Exploiting a Remote Client Application

Exploiting the FTPShell Client Application

In this Lab we want to write an exploit to achieve arbitrary code execution using a vulnerability in the FTPShell client application. This type of exploit is considered a remote client exploit, since you can achieve this only when the vulnerable client application speaks over the network with a malicious FTP Server. This means the client must have network access to the system running the malicious FTP server, which you will be creating. This application is also vulnerable to a memory corruption (buffer over) which is found when sending back the client a long directory. Therefore, in order to exploit the application, we need to create an FTP Server which can forge responses back to the FTP client to achieve our exploitation purposes.

Note:

Before doing anything related to exploitation, make sure both your Kali Linux and Windows machine can communicate with each other. We can prove that by sending a ping request from Windows to Kali Linux, or the opposite (requires an update to the Windows firewall).

This time you are on your own!!! Use the code given to start your exploitation process. Kali will hold the malicious FTP Server code and the ftp client will be on Windows speaking to the Kali system.

Deliverable: you are required to either submit a video or a document with a full walkthrough of the process.

Reflection: please reflect on what you learned from this lab by working on it with no instructions given.