SSH Cheat Sheet

SSH has several features that are useful during pentesting and auditing. This page aims to remind us of the syntax for the most useful features.
NB: This page does not attempt to replace the man page for pentesters, only to supplement it with some pertinent examples.

SOCKS Proxy

Set up a SOCKS proxy on 127.0.0.1:1080 that lets you pivot through the remote host (10.0.0.1):

Command line:

```
ssh -D 127.0.0.1:1080 10.0.0.1
```

~/.ssh/config:

```
Host 10.0.0.1

DynamicForward 127.0.0.1:1080
```

You can then use tsocks or similar to use non-SOCKS-aware tools on hosts accessible from 10.0.0.1:

```
tsocks rdesktop 10.0.0.2
```

Local Forwarding

Make services on the remote network accessible to your host via a local listener.
NB: Remember that you need to be root to bind to TCP port <1024. Higher ports are used in the examples below.

Example 1

The service running on the remote host on TCP port 1521 is accessible by connecting to 10521 on the SSH client system.

Command line:

```
ssh -L 127.0.0.1:10521:127.0.0.1:1521 user@10.0.0.1
```

~/.ssh/config:

```
LocalForward 127.0.0.1:10521 127.0.0.1:1521
```

Example 2

Same thing, but other hosts on the same network as the SSH client can also connect to the remote service (can be insecure).

Command line:

```
ssh -L 0.0.0.0:10521:127.0.0.1:1521 10.0.0.1
```

~/.ssh/config:

```
LocalForward 0.0.0.0:10521 127.0.0.1:1521
```