1 SSH CheatSheet Tools

- PDF Link: cheatsheet-ssh-A4.pdf
- Blog URL: `https://cheatsheet.dennyzhang.com/cheatsheet-ssh-A4`
- Category: tools

File me Issues or star this repo.
See more CheatSheets from Denny: #denny-cheatsheets

1.1 ssh general

Name	Summary
run ssh command by muting host key check	`ssh -o StrictHostKeyChecking=no root@192.168.75.109 date`
ssh tunnel	`ssh -N -p 22 -i <ssh-keyfile> -f root@172.17.0.8 -L *:18085:localhost`
ssh agent load key	`exec ssh-agent bash && ssh-keygen`, `ssh-add`
generate a new key pair	`ssh-keygen`, `ssh-keygen -C "your_email@example.com" -t rsa`
generate a new key pair without interaction	`ssh-keygen -t rsa -f /tmp/sshkey -N "" -q`
fail2ban	protect SSH server from brute force attacks

1.2 advanced ssh

Name	Summary
Diff local file with remote ssh file	`diff local_file.txt <(ssh user@remote_host 'cat remote_file.txt')`
Diff two remote ssh files	`diff <(ssh user@remote_host 'cat remote_file.txt') <(ssh user2@remote_host2 'c`

1.3 ssh security

Name	Summary
Disable ssh by password	`sed -i 's/PasswordAuthentication yes/PasswordAuthentication no/g' /etc/s`
Disable root login	`sed -i 's/^PermitRootLogin yes/#PermitRootLogin yes/' /etc/ssh/sshd_conf`
Enable/Disable SSH Host Key Checking	`StrictHostKeyChecking yes` change ~/.ssh/config
Add passphrase protection to ssh keyfile	`ssh-keygen -p -f id_rsa` link: Manage SSH Key File With Passphrase

1.4 scp

Name	Summary
Download remote folder	`scp -r -i <ssh-keyfile> ec2-user@<ssh-host>:/home/letsencrypt-20180825 ./`

1.5 parse ssh log

Name	Command
ssh down	`grep -R "ssh.*Received signal 15" /var/log/auth.log`
ssh up	`grep -R "sshd.*Server listening" /var/log/auth.log`
ssh failed login	`grep -R "sshd.*Failed password for invalid user" /var/log/auth.log`
ssh break-in attemp	`grep -R "sshd.*POSSIBLE BREAK-IN ATTEMPT!" /var/log/auth.log`
ssh port scap	`grep -R "sshd.*Bad protocol version identification" /var/log/auth.log`
ssh login by public key	`grep -R "sshd.*Accepted publickey for" /var/log/auth.log`
ssh login by password	`grep -R "sshd.*Accepted password for" /var/log/auth.log`
ssh logout event	`grep -R "sshd.*pam_unix(sshd:session):  session closed for" /var/log/auth.log`

1.6 Common Config

- Inject ssh public key

```
echo "ssh-rsa AAA...0r contact@dennyzhang.com" >>  ~/.ssh/authorized_keys
```

- Define ssh alias

```
Host sandbox
     HostName 192.168.50.10
     StrictHostKeyChecking no
     User root

Host 192.168.1.*
   StrictHostKeyChecking no
   Port 32882
   UserKnownHostsFile=/dev/null
   IdentityFile ~/.ssh/id_rsa
```

- Turn off host key checking for all hosts

```
# In ~/.ssh/config or /etc/ssh/ssh_config

Host *
    StrictHostKeyChecking no
```

- Use expect to run ssh command with credential auto input

```
#!/usr/bin/expect
set timeout 20
set command "cat /etc/hosts"
set user "vagrant"
set password "vagrant"
set ip "192.168.50.10"
spawn ssh -o stricthostkeychecking=no $user@$ip "$command"
expect "*password:*"
send "$password\r"
expect eof;
```

- ssh reverse tunnel

```
# https://www.howtoforge.com/reverse-ssh-tunneling

autossh -M 40000 -p 2702 -i /home/denny/al -fN \
    -o "PubkeyAuthentication=yes" \
    -o "StrictHostKeyChecking=false" -o "PasswordAuthentication=no" \
    -o "ServerAliveInterval 60" -o "ServerAliveCountMax 3" \
    -R 123.57.240.189:29995:localhost:22 root@123.57.240.189
```

1.7 More Resources