Utica University Attack Surface Mapping

This project involves using OWASP Amass to enumerate the subdomains of Utica University's domain (uti

Tools Used:

- OWASP Amass: For domain enumeration and attack surface mapping.
- Go Language: Required to install and run Amass.
- Optional Tools: Gephi, Maltego, or Excel for external visualization if necessary.

Steps Involved:

1. Installation of OWASP Amass

Before enumerating the domain, ensure OWASP Amass is installed:

```bash
go install -v github.com/owasp-amass/amass/v3/...@master
```

or

```bash
brew install amass
```

2. Enumeration of utica.edu

To enumerate subdomains associated with Utica University, run the following command:

```bash
amass enum -d utica.edu
```

If no results are found, you can use brute-force enumeration:

```bash
amass enum -brute -d utica.edu
```

Example of discovered subdomains:

```bash
ns2.utica.edu
lists.utica.edu
drupal.utica.edu
connect.utica.edu
```

3. Visualizing the Results

The tool oam_viz can be used to visualize the results, but if that doesn?t work, you can generate output in

```bash
amass enum -o amass_output.txt
```

Alternatively, Amass has its own simple visualization:

```bash
amass viz -d utica.edu
```

You can also output the results in JSON for further processing:

```bash
amass enum -d utica.edu -json amass_output.json
```

4. Optional Visualization Tools

- Gephi: Import results into Gephi for advanced network graph visualization.

- Maltego: Use Maltego for mapping relationships between subdomains.

- Excel: Load CSV outputs into Excel to analyze and chart subdomains.

Conclusion

This process outlines how to map the attack surface of a domain using Amass. The results can be further a