**Services Assigned to Students for Individual Projects**

Top of Form

Bottom of Form

* This project is based on defending a Linux or Windows system service.
* Server: FileZilla FTP Server
* Operating System: Windows

Over the semester you will be responsible for:

1. Installing the service and learning how it functions

2. Understanding the default and non-default configuration options and how they can be vulnerable

3. Learning multiple methods to attack the service

4. Learning how to harden the service to defend against your attacks

Below is an example of a timeline that would allow you to be most successful for your project:

1. You should have your service installed, functioning, and understand the default options before class on Feb 15th

2. You should understand and be able to demonstrate all of the methods to attack the service before class on Mar 21st

3. You should be able to describe your methods of hardening the service and have your slides and video completed before class on Apr 11th 

Notes:

Do NOT use your RADISH VMs to work on your individual project as any new configurations could affect your ability to complete homework labs over the course of the semester.

If Column C of the spreadsheet shows:

**Windows** – You may install the service on your local personal machine or can create a separate Windows OS in a VM after installing VirtualBox or VMware Player (both are free) or using BootCamp if you have a Mac.  Windows OS can be found on Dreamspark.

Tips:

Once you install your service, use netstat or nmap to determine what ports are open.  Try to connect to those ports in various ways (web browsers, telnet, ssh, etc.)  Perform research online to try to find information about common vulnerabilites in the service and common misconfigurations that led to security issues.  Your service may allow an attacker to be able to steal data, intrude into a network, install malicious software into a network, or perform functions that they shouldn't be authorized for.  Once you find all of these vulnerabilities, learn how to attack/exploit them and then how to harden the service to prevent your attacks.  I would like you to focus on misconfiguration issues or other hand's on vulnerabilities.  I don't want you to simply mention an issue such as a buffer overflow that can be fixed with a patch.

Each student will turn in the following to me before class on April 11th:

5-10 PowerPoint slides in your own words explaining:

1. What your service does

2. Common default or non-default configuration options that led to a vulnerability and any other insecure issues you uncovered with the service

3. Your methods to harden the service to defend against these attacks

4. \*\*Make sure you include a Bibliography slide with citations for any resources you used for the project.

5. Short video (1 minute) showing at least one example of your running service being attacked by you and then showing your service resisting that same attack after being hardened.  (I want to see a hand's on attack and do not want to simply see you mention your service is vulnerable to a software issue and then just show yourself fixing it by downloading a patch.)

I will review the PowerPoints and videos shortly after April 11th and will provide feedback for any needed changes.

On Apr 25th, each sutdent will present their PowerPoint and video to the class.  Each student will have around 7 minutes total to present.