**实验4：缓冲区溢出攻击实验**

**时间：**第4周

**地点及方式**：教室

**人员：**全体学生

**实验内容：**

本实验的学习目标是让学生将从课堂上学到的有关缓冲区溢出漏洞的知识进行实践，从而获得有关该漏洞的第一手经验。缓冲区溢出是指程序试图将数据写入预先分配的固定长度缓冲区边界之外的情况。恶意用户可利用此漏洞改变程序的流控制，甚至执行任意代码。此漏洞是由于数据存储（如缓冲区）和控件存储（如返回地址）的混合造成的：数据部分的溢出会影响程序的控制流，因为溢出会改变返回地址。

本实验将提供四台不同的服务器，每台服务器运行一个带有缓冲区溢出漏洞的程序。实验任务是开发一个利用漏洞的程序，并最终获得这些服务器上的root权限。除了进行这些攻击实验之外，还将试验几种针对缓冲区溢出攻击的对策。学生需要评估这些计划是否有效，并解释原因。

**实验报告：**

需要提交一份详细的实验报告和截图，来描述做了什么和观察到了什么。**还需要对观察结果进行解释**。还请列出重要的代码片段，然后进行解释。仅附加代码而不作任何解释将不得分。

**评分要点：**

1. 功能完成情况：60%；
2. 代码规范性：20%；
3. 报告质量：20%

**提交方式：**

请在学习通作业模块提交，选择对应的作业编号进行提交，请注意：

* 代码命名为：Lab4\_code\_学号.zip
* 文档命名为：Lab4\_doc\_学号.pdf