blackmoreops.com

Kali Linux remote SSH – How to configure openSSH server

3 minutes

Step 6: Change SSH server port for extra safety

As a last step and just to be sure, you should also change SSH `port` from `22` to something else. (any port between `10000-64000` is okay)

Make a backup of existing SSH config file.

```
root@kali:/etc/ssh# cp /etc/ssh/sshd_config
/etc/ssh/sshd_config_backup
```

Edit the `SSH_Config` file.

```
root@kali:/etc/ssh#  vi /etc/ssh/sshd_config
```

Look for the following line:

```
    #Port 22
```

Change the line so it looks like this:

```
    Port 10101
```

Restart `OpenSSH` server

```
root@kali:/etc/ssh#  service ssh restart
```

Next time you SSH, you use the following command:

```
root@kali:~#  ssh username@myhostnaname.com -p
10101
```

Where

1. username@myhostnaname.com = Username and Hostname where hostname can be an IP or FQDN.
2. -p = Port
3. 10101 = Destination Port

Conclusion:

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model.

The standard TCP port 22 has been assigned for contacting SSH servers. If you scan for this port using NMAP, you will see many servers has it open to the world and you can try to bruteforce it and gain access.

An SSH client program is typically used for establishing connections to an SSH daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, most distributions of GNU/Linux, OpenBSD, FreeBSD, NetBSD, Solaris and OpenVMS. Notably, Windows is one of the few modern desktop/server OSs that does not include SSH by default. Some common SSH clients includes

1. PuTTY
2. Cygwin

3. WinSCP

and they all provide similar file management (synchronization, copy, remote delete) capability using PuTTY as a back-end.

Both WinSCP and PuTTY are available packaged to run directly off of a USB drive, without requiring installation on the client machine. Setting up a SSH server in Windows typically involves installation (e.g. via installing Cygwin, or by installing a stripped down version of Cygwin with the SSH server.

SSH is important in cloud computing to solve connectivity problems, avoiding the security issues of exposing a cloud-based virtual machine directly on the Internet. An SSH tunnel can provide a secure path over the Internet, through a firewall to a virtual machine.

Thanks for reading. Please share.

Pages: 1 2 3