**Brute Force Attack on Linux Servers**

================================ **Brute Force Attack Troubleshooting** ================================

1. **Verify the logs with following command**

# cat /var/log/auth.log | grep "Failed password"

# cat /var/log/secure | grep "Failed password"

# journalctl -u sshd | grep "Failed password"

RHEL-6/CentOS-6 ----> /var/log/secure

RHEL-7/CentOS-7 ----> /var/log/auth.log

2. **Once the IP is located find the details of IP as**

# whois xxx.xxx.xxx.xxx

This will give entire information about the IP

3. If you don’t have access for VM use run command option to find the "Failed password" logs

run same commands

**==================security measurements on Linux Machine to avoid Brute Force attack ==================**

1. Check the port and change it to custom port from 22

2. change the username and password of VM

3. Harden NSG level Access for VM

4. MaxAuthTries variable in sshd\_config file helps you to limit login attempts

5. The Bruit Force attack is the mechanism of trying continuous random username password combination, we can restrict the access to VM by using the Pluggable Authentication Module(PAM)

6. In order to keep a close eye on your incoming SSH connections is to set up a quick script to send an alert once someone is logged in as root or normal user via SSH. Script will be as follows needs to be appended in /root/.bashrc

echo 'ALERT - Root Shell Access (ServerName) on:' `date` `who` | mail -s "Alert: Root Access from `who | cut -d'(' -f2 | cut -d')' -f1`" your@email.com

For this script to be working need to have mailx package installed

# apt-get install mailx

7. Keeping SSH package updated is the basic rule to improvise the SSH security, you can use following command to update package

apt-get update openssh-server

======================================== **Important Links** =========================================

https://securitytrails.com/blog/mitigating-ssh-based-attacks-top-15-best-security-practices

https://www.tecmint.com/lock-user-accounts-after-failed-login-attempts-in-linux/

https://www.tecmint.com/use-pam\_tally2-to-lock-and-unlock-ssh-failed-login-attempts/

http://www.tuxfixer.com/detect-ssh-brute-force-attack-locate-attacker-isp/