

building the GPT

start with a basic template.

```
TA0001 - Initial Access
```

```
---
```

```
aliases:
```

```
  - Initial Access
```

```
tags:
```

```
  - tactic
```

```
  - initial_access
```

```
title: Initial Access
```

```
id: TA0001
```

```
---
```

```
The adversary is trying to get into your network.
```

prompt:

if free version:

"Give me a python script that will generate MD files in the format of the attached MD file of each mitre att&ck tactic, within a folder named after itself."

if paid version, and you dont want to build any scripts:

"Give me an MD file for each mitre att&ck tactic in the format of the given MD file, within a folder named after itself"



TA0043 - Reconnaissance.md

File

give me a python script to create markdown files of all the mitre tactics
in the format of the attached markdown file

this will give you the basic mitre framework for tactics. i suggest not doing techniques until you flesh out your tools, protocols, and other notes.

now, you can use the same format to build your tools. you can either ask it to build some examples for you, or add your own. this whole process is highly customizable.

prompt:

for examples:

"using the same format, write me a python script to give me markdown files for offensive security tools with the tag 'tool'. put these in a folder called 'tools'. map them to the mitre tactics using tags, and include a tactics field in the YAML frontmatter. also include a synopsis about the tool, a basic usage section with a codeblock, and reference links to the tool."

to generate a markdown file for a tool of your choosing, it is easiest to first let it build you examples and use one of those markdown files as a template.

prompt:

```
write me a MD file on the offensive security tool 'certipy' using this example
template: --- aliases: - Nmap tags: - tool - references - reconnaissance
title: Nmap id: TL0001 tactic: Reconnaissance related_tactic: TA0043 --- ##
Synopsis Nmap is a network scanner used to discover hosts, services, and
vulnerabilities. ## Basic Usage
\```
bash
nmap -sV target.com
\```
## References - https://nmap.org/ - https://github.com/nmap/nmap
```

(omit the backslashes for the bash code block, this is for the purpose of this pages markdown formatting)

write me a MD file on the offensive security tool 'certipy' using this example template:

```
---
aliases:
  - Nmap
tags:
  - tool
  - references
  - reconnaissance
title: Nmap
id: TL0001
tactic: Reconnaissance
related_tactic: TA0043
---

## Synopsis
Nmap is a network scanner used to discover hosts, services, and
vulnerabilities.

## Basic Usage
bash
nmap -sV target.com

## References
- https://nmap.org/
- https://github.com/nmap/nmap
```

now, we can do something similar for protocols.

prompt:

for examples:

"using the same format, write me a python script to give me markdown files for commonly abused protocols with the tag 'protocols'. put these in a folder called 'protocols'. map them to the mitre tactics using tags, and include a tactics field in the YAML frontmatter. also include a synopsis about the protocol, and reference links to the protocol."

after putting all the folders inside of your obsidian vault, your graph should look something like this.



now its up to you to build upon the notes!

justification for python scripts and CLI: