**CEG4430/6430 Homework 3**

(50 Points)

1. Conficker is a piece of sophisticated malware. Many of its designs aim at counteracting the malware analysis, detection, and disruption techniques. Please read the given article (conficker.pdf) and answer the following questions.
   1. A student wants to capture the first packet after 3-way handshake sent from a Conficker binary to the web-based C&C server. Of course, this binary will generate a large number of randomly generated domains. Towards this end, the student leverages the open source DNS relay we used for the lab and configures the conficker-infected host to use this DNS relay as the recursive DNS server. The student instruments the DNS relay to directly answer all DNS requests generated by the infected host.
      1. Scenario-1: The DNS responses (answers) will contain two IP addresses of two web servers that are managed by this student. Will this student be able to capture the first packet after the 3-way handshaking initiated from the Conficker-infected host to his/her server? Justify your answer. (5 Points)

Answer Question 1.a.i: By reading the HW3\_Conficker paper, it seems that it is impossible for the student to get the required packet after the Handshake with this result. The reason for this is that according to the paper the responses will each come from there own IP address to a connected web server. In-addition,

* + 1. Scenario-2: The DNS responses (answers) will contain one IP address of one web server that is managed by this student. Will this student be able to capture the first packet after the 3-way handshaking initiated from the Conficker-infected host to his/her server? How many such packets can be observed if your answer is not 0? Justify your answer. (5 Points)
  1. You have installed an antivirus tool called “avenger”. Unfortunately, when Conficker attempts to compromise your host, the avenger is not up to date. Therefore, your host is infected by Conficker successfully. Later, the update is available for this tool to download and install. Will avenger now be able to detect Conficker in your host? (5 Points)
  2. Determine if the following statements are true or false and justify your answer.
     1. A Conficker-infected host will result a large number of failed DNS queries (i.e., NXDOMAIN responses) (5 Points)
     2. A Conficker-infected host will cause a large number of failed TCP connections (5 Points)
     3. All IP addresses that are connected by a Conficker are malicious (i.e., either C&C server or other infected peers). (5 Points)

1. You are provided with the source code for an IRC-based bot (in the .zip file). This is a real bot that can be used for various malicious purposes. It implements all the basic functionalities of a bot. For example, it can update itself and is capable of launching DDoS attacks. It is invaluable resource for you to learn how malware works under the hood although this code is a baby-version. Please answer the following questions and **justify your answers** based on your analysis of the source code (e.g., list the code snippet and explain its function if necessary). The code is available from

<https://www.dropbox.com/s/to2y2kafjhm0gv3/IRCBot.student.zip?dl=0>

* 1. **Question:** For the command in the table**,** please describe what this command is used for, provide **evidence for conclusion based on source code and analysis**, and an example of its usage. (5 Points)

|  |  |  |  |
| --- | --- | --- | --- |
| **Command** | **Function** | **Evidence** | **Example** |
| **login** |  |  |  |
| **open** |  |  |  |
| **execute** |  |  |  |
| **die** |  |  |  |
| **remove** |  |  |  |
| **download** |  |  |  |
| **update** |  |  |  |
| **systeminfo** |  |  |  |
| **netinfo** |  |  |  |

* 1. **Question:** Compare pairs of commands and present your analysis based on the source code. (5 Points)

|  |  |
| --- | --- |
| **Commands** | **Comparison** |
| **die v.s. remove** |  |
| **download v.s. update** |  |
| **open v.s. execute** |  |

* 1. **Question:** Analyze the source code and list three commands that can be used for issuing DDoS attacks against network services. Explain how they can be used for such attacks. (10 Points)