# TEA Development – Exercise Template

## TEA Template:

(Duplicate as needed to create additional TEAs.)

|  |  |
| --- | --- |
| **Threat Emulation Action 1** | |
| **Overview** | Conduct a targeted phishing campaign and record the number of clicks a link gets. This would simulate how a threat actor could compromise credentials or gain access to the network. |
| **Discussion** | Using messaging methods such as email, attackers can socially engineer users into downloading and executing software, which quietly installs malware alongside of the desired program. |
| **Expectations IAW Documentation** | The local user awareness policy training policy should prevent this type of attack. The local defender may get help desk calls regarding the phishing attempt. The email message can be purged from the servers after the event is over. |
| **Timeline** | Initial timeline would be the first week of the operation possibly extend longer depending on command emphasis. |
| **Assumptions** | Users will click on the link exposing the environment to risk. This is a common form of attack, so we are expecting to have a high volume of clicks. |
| **Procedure** | Craft a special e-mail that would entice the user to follow the link or open an embedded file and track the hits for reporting purposes. |
| **Targets** | Are targets will be senior ranking personnel at first and expand out if needed. |
| **Proof of Success** | The click counter will increase. |
| **Cleanup Actions Required** | The message will be purged from the servers at the end of the operation and training material will be provided to those that clicked. |