Intrusion Vector Attack– Phishing + DNS Tunneling

Author: Michael Perry

OS: Linux

Python Version: 3.8

First vector attack - **Phishing.py**

Prerequisites - Libraries:

- OS – operating system operations such as delete, create, basename and more.
- Validators – checking weather string is URL,File etc…
- Smtplib – connection to local mail service.
- Time – for sleeping the program.
- Requests – for http get requests.
- Spacy – NLP library for learning more efficiently the email.
- Html2text
- Base64 – decode emails that encoded in base64
- Inquirer – command line GUI for user interface choices
- Sys – argument handler
- Quopri – decode quoted-printable html encode properly
- Email – handle parsing emails

Running instruction:

```
python3.8 Phishing.py [username] [mail service] [job title] [URL]/[File name]/[Text]
```

Optional arguments.

Must arguments. If you will enter less it will do nothing.

Description: this tool will generate email phishing by given arguments and learning some more information like emails.

With the generate email the tool send attachment file called Attachment.py and will activate stage 2 of the attack.

Second vector attack – **Attachment.py**

Prerequisites - Libraries:

- Subprocess – execution of bash script**.**
- Requests – http get requests**.**
- Os – operating system manipulation such as : chmod +x , stat and more..
- Scapy – for dns queries (DNS tunneling)

Running instruction:

Tunneling IP Target Machine: 10.0.2.8

```
sudo python3.8 Attachment.py
```

Description: this tool will use LinEnum tool , generate the shell script, make the script executable, running it, mapping all the system and send it all via DNS protocol and after that delete all the created files.