How-Tos

Escape Characters: Port Forwarding in Existing Session

```
<ENTER>~C
    ssh> -L 5000:localhost:5000
```

Deliberately Use Password Authentication Instead of PubkeyAuth

```
ssh -o PreferredAuthentications=password -o PubkeyAuthentication=no myhost
```

Escape Characters: Kill Unresponsive Session

```
<ENTER>~.
```

Multi-hop SSH

Scenario: `host1` is accessible from the local machine, but `host2` is only accessible from `host1`, and `host 3` only through `host2`.

~/.ssh/config

```
Host host1
  HostName host1.example.com
Host host2
  ProxyCommand ssh -q host1 nc -q0 host2 %p
Host host3
  ProxyCommand ssh -q host2 nc -q0 %h %p
```

Command Line

```
ssh -A -t host1.example.com ssh -A -t host2 ssh -A host3
```

SSH through SSL, e.g. for IDS Evasion

So traffic over 443 appears to be SSL, and therefore not triggering IDS. See also stunnel or

Proxytunnel for alternative setups.

```
ssh -o ProxyCommand="openssl s_client -host <H> -port <P>" ...
```

Use PKCS8 for private Keys

```
mv ~/.ssh/id_rsa ~/.ssh/id_rsa.old
openssl pkcs8 -topk8 -v2 des3 -in ~/.ssh/id_rsa.old -out ~/.ssh/id_rsa
chmod 600 ~/.ssh/id_rsa
# Check that the converted key works; if yes, delete the old one:
rm ~/.ssh/id_rsa.old
```

Access Windows Share

```
smbclient -U "DOMAIN\user" //dc.domain.com/share/test/dir
```

Append Text to a File that Requires Raised Privileges

```
echo "some text" | sudo tee -a /path/file
```

Feed Local Wireshark with Remote tcpdump

```
ssh gw tcpdump -i eth3 -U -s0 -w - 'tcp port 80' | wireshark -k -w
/tmp/gw.cap -b filesize:50000 -b files:10 -i -
```

Correct ownership and permissions of SSH user directory

```
chmod go-w $HOME $HOME/.ssh
chmod 600 $HOME/.ssh/authorized_keys
chown `whoami` $HOME/.ssh/authorized_keys
```

Autossh

```
autossh -M 0 -fN foo
```

systemd integration (e.g. /etc/systemd/system/autossh.service)

```
[Unit]
Description=AutoSSH tunnel service
```

```
After=network.target

[Service] Environment="AUTOSSH_GATETIME=0"
ExecStart=/usr/bin/autossh -M 0 -N mysshserver.example.com  -L
25:127.0.0.1:25 -R 2222:localhost:22

[Install] WantedBy=multi-user.target
```

ssh-keygen

```
ssh-keygen -C "foo@bar.com" -t rsa -b 4096 -a 500 -f ~/.ssh/id_rsa_foo_2021
```