**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).

In case not found on your virtual machine:

* [FTPShell](https://www.exploit-db.com/apps/40d5fda024c3fc287fc841f23998ec27-fa_ftp_setup.msi) Client Application
* Starting python template “Lab-17-exploit1.py” renamed to exploit1.py in the lab
* Shellcode to be used “payload.txt” renamed to payload.txt in the lab
* Exploit could be found here: <https://www.exploit-db.com/exploits/44596>

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.