Rootkits - 2

Objectives

- use a CC server to interact with compromised hosts (your windows7 instance) (from project 2)

Description

You have delivered a payload to compromise a windows host. Your objective now is to maintain that access, and control access to the target.

On your Kali machine, you should install powershell empire. I found it easiest to connect to my Kali instance via ssh. We will be installing this via docker. So on your Kali instance, you need to install docker.io. I have recorded a video to show you how to do this install.

A good overview of how to exploit and other things you can do with Empire is found here.

- You can exit and re-launch the docker container if you mess up. You will have to re-launch empire and re-create any listeners or agents though.
- You will need to copy the powershell script gobbledygook to your windows machine. Perhaps one suggestion as to how to do this, is install apache2 on kali if not already installed, copy the powershell commands to the document root, visit that page from a web browser on your windows instance. Or perhaps you could scp it over. In either case you will need to some how run the powershell code.
- Depending on the user that you logged into windows with will determine the `high_integrity` value of your agent. (So if it already is a 1, you need not do the bypassuac stuff)

TO submit

A single pdf with the following:

- Output of the `creds` command while interacting with your agent should show a list of some credentials.
- Experiment with at least 3 modules (preferably ones we didn't use in class) and take screenshots of what they did.
- A short paragraph explaining what powershell empire does.