**COS30015 IT Security**

**LAB 2 (week 2)**

Purple Team Exercise Planning Template

**Task 1**

|  |  |  |
| --- | --- | --- |
| Threat | Example | Characteristic identified |
|  |  |  |

**Task 2**

Case summary of chose threat and example (max 4 paragraphs):

Task 3

Outline your scenario with a diagram and steps

**Task 4**

Record identified information.

Offensive Tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool/Activity** | **Ease of Install** | **Amount of Documentation** | **Community Activity** | **Available Features to Produce Threat** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Defensive Tools

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tool/Activity** | **Ease of Install** | **Amount of Documentation** | **Community Activity** | **Available Features Against Threat** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Task 5**

Outline relevant MITRE TTPs: