20 SSH Secure Shell Linux Interview Questions and Answers

BY [ARK](https://arkit.co.in/author/admin/) · PUBLISHED DECEMBER 17, 2016 · UPDATED DECEMBER 17, 2016

In most of the Interviews it’s an common questions they ask is about SSH (Secure Shell) because in regular day to day tasks they required to use SSH. Usage of SSH protocol is high then employee should know about SSH before they are going to use that’s why interviewer will ask at least one question from these 20 SSH Secure Shell Linux Interview Questions and Answers.

20 SSH Secure Shell Linux Interview Questions and Answers

**Q1: What is SSH protocol.?**

**Ans:** SSH, or secure shell, is a secure protocol and the most common way of safely administering remote servers. Because it encrypt data while transferring from one host to another host throughout network.

**Q2: What is the default port for SSH and configuration file path.?**

**Ans:** Default port number 22. Configuration file path /etc/ssh/sshd\_config

**Q3: What are different data manipulation (Encryption) techniques supported by SSH ..?**

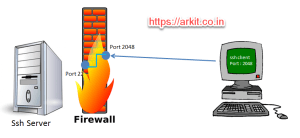
**Ans:** SSH supports Symmetric and Asymmetric encryption methods

**Q4: How to change default SSH port number .?**

**Ans:** We can change the Default port by editing it’s configuration file /etc/ssh/sshd\_config & change Port 22 to other port number. After change restart sshd service to effect changes. If your firewall and SELinux is enabled then write the rule in firewall for new port number otherwise clients can’t connect.

**Q5: How does port forwarding works in SSH ..?**

**Ans:** Client is going to connect using different port number ( in this case 2048 ) other than default, but server ssh service will respond on default port. We have to use ssh -p 2048 from client machine.

[](https://i0.wp.com/arkit.co.in/wp-content/uploads/2016/12/ssh-port-forwading.png?ssl=1)

*ssh server port forwarding using firewall redirection*

**Q6: How to disable root login for ssh server.?**

**Ans:** Disabling the root login for ssh is very secure way. we can do that by editing ssh configuration file/etc/ssh/sshd\_config then change ‘PermitrootLogin no‘

#LoginGraceTime 2m

PermitRootLogin no

#StrictModes yes

#MaxAuthTries 6

#MaxSessions 10

**Q7: How to Enable only Key based authentication..?**

**Ans:** This feature provides more/high security because any user can’t login without SSH key.

Note: We have to disable user login to SSH.

#RSAAuthentication yes

#PubkeyAuthentication yes

**Q8: Is it possible to Login to remote SSH server without password.?**

Ans: Yes, we can do by setting up Key based authentication (password less authentication setup)

**Q9: What is different between Telnet & SSH.?**

**Telnet                                                                      SSH**

1. Data goes on network as plan text.                Data will be encrypted using key pair (public key and private key)

2. Default port 23                                                   Default Port 22

3. Bandwidth usage is less compare to SSH      Bandwidth is high compared to telnet 20 ssh

**Q10. How to Limit SSH access to specific subnet.?**

Limiting SSH access to specific subnet will gives more secure environment, other than given subnet network can’t access SSH server. Edit sshd\_config file and add subnet as mentioned 20 ssh

AddressFamily 192.168.4.0/24

**Q11: How to restrict SSH server to use only protocol version 2 Or 1..?**

Edit default configuration file and un-comment below shown line and restart service

# The default requires explicit activation of protocol 1

#Protocol 2

**Q12: What do you mean by SSH cipher.? Tell me different types of ciphers..?**

Cipher is an algorithm to perform encryption and decryption.

Types of cipher supported by SSH are

1. 3des
2. blowfish
3. des

**Q13: How do you access GUI using SSH connection ..?**

SSH will also support of transferring X11 forwarding, we have to use options calle -XY to open server GUI app from client.

**Q14: What the best procedure to troubleshoot SSH connection error .?**

To Enable Debugging in ssh command use -v option which gives more appropriate and deep analysis. Secure Shell Linux Interview Questions

**Q15: How to Check ssh version .?**

[root@ArkIT-Serv ~]# ssh -V

OpenSSH\_6.6.1p1, OpenSSL 1.0.1e-fips 11 Feb 2013

**Q16: How to Connect to remote IPv6 enabled server ..?**

It’s so simple to connect ssh using IPv6 version

ssh -6 root@remoteserver.arkit.co.in

**Q17: What is the procedure to log SSH errors to separate file .?**

Using option -E log\_file it will send an standard errors to specified file

**Q18: How many types of Key types SSH supports..?**

* RSA
* DSA
* ECDSA
* ED25519

**Q19: Where SSH will store its trusted ssh client keys .?**

By default whenever you trying to connect to remote SSH host for the first time it will ask you to confirm Yes/No as soon as we say yes, it will copy public key pair to ./ssh/known\_hosts

**Q20: What is the role of authorized\_keys file .?**

Authorized\_keys file stores all client keys to provide password less authentication. Secure Shell Linux Interview Questions