|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Team:** | | | **Introduction to Covert Channels**  **Lecture Rubric** | | | | | **Date:** | | | |
|  | | | **Grader: Lt Daniel Fitzgerald** | | | | | **Overall Score:** | | | |
|  | **Criteria** | **Unsatisfactory** | | | **Minimal** | | **Proficient** | | | **Exemplary** | **Score** |
|  | | | | | | | | | | | |
| 40% | **Working Code**   * Code written in C/Python * Code runs * Channel transfers data * PCAP of channel running | * Code does not run * Client/Server do not connect * Data is not transferred * PCAP not included | | * Data is being transferred but complete error-free file is not transferred * PCAP included does not match traffic produced by code * Code errors / crashes | | * Code runs and can transfer data * PCAP is included and mostly matches running code * Code occasionally returns incorrect results | | | * Code runs and can transfer data including the target file over the target network * PCAP is included and accurately matches running code * Code has error checking and exits gracefully depending on situation | |  |
| 30% | **Write Up: Metrics**   * Discusses metrics of chosen channel * Tradeoffs made and why channel was chosen * Other channels considered | * No metrics discussed * No discussion of design choices or tradeoffs * Chose channel for no reason with no comparison | | * Minimally discusses metrics * Limited discussion of design choices and tradeoffs * Chose channel for poor or incorrect reasons | | * Discussion of channel metrics is present * Tradeoffs and design choses are listed * Chose channel for logical reasons with a modest comparison | | | * A complete evaluation of metrics and tradeoffs is done in relation to the target network * Chose channel for ideal reasons and completed a comparison of channels to determine most likely avenue of success | |  |
| 10% | **Write Up: Definition and Description**   * Discussion of what covert channels are and the different types * Description of chosen channel and how it works | * Incoherent * Does not follow writing guide * Does not accurately portray the work or the result * Not finished | | * Point conveyed, after careful analysis of report * Multiple distracting mistakes * Accurately portrays results * Addresses required points | | * Demonstrates point with little logical distractions * No glaring mistakes * Accurately portrays results with minimal insight * Addresses required points and relevant processes in logic and development | | | * Publishable clarity and brevity * No mistakes * Accurately addresses results and technical insight into failures/successes * Addresses all relevant points along with requirements. No follow up questions required | |  |
| 15% | **Documented/Commented**   * Functions and variables are commented properly * User Manual created detailing configuration and use of channel | * No comments in code * No User Manual included * Unable to understand program flow | | * Code poorly commented or comments do not make sense * Minimal or incorrect User Manual * Difficult to understand program flow | | * Code is commented but is either under or over commented (i.e. every line commented) * User Manual is complete but difficult to understand * Can understand flow with some effort | | | * Code is properly commented and understandable (i.e. Doxygen/PEP8) * Complete and easy to use User Manual * Easily able to understand program flow | |  |
| 5% | **Application**   * Channel has the ability to tunnel traffic through it * Steps to enable this feature are documented * Scenario: You have a foothold on a network and want to create a covert tunnel to pass all your traffic through to evade detection. | * No tunnel functionality * No documentation | | * Channel attempts to integrate functionality but fails * Limited or incorrect integration documentation | | * Functionality present but will occasionally drop packets or crash the tunneled connection * Integration steps are correctly documented | | | * Channel successfully implements tunnel functionality * Integration steps are correctly documented * Simple and easy to use * Traffic tunnels seamlessly | |  |
| **Comments on Reverse** | | | | | | | | | | | |