SSH Advanced

Use strong passwords or, preferably, SSH key-based authentication: SSH key pairs provide a more secure method of authentication compared to passwords

Keep SSH software up to date: Regularly update your SSH client and server software to ensure you have the latest security patches and improvements.

Disable SSH root login: It's generally recommended to disable direct root login via SSH. Instead, log in as a regular user and use sudo or su to escalate privileges when necessary. This adds an extra layer of security by reducing the potential attack surface.

Limit SSH access through firewall rules: Configure your firewall to allow SSH connections only from trusted IP addresses or networks.

Use strong encryption algorithms: Ensure that your SSH configuration uses strong encryption algorithms for secure data transmission. The configuration file is typically located at /etc/ssh/sshd_config on the server.

Implement two-factor authentication (2FA): Consider enabling two-factor authentication for SSH to add an extra layer of security. This involves requiring an additional verification method, such as a code from a mobile app or a physical token, in addition to the SSH key or password.

Monitor SSH logs: Regularly review SSH logs for any suspicious activity or failed login attempts. Unusual or repeated failed login attempts may indicate a brute-force or unauthorized access attempt.

Generate ssh keys:

```
ssh-keygen -t rsa -b 4096 -C "devsecops" -f
~/devsecops
```

Login via keys using ssh:

```
ssh -i ./devsecops jenkins@ip
```

Configuring sshd_config file:

Disable root login: PermitRootLogin no

Whitelist user login: AllowUsers username1 username2

Use SSH key-based authentication: PubkeyAuthentication yes

Set stronger encryption algorithms: Ciphers aes256-ctr
MACs hmac-sha2-256

Set a non-standard SSH port: Port 2222

Enable two-factor authentication (2FA): ChallengeResponseAuthentication yes
UsePAM yes

Set idle timeout: ClientAliveInterval 300
ClientAliveCountMax 0

Restart after all these changes are done : sudo service ssh restart