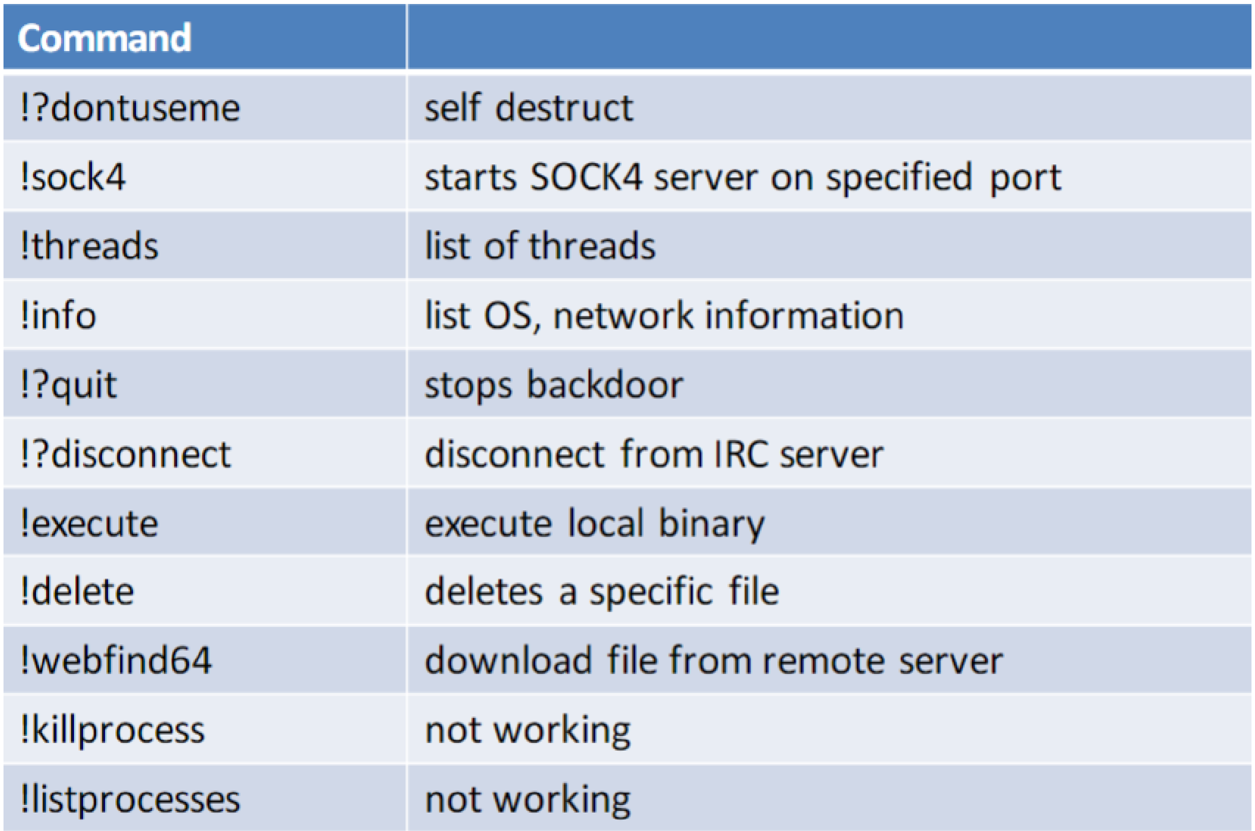
Practical 4

Software Reengineering • Auburn University • COMP 7720/7726/4970 • Summer 2018

This practical will focus on chapter 8 (malware analysis), you will need copy of the malware we used in class (Webcam Shot.scr: posted on canvas). The goal of this practical is to understand how the malware execute the hacker commands which is delivered through IRC server.

As mentioned in class hackarmy malware support several commands such as delete, execute, disconnect, dontuseme and more (complete list in the table below).



Command	
!?dontuseme	self destruct
!sock4	starts SOCK4 server on specified port
!threads	list of threads
!info	list OS, network information
!?quit	stops backdoor
!?disconnect	disconnect from IRC server
!execute	execute local binary
!delete	deletes a specific file
!webfind64	download file from remote server
!killprocess	not working
!listprocesses	not working

In this practical our focus is going to be on two commands dontuseme and webfind64. Based on the description in the book, dontuseme will destroy the malware and webfind64 is used to download a file from the internet (or remote server) into the infected machine.

(continued next page)

Practical 4

Software Reengineering • Auburn University • COMP 7720/7726/4970 • Summer 2018

Questions

Answer the following questions:

Q1. **dontuseme** command:

  a. From the assemble code of hackarmy malware, find where this command is implemented (verify your answer).
  b. In a step by step fashion, describe how this command is executed.
  c. using pseudocode rewrite this command.

Q2. **wibfind64** command:

  a. From the assemble code of hackarmy malware, find where this command is implemented (support your answer).
  b. In a step by step format describe how this command is executed.
  c. (grad only) using pseudocode rewrite this command.

Hints:

H1. Threads are usually used to execute code concurrently, for example if you are about to execute a piece of code that interacts with a slow resource (network, keyboard...etc.) rather than running it on the main thread which will hang the program, you can create a new thread to accomplish that.

H2. When creating a thread, you pass a pointer to the code to be executed.

H3. You can skip **sub_4015A6**.

H4. Don't get lost in the details.

H5. You didn't start working on the project! This is not a good idea :(at all. The due date counter (https://goo.gl/QPKzwR)