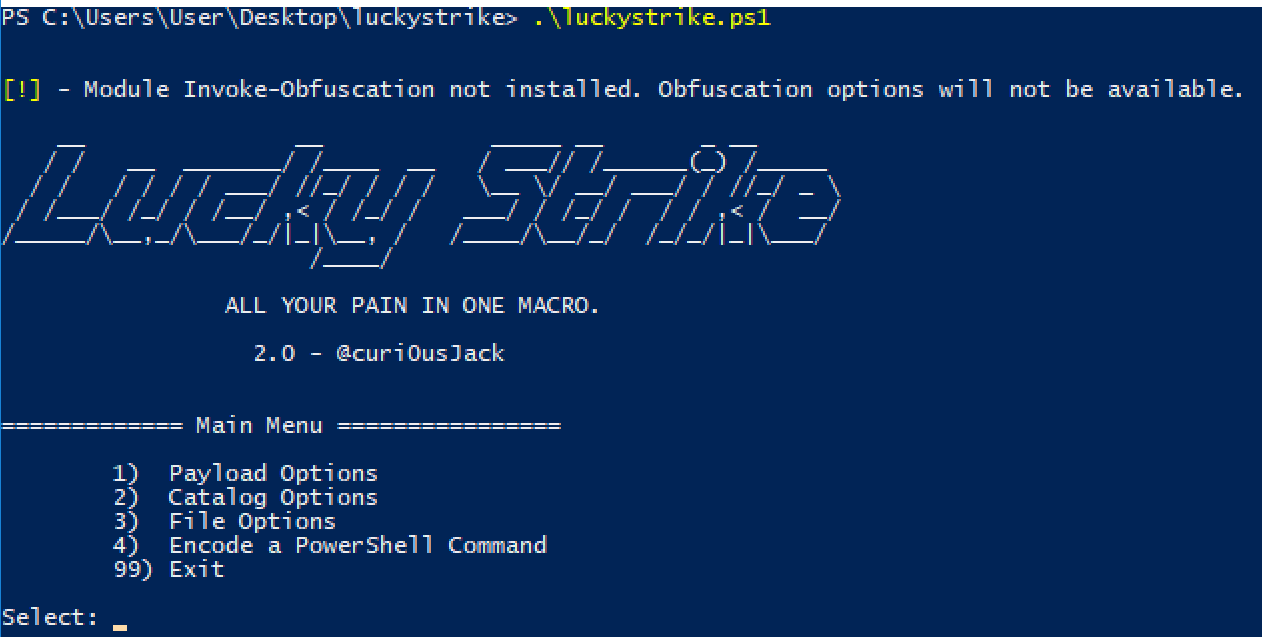
Lab 13 - Phishing and Shells

We want to explore the use of Office documents as a means for gaining access to our target environment. This will require the following tools/resources:

* A Windows 7 - 10 VM
* Powershell
* Luckystrike framework
* Microsoft Office **(necessary)**

Please complete the following steps:

1. Follow the setup instructions located here: <https://www.shellntel.com/blog/2016/9/13/luckystrike-a-database-backed-evil-macro-generator> and install LuckyStrike in your Windows VM. Demonstrate successful setup by showing the primary menu via screenshot. For example:  
     
   
2. Generate 2 - 3 malicious office documents, explore the different options within the framework to generate these. Detail the documents you created: what did they do and what is unique in relation to other documents you created. Provide screenshots along with your description.
3. Finally, these documents do not contain any content outside of the macro code. Discuss what you might add to these documents to customize and them to increase the likelihood that a user will open them and enable the macros.

**Deliverable**

Turn in a PDF or (non-macro) Word document with your lab report.