## Challenge Name: Ghost of a Chance

## Suggested Category: Web

## Submitter Name: Matt Weir

## Suggested Point Level: 200-300

## Description: The Gh0st Remote Access Toolkit (Gh0st RAT), is a well-known tool used by APT actors. What’s nice is if you know the protocol, it is very easy to decode sessions from network captures. Also it is very easy to detect since all sessions start with the string “Gh0st”. For example, the public release version of MITRE’s Chopshop program, (<https://github.com/MITRECND/chopshop>), has a built in decoder for Gh0st traffic.

**For the challenge, a pcap is provided that shows Gh0st encrypted traffic between a C&C server and a client, where the hacker is looking through a compromised computer and eventually finds the flag file. You could get as elaborate, (or as funny), as you want to show an attack session in progress. For the teams to solve it, they would simply need to run the pcap through Chopshop and read the flag from the output. The reason this might be a 300 level challenge is many of the teams might not know about Chopshop.**

## External Resources: None

## Suggested Tools/Solution Methods: MITRE’s Chopshop would be the easiest, but I’ve heard there are also plugins for McAffee’s File Insight to decode Gh0st C&C traffic.

## Solution (if known):

## Infosec Reviewer Name:

## Infosec Reviewer Notes:

## Implementer Name:

## Repository Location:

## Final Infosec Approver Name:

## Tester Name:

## Test Script: (detailed steps used to solve this challenge)

## Solution Files: (any code the tester wrote to solve this challenge)

## Notes: