Nagar, V. (2022). Enhancing Security with In-Depth Analysis of Brute-Force Attack on Secure Hashing Algorithms. In: Kaiser, M.S., Bandyopadhyay, A., Ray, K., Singh, R., Nagar, V. (eds) Proceedings of Trends in Electronics and Health Informatics. Lecture Notes in Networks and Systems, vol 376. Springer, Singapore.

[4] Wanjau, Stephen & Wambugu, Geoffrey & Kamau, Gabriel. (2021). SSH-Brute Force Attack Detection Model based on Deep Learning. International Journal of Computer Applications

Technology and Research. 10. 42-50. 10.7753/IJCATR1001.1008.

[5] Hofstede, R., Jonker, M., Sperotto, A. et al. Flow-Based Web Application Brute-Force Attack and Compromise Detection. J Netw Syst Manage 25, 735–758 (2017).

[6] T. Gautam and A. Jain, "Analysis of brute force attack using TG — Dataset," 2015 SAI Intelligent Systems Conference (IntelliSys), London, UK, 2015, pp. 984-988, doi: 10.1109/IntelliSys.2015.7361263.

[7] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya and R. Zuech, "Machine Learning for Detecting Brute Force Attacks at the Network Level," 2014 IEEE International Conference on Bioinformatics and Bioengineering, Boca Raton, FL, USA, 2014, pp. 379-385, doi: 10.1109/BIBE.2014.73.

[8]Ren, P., Xiao, Y.,et al. (2021). A survey of deep active learning. *ACM computing surveys (CSUR)*, *54*(9), 1-40.

[9]Cvitić, I., et al.(2021). Boosting-based DDoS detection in internet of things systems. *IEEE Internet of Things Journal*, *9*(3), 2109-2123.

[10]Lv, Let al.. (2022). An edge-AI based forecasting approach for improving smart microgrid efficiency. *IEEE Transactions on Industrial Informatics*.

[11]Stergiou, C. L.,et al. (2021). InFeMo: flexible big data management through a federated cloud system. *ACM Transactions on Internet Technology (TOIT)*, *22*(2), 1-22.