CS 340: Cyber Security

Vulnerable Web Service (40 points)

# Building a Backdoor and Listener

DUE: End of day Monday, March 23, 2015

**Description**

Since you have mastered Socket programming, we will develop a Backdoor and a Listener. In the end, you will have built two tools that are capable of obtaining command line access to one machine from another, while remaining undetected. Your final result should be able to demonstrate that your Backdoor is capable of delivering a command line to the user, through the listener, and is capable of executing commands sent from the user and be undetected by the target(console popups, .NET error messages, etc..).

A Backdoor is a method of bypassing normal authentication, securing illegal remote access to a computer and obtaining access to the computers resources, while attempting to remain undetected. When the listener receives a connection request, it sets up a TCP connection through a static port and opens the connection to the backdoor. In the first stage of this assignment, you should write a listener that simply displays the contents of a request message that it receives. Next, you should develop the Backdoor program that notifies the listener that it has started and is able to run system commands as requested. After this program is running properly, you should add the code required to generate a command line on your listener.

You can test your listener via command line and localhost. Recall that you should not listen on an in-use port, so you need to specify a port number that will likely be unused on the target machine. For example, if your target machine is only running HTTP and FTP, your Backdoor and listener can open a socket on any port other than 80 and 21. It is highly recommended that you perform all testing in a Virtual Machine to avoid exposing your machine possible exploits and to avoid introducing new vulnerabilities.

Once completed, add a keylogger capability to your backdoor system that can be activated and deactivated remotely. It is at your discretion to decide how the log is transmitted. It can be streamed to the listener, stored in a local file and transferred after done recording, viewed in the remote machine, etc.

**Requirements:**

1. Your Backdoor must be a Windows executable (.exe) and must be written in C#. You need to make sure that the backdoor's port number and ip address (IP address to listener) can be set and generated as needed.
2. To avoid detection, you should write your executable on a version of .NET earlier than 3.0. If your target has .NET 3.0 installed and you send an executable requiring .NET 4.0, the target will get suspicious of the error message and your task will fail.
3. You can assume that the infected user has administrator privileges. The basic requirements for the backdoor includes but is not limited to directory traversal, creation of new file, deletion of a file, reading a file, copy/transfer file from and to the target machine and reboot/shutdown the remote machine.
4. The listener must be a script written in Ruby, Python, or Perl. You need to make sure that the listener port can be changed as needed (not hardocded).
5. The keylogger only need to log what keys are pressed, you do not have to log duration. You do not have to record other input device such as the mouse, scanner, etc.
6. Write a short and concise report (two pages max, 1 inch margin all around, 12 pt font size) on how you approach the problem, explain the libraries used, describe some of the methods developed and show some examples. The idea of the report is to provide an overview of your program without having to go through the source code. If you are implementing someone else’s approach to the problem, you must add reference(s) to the author.

**Deliverables:**

* The source code for web server, source code the backdoor (make sure that you submit the complete project for C#), the backdoor executable, the listener script, report and all other pertinent files should be submitted.
* Submit your files and the report document (Word or PDF) through MUOnline. Make sure they are zipped into one file with separate folders for each part (report, backdoor, listener).

**Grading:**

Part 1: Backdoor and Listener – 20 points

Part 2: Keylogger – 10 points

Part 3: Report – 10 points