

Lab – Installing PowerShell Empire On Kali Linux

Overview –

In this lab, you will be shown how to install PowerShell Empire on Kali Linux 2021.1. When it comes to PowerShell Empire, not all installation packages are created equal.

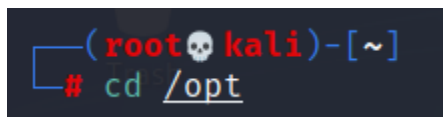
Lab Requirements

- One install of VirtualBox, with latest version and extension pack.
- One virtual install of Kali Linux, latest version.
- Snapshot of current configuration

Install PowerShell Empire

From your Kali desktop, open a new terminal window. At the prompt, copy and paste or type in the following command—press enter.

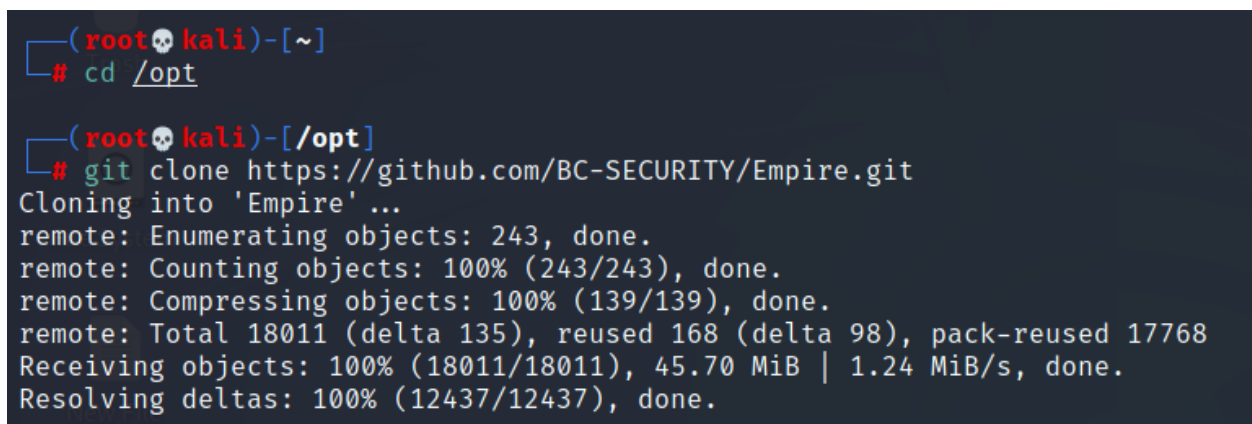
```
cd /opt
```



```
(root@kali)-[~]  
# cd /opt
```

Clone PowerShell into your installation of Kali using the following command.

```
git clone https://github.com/BC-SECURITY/Empire.git
```



```
(root@kali)-[~]  
# cd /opt  
  
(root@kali)-[/opt]  
# git clone https://github.com/BC-SECURITY/Empire.git  
Cloning into 'Empire' ...  
remote: Enumerating objects: 243, done.  
remote: Counting objects: 100% (243/243), done.  
remote: Compressing objects: 100% (139/139), done.  
remote: Total 18011 (delta 135), reused 168 (delta 98), pack-reused 17768  
Receiving objects: 100% (18011/18011), 45.70 MiB | 1.24 MiB/s, done.  
Resolving deltas: 100% (12437/12437), done.
```

Once the download has finished, copy and paste or type each of the commands one at a time into the terminal prompt.

- cd Empire/
- ls
- cd setup/

- `ls`

```
(root@kali)~/opt
# cd Empire

(root@kali)~/opt/Empire
# ls
changelog  config.yaml  Dockerfile  lib  plugins  pyproject.toml  setup  wiki
cli        data        empire      LICENSE  poetry.lock  README.md      VERSION

(root@kali)~/opt/Empire
# cd setup

(root@kali)~/opt/Empire/setup
# ls
cert.sh  install.sh  requirements_libssl1.0.txt  requirements.txt  reset.sh  setup_database.py
```

We next need to install the application running the **install.sh**. At the prompt, type in the following command.

`./install.sh`

Some files will need to be updated, and others will need to be downloaded, so be patient and do not interrupt the install!

```
(root@kali)~/opt/Empire/setup
# ./install.sh
Get:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease [30.5 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Contents (deb) [39.7 MB]
Get:4 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Packages [199 kB]
Get:6 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Contents (deb) [942 kB]
```

Launch PowerShell Empire

Move back one directory using the following command.

`cd ..`

```
(root@kali)~/opt/Empire/setup
# cd ..
```

Launch PowerShell Empire using the following command. Press enter.

`./empire`

```
(root@kali)~/opt/Empire
# ./empire
```

PowerShell Empire launches.

```
[Empire] Post-Exploitation Framework

[Version] 3.8.2 BC Security Fork | [Web] https://github.com/BC-SECURITY/Empire

[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller

EMPIRE

319 modules currently loaded
0 listeners currently active
0 agents currently active

(Empire) > 
```

Using the help command

At the Empire prompt, type help to see what options are available.

```
(Empire) > help

Commands
=====
agents          Jump to the Agents menu.
creds           Add/display credentials to/from the database.
exit            Exit Empire
help            Displays the help menu.
interact        Interact with a particular agent.
keyword         Add keyword to database for obfuscation

list            Lists active agents or listeners.

listeners       Interact with active listeners.
load            Loads Empire modules from a non-standard folder.
plugin          Load a plugin file to extend Empire.
plugins         List all available and active plugins.
preobfuscate    Preobfuscate PowerShell module_source files
reload          Reload one (or all) Empire modules.
report
```

Beware that each time you need to launch PowerShell Empire, you will need to first change the location of your working folder over to the Empire directory.

```
(root@kali)-[/opt/Empire]
# ./empire
```

Summary –

In this short lab, you got to install PowerShell Empire. There are plenty of tutorials on the Internet and YouTube that show you how to install PowerShell Empire. Because of upgrades with Kali and Python dependencies with the program, the older tutorials no longer work.

In our next lab, we will cover the basics of what you need to know to use the PowerShell Empire Framework. Stay tuned!