CHEAT SHEET
SSH - common commands and secure config

BlowStack

SSH connections

connects to a server (default port 22)
$ ssh user@server

uses a specific port declared in sshd_config
$ ssh user@server -p other_port

runs a script on a remote server
$ ssh user@server script_to_run

compresses and downloads from a remote server
$ ssh user@server "tar cvzf - ~/source" > output.tgz

specifies other ssh key for connection
$ ssh -i ~/.ssh/specific_ssh_fkey

SSH service

starts ssh service
$ (sudo) service ssh start

checks ssh service status
$ (sudo) service ssh status

stops ssh service
$ (sudo) service ssh stop

restarts ssh service
$ (sudo) service ssh restart

SCP (Secure Copy)

copies a file from a remote server to a local machine
$ scp user@server:/directory/file.ext local_destination/

copies a file between two servers
$ scp user@server:/dir/file.ext user@server:/dir

copies a file from a local machine to a remote server
$ scp local_destination/file.ext user@server:/directory

uses a specific port declared for SHH in sshd_config
$ scp -P port

coppies recursive a whole folder
$ scp -r user@server:/directory local_destination/

copies all files from a folder
$ scp user@server:/directory/* local_destination/

copies all files from a server folder to the current folder
$ scp user@server:/directory/* .

compresses data on network using gzip
$ scp -C

prints verbose info about the current transfer
$ scp -v

Full articles about cyber security at
https://blowstack.com/blog/cyber-security

SSH keys

generates a new ssh key
$ ssh-keygen -t rsa -b 4096

sends the key to the server
$ ssh-copy-id user@server

converts ids_rsa into ppk
$ puttygen current_key -o keyname.ppk

SSH config

opens config file (usual location)
$ sudo nano /etc/ssh/sshd_config

changes default SSH port (22)
Port 9809

disables root login
PermitRootLogin no

restricts access to specifucusers
AllowUsers user1, user2

enables login through ssh key
PubkeyAuthentication yes

disables login through password
PasswordAuthentication no

disables usage of files .rhosts and .shosts
IgnoreRhosts yes

disables a less secure type of login
HostbasedAuthentication no

number of unauthenticated connections
before dropping
MaxStartups 10:30:100

no. of failed tries before the servers stops
accepting new tries
MaxAuthTries 3

max current ssh sessions
MaxSessions 1

disables interactive password authentication
ChallengeResponseAuthentication no

no empty password allowed
PermitEmptyPasswords no

disables Rhost authtentication
RhostsAuthentication no

disables port forwarding (blocks i.e MySQL Workbench)
AllowTcpForwarding no
X11Forwarding no

prints much more info about SSH connections
LogLevel VERBOSE

Author: Piotr Golon, piotr.golon@blowstack.com, https://blowstack.com

Amazing Apps