* **Brute Force Attack Troubleshooting**

* **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"

* **SSH Log Verification**
* RHEL-6/CentOS-6 ----> /var/log/secure
* RHEL-7/CentOS-7 ----> /var/log/auth.log

* **Once the IP is located find the details of IP as**
* whois xxx.xxx.xxx.xxx (This will give entire information about the IP)

* If you don't have access for VM use run command option to find the "**Failed password**" logs

run same commands mentioned above

* Monitor network flow like outgoing data for certain time of period, which will give idea whether any script placed for sending packets to outside network to get captured
* Check **.bashrc** file as executables can be placed at the bottom of this file also

* Check the cronjob has been placed for making automated attacks from same server to Application hosted in same server

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

* Check the port and change it to custom port from 22
* change the username and password of VM
* Harden NSG level Access for VM
* MaxAuthTries variable in sshd\_config file help you to limit login attempts
* 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)
* 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*

* 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*

* Stopping and Starting machine in such cases after making above changes is a kind of solution which will stop the outgoing packets which will remove the possibility of packet capture eventually IP capturing

* **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/>
* <https://azure.microsoft.com/en-us/blog/how-azure-security-center-helps-detect-attacks-against-your-linux-machines>
* <https://azure.microsoft.com/en-in/blog/detecting-script-based-attacks-on-linux/>