Introduction to Covert Channels

18 July 2022

# Instructor Information

|  |
| --- |
| Name: Daniel Fitzgerald  Organization: 70th Operations Support Sq |

Description

Interns will learn the history and basics of covert channels. The lecture will cover network and packet analysis fundamentals, types of covert channels, metrics associated with covert channels, defenses against them, and integrating them into existing platforms such as Cobalt Strike. A follow-on assignment will task them with creating their own unique covert channel over a given network and require them to evaluate the metrics of this channel and discuss the tradeoffs they made in the development process. This will allow interns to demonstrate evasion of defenses, covert C2 integration with Cobalt Strike, and expose them to weaknesses in these systems.

# Learning Objectives

This lecture will expose students to covert communication channels. They will learn about how malicious actors evade network defenses for communication, and ultimately have a better knowledge of network fundamentals as well as the offensive and defensive techniques for C2.

# Prerequisites

Networking fundamentals

C and/or Python

Network programming in C and/or Python

# Required Preparation

None

# Course Outcomes

After this lecture, students should be able to accomplish the following things, organized according to Bloom’s taxonomy:

1. **Know**
   * Define what covert channels are and describe the various types
   * Identify the metrics associated with covert channels
2. **Understand**
   * How network defenses detect and categorize suspicious traffic
   * Compare/contrast types of channels for target use
3. **Apply**
   * Modify existing channels to evade network defenses
   * Articulate testing methodology
   * Discover weaknesses in network defenses and successful evasion methods
4. **Analyze**
   * Study target’s base-line network traffic
   * Survey available C2 techniques for use
   * Deduce best option for use in test networks
5. **Evaluate**
   * Judge the success of their attempts at bypassing various defenses
   * Determine metrics of channel and decide if they meet requirements
   * Consider alternatives if attempts repeatedly fail
6. **Create**
   * Develop covert channel to bypass defenses
   * Integrate channel with existing framework (Cobalt Strike)
   * Technical solutions to realistic problems with resource constraints

# Challenge Problem

Interns will be given an example PCAP file of traffic traversing a target network. They will be tasked with creating a covert channel to exfiltrate a file over the target network without triggering an IDS on the network. They will be responsible for providing the code, a PCAP of the traffic from the channel, a User Manual for proper use of the channel, and a write up with a description, the design decisions of the channel, metrics, and tradeoffs they made in the development process. The code will be in C and/or Python unless other language approved by instructor and will be properly documented and commented.

# Evaluation Criteria

The grades will be broken out based on the following criteria:

* Code runs and transfers data
* Code is commented and documented with a User Manual
* Metrics and tradeoffs are evaluated and discussed in the write up along with why specific channel was chosen
* Write up includes discussion of covert channels and the various types along with description of chosen channel
* Optional: Channel integrates into Cobalt Strike or additional alternate channel implements a Malleable C2 Profile.

See rubric for description and percentage breakdown.

# Tools and Techniques

They will learn the basics of covert channels and the various types. It will be up to them to figure out what type of channel they want and what, if any, tools they use. The other tools/techniques they would use would be socket programming in C/Python where they will be able to choose their own development environment and open source tools such as Scapy for crafting packets.

# Other Information

Cloud infrastructure to run the VMs.

Ability to run channels and dump traffic from SISI and IronZone networks.

Scripts to create “normal” traffic over the networks for the channels to blend into.