Efficient Brute Force Attack Handling: Server Virtualization

Lovely Anna John
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
lovelyannajohn2021@mca.ajce.in

Dr. Juby Mathew
Department of Computer Applications
Amal Jyothi College of Engineering
Kanjirappally, India
jubymathew@amaljyothi.ac.in

Abstract- **Security of server in all contexts is dominating in every field of computing, while working on the servers numerous threats and attacks like cracking of passwords, knowing the root of machine, giving privilege to unauthorized users are common attacks that can harm the system and take access of servers. The most prevalent commands like Hydra and Medusa, Ncrack are there which can be used for cracking the passwords of server and unauthorized users can take the access of serverby applying these commands. In this paper we will consider brute force attack and its tools with its implementation and prevention ways or techniques to avoid these types of attack**.

Keywords: Cracking Software Tools, Brute-Force, Cracking Passwords, Password Cracking

I. INTRODUCTION

Sever security is a trending topic in today's world. Every year millions of dollars are spent to achieve the security and hundreds of researches are currently underway to solve the problems of security. Despite working on the well-defined security mechanisms there exist many loopholes in this like cracking of password, unauthorized access of server. For cracking passwords of server Brute force method is one of the most common used technique. There are many tools associated with brute force such as Hydra ,N crack and Medusa This attacks work by testing every possible combination that could be used as the password by the user and then testing it to see if it is the correct password. To find if the password is correct or not it further checks for any errors in the response from the server. These tools are used as bruteforce SSH. Hydra, a password detection tool (cracking) which can be used in many situations that includes authentication-based forms which are used in web applications. On the other hand Medusa is a speedy, parallel, and modular, login brute force that is used to support as many services which allow remote authentication as possible. While N crack is a tool that is used as a Brute Force tool to target small and large networks. WordPress is an open source platform for web development. By using this platform 30% of the websites are designed. It is in fact one of the most popular target of hackers because of its fame. In this paper we will study following tools in detail and techniques to overcome from these attacks[2][3].

II. BRUTE FORCE ATTACK

Brute Force Attack is most conventional attack that workagainst web applications. To acquire access of user accounts by trying to guess the passwords of the single user or group of users is the core aim of brute force attack. Web application should be robust enough to work against on this attack, unless attacker will get the privilege of the system. Brute Force attacks can be applied in numerous ways. Length of the password known by attacker can cause the brute force attack, combination of numbers, letters and symbols can be applied unless a suitable match is found. However, this is a slow process, especially as the length of the password increases. One of the way of the brute force attack is if illegitimate user is aware of username which is generally root for a web application. Further it can based on the complexity of the password like if a weak password is used then it also becomes victim for attack[3][4].

Tools are the techniques or methods that help to crack the passwords. Brute force attacks are considered to test all the feasible combinations for cracking the passwords of server. Following are the tools that we will apply to crack the password named as Hydra, Medusa and Ncrack[3].

A. Hydra Tool for Brute Force

Hydra is one of the best login cracker tool that further supports various protocols for attack. It is fast and flexible method to add new modules. There are various protocols that support to Hydra tools which are Cisco AAA, Ciscoauth, Cisco enable , CSV, FTP, HTTP(S)-FORMGET, HTTP(S)- FORM-POST, IMAP, IRC,MY-SQL, NNTP, POP3, SMTP,
Telnet etc.[3].
Following are the Flags used for Hydra

DOI: 10.5281/zenodo.5090544
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

Flag	Description
-t	Number of parallel Threads
-l	Single Username
-L	Provide wordlist for users
-P	Provide wordlist for password
-p	Single Password
http-post—form	To use HTTP post Request
https-form-form	To use HTTPs post Request
F=<string>	A string containing failure message

B. Medusa Tool for Brute Force

Medusa is a Parallel, Modular and Speedy method of brute-forcewhich isused for remote authentication, Following are applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols areAFP,CVS,FTP,HTTP,IMAP,MSSQL,NetWareNCP ,NNTP,POP3,REXEC,SNMP,SSHv2,WebForm.

Flags used for Medusa

Flag	Description
-h [TARGET]	Target hostname or IP address
-u [TARGET]	Target username
-U [FILE]	Read target usernames from a wordlist file
-p [TARGET]	Target Password
-P [TARGET]	Read target passwords from a wordlist file
-O [FILE]	Write the log in file
-M [TEXT]	Module to execute (without .mod extension.)
-n[NUM]	Use for non-default TCP port number

C. Ncrack Tool for Brute Force

Ncrack is a cracking tool that is highly recommended for high-speed network authentication. It was majorly designed for the companies to secure networks by proactively testing for weak passwords. It followed a design technique which was based on modularization related to Nmap and a dynamic engine with friendly interface which infact gives full control of operations of network. Some of the protocols which support include SSH,RDPRDP, FTP, Telnet, HTTP(S), Wordpress, POP3(S), IMAP, CVS, SMB, VNC, SIP, Redis, PostgreSQL, MQTT, MySQL, MSSQL, MongoDB, Cassandra, WinRM, OWA, and DICOM. Following are the Flags used for Ncrack.

Flags used for Medusa

Flag	Description
-p [SERVICE-LIST]	Services will be applied to all non-standard notation hosts
-m [SERVICE][OPTIONS]	Options will be applied to all services of this type
-g [OPTIONS]	Options will be applied to every service globally
-U [FILENAME]	User Name File
-P [FILENAME]	Password File
-oN/-oX [FILE]	Output scan in normal and XML formatrespectively, to the given filename.
-oA [BASENAME]	Output in the two major formats at once
--resume [FILE]	Continue previously saved session
--save [FILE]	Save restoration file with specific filename

III EXPERIMENTAL SETUP AND RESULT OF ATTACK

Passwords and username are the weakest link in the system. It is very important for security assessments to test weak passwords. In this Paper we focus on some tools that facilitate remote service and brute-forcing. One type of password in brute-forcing is to temper attack against the password hash, by applying tools such as Hashcat, that is a powerful tool that can crack encrypted password hashes on a local system. Hydra, Medusa and Ncrack will be implemented in this paper

A. Installation of Hydra, Medusa and Ncrack

Hydra, Medusa and Ncrack are best password cracking tools. Following are the steps for Installation of all three tools was straight forward on Ubuntu Linux. There are standard methods to compile an application from source[4].

B. Brute force using Hydra

Hydra is one of the popular brute forcing tool through this password can be easily cracked of remote machine. To download Hydra in Kali Linux machine, type below command: hydra -L user.txt -P pass.txt 192.168.43.100ssh

Fig 1 : Hydra Attack

C. Brute force using Medusa –

Medusa is another popular brute forcing tool through which you can easily crack the SSH password of any remote machine. To download Medusa in your Kali Linux machine, type below command [5][19]

DOI: 10.5281/zenodo.5090544
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

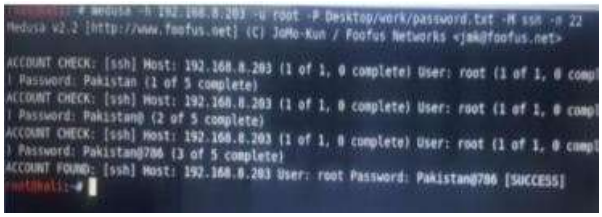

Fig 2 : Medusa Attack

C. Brute force using Ncrack-

Ncrack is little bit harder than Hydra but is more powerful amongst all other tools. To download Ncrack, the command is

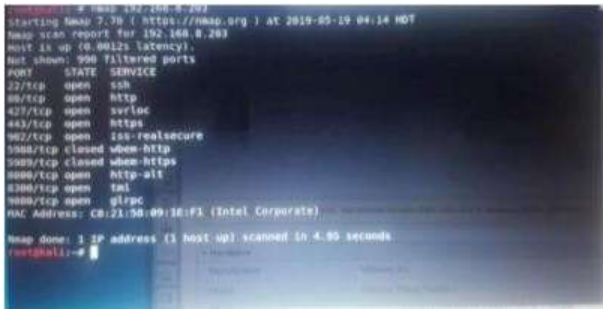

Fig 3: Ncrack Attack

IV. EXPERMENTAL SETUP AND RESULTS TO PREVENT THE BRUTE FORCE ATTACK

There are numerous techniques which can prevent brute force attack like keeping passwords complexity strong, applying captcha codes and failed login attempt. In our work we will implement the above methods to prevent the common brute force attack and will be achieved by applying tools such as hydra medusa and ncrack. In Brute force attack if attacker is aware of default password which is root only then password can also be easily cracked by him. To avoid such attack username must be changed and it should be chosen a stronger one and by this hacking of the password can be avoided. Also if a weak password is chosen the system will not accept the same. So a stronger password can prevent brute force attack. Another feature which a VMware Exsi has a way be to be automatically logged out user needs to be login again to work on server. This will also be helpful to prevent brute force attack[21].

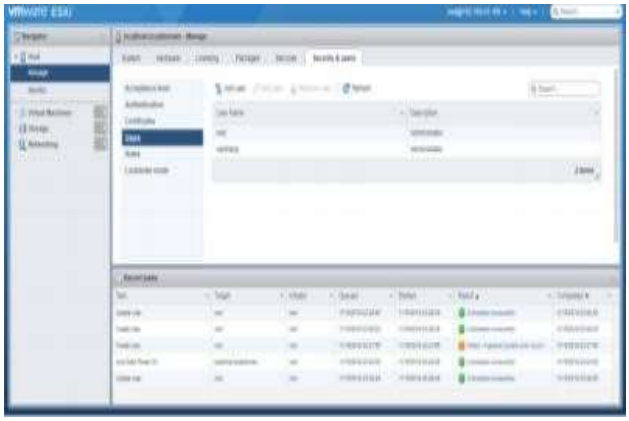

Fig 4: Changing Username

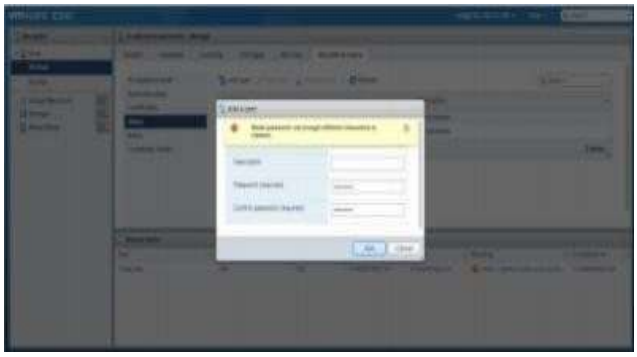

Fig 5: Snapshot using weak password

To enable each of these sections to uncomment header [ssh] and modify the enabled value into "true" as shown in the below image, and then save the jail.local file and restart the fail2ban service:
[ssh]

enabled = true

service fail2ban restart

Following is the code to implement prevention of brute force

[SSH]

enabled = true port = ssh filter = sshd

logpath =var/log/auth.log maxretry=6

Let's test host machine against brute force attack for ssh login once again:

hydra -L user.txt -P pass.txt 192.168.43.100 ssh

DOI: 10.5281/zenodo.5090544
ISBN:978-93-5426-386-6@2021 *MCA, Amal Jyothi College of Engineering Kanjirappally, Kottayam*

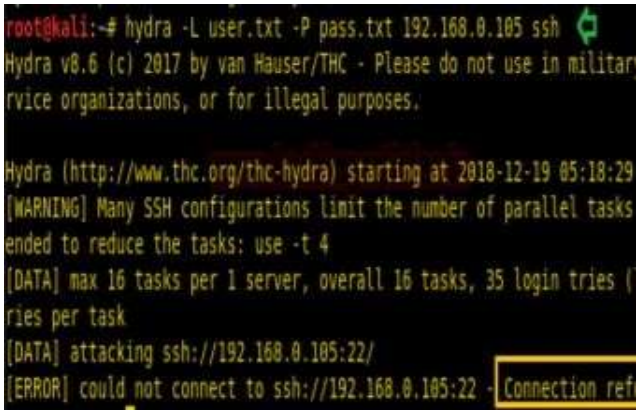

Fig 6 Prevent Attack

V. CONCLUSION AND FUTURE WORK

A brute force attack is very effective way to take access of server by cracking passwords. It tries various combinations of usernames and passwords again and again to get the actual password. A Brute-force attack is dangerous for system. More than 30 percent website are developed using WordPress platform due to its popularity. WordPress is an open source and famous platform. It is a target of hackers. These attacks include three tools such as Hydra, Medusa and Ncrack, by applying these commands hacker can take access of system and privileges. There are following methods and techniques such as password complexity, captcha and limit login access etc. to avoid this brute force attack. These methods are helpful to overcome the attacks which occur due to brute force. Although these attacks are defendable but still they are prone and found to be vulnerable with enormous growth of security loop holes.

VI. REFERENCES

1. L. Bošnjak,J.SrešandB.Brumen: Brute-force and dictionary attack on hashed real-world passwords, International Convention on Information and Communication Technology(2018), Electronics and Microelectronics

2. Mohammed et al: Brute Force Attack Detection and Prevention using Wireshark Analysis(2017), International Journal of Engineering Science and Research Technology ,vol. 6, pp 26-37

3. G. SunithaRekha.: A Study on Virtualization and Virtual Machines (2018). International Journal of Engineering Science Invention (IJESI) pp 51– 55.

4. Pedro A. R. S. Costa et. al : Medusa: An Efficient Cloud Fault-Tolerant Map Reduce (2015), INESC-ID, Instituto Superior Tecnico, Universidade de Lisboa, Portugal ,vol 1

5. Priyanka Mod, Prof. Mayank Bhatt : A Survey on Dynamic Resource Allocation Technique in Cloud Environment - A Survey (2014), International Journal of Advanced Research in Computer Engineering and Technology, vol.3 pp 7815-7818

6. Durairaj.M, Kannan.P : A Study in Virtualization Techniques and Challenges In Cloud Computing (2014) , International Journal of Scientific and Technology Research, vol. 3, pp 147-151

7. BhuvneshProhit, Tushar Sharma, ShreyanshJarged : Virtualization Techniques in Cloud Computing (2016), Imperial Journal of Inter disciplinary Research (IJIR), vol 2, pp 1476-1479

8. Tomas Frtala and Katarina Zokova : Virualization: An Answer to Secure Development of Online Experiments (2014) , The International Federation of Automatic Control, pp 9738-9743

9. Amit K Sharma, Priyanka Soni. Mobile Cloud Computing(2013), International Journal of Innovations in Engineering and Technology (IJIET) , pp 24-27

10. Nitesh Kaushik, Gaurav, Jatinder Kumar. A Literature Survey on Mobile Cloud Computing (2014): Open Issues and Future Directions , International Journal of Engineering and Computer Science, vol. 3, pp 6165-6171

11. Jon Oberheide, Kaushik VeeraraghavanEvam Cooke, Jason Flinn, FarnamJohanian. Virtualized In- Cloud Security Service for Mobile Devices (2011), Electrical Engineering and Computer Science Department, pp 1-5

12. Nirorshinie Fernando, Seng W. Loke, WennyRahayu. Mobile cloud computing: A survey (2013), Department of Computer Science and Computer Engineering. La Trabe University, Austraila , pp 84-106

13. Nirbhay K Chaubey, Darshan M Tank. Security, Privacy and Challenges in Mobile Cloud Computing(MCC) - A Critical Study and Comparison (2016),, International Journal of Innovative Research in Computer and Communication Engineering pp 1-5

14. Rabi Prasad Padhy, ManasRanjanPatra , Suresh Chandra Satapathy . Cloud Computing: Security Issues and Research Challenges (2011), International Journal of Computer Science and Information Technology & Security (IJCSITS). pp. 136- 146

15. Yogesh Ghorpade, TajuddinBennur, Dr. H. S. Acharya and Dr. R. Kamatchi : Server Virtualization Implementation: An Experimental Study for Cost Effective and Green Computing Approach (2015), International Journal of Computer Science Trends and Technology (IJCST), pp 109-123

16. Chuan-Fu Chuang and Shiuann-Shuoh Chen.: To Implement Server Virtualization and Consolidation Using 2P-Cloud Architecture (2017), Journal of Applied Science and Engineering. pp 121-130

17. A. Tayab, Junaid, W. Taliband and M. Fuzai.: Security Challenges of Virtualization in Cloud Technical Journal(2015) , University of Engineering and Technology (UET) Taxila, Pakistan pp111-116

18. Muhammad Arif and Haroon Shakeel : Virtualization Security: Analysis and Open Challenges (2015), International Journal of Hybrid Information Technology, vol. 8 ,pp 237-247

19. Nadiah M. Almutairy, Khalil H. A. Al-Shqeerat and Husam Ahmed Al Hamad.: A Taxonomy of Virtualization Security Issues in Cloud Computing Environments (2019), Indian journal of science and technology,vol 12

20. Amazon Web Services Inc, "Amazon EMR." http://aws.amazon.com/ elasticmapreduce