实验 9 缓冲区溢出攻击与防范

## 实验目的

通过实践掌握缓冲区溢出的原理；掌握常用的缓冲区溢出方法；理解缓冲区溢出危害 性；掌握防范和避免缓冲区溢出攻击的措施。

## 实验准备

（1）理解缓冲区溢出攻击的原理。

（2）获取 War-ftp 1.65，学习使用该软件。

（3）了解 War-ftp1.65 漏洞细节：发送长度超过 480 字节的用户名给 War-ftp 服务器可 以触发漏洞(即 USER longString\r\n) ，溢出之后 ESP 指令寄存器的内容包含了 longString 中的部分内容。远程攻击者可利用此漏洞以应用程序进程权限执行任意指令。

（4）熟悉 www.metasploit.com 中生成 shellcode 的方法。

（5）安装perl，学习使用光盘中的patternCreate.pl和patternOffset.pl，其中patternCreate.pl 用于创建不重复的字符串，patternOffset.pl 用于定位字符串。

（6）学习使用一种调试工具，因为要查看溢出后缓冲区里的情况和各寄存器的信息， 需要用到调试工具。比较专业的调试工具有 OllyDBG、IDA Pro 等，比较简单易用的调试工具有 NTSD、CDB 和 WinDbg（这三个工具都包含在 Debugging Tools for Windows 中，其中 Windows 2000 以上的系统自带有 NTSD）。在此实验中推荐使用 CDB 或者 NTSD，两者的 使用方法基本一致。

（7）学习参考书目中对 CCProxy6.2 Ping Overflow 漏洞的分析与利用，在理解实例的基础上完成此实验。

## 实验内容

利用 War-ftp 1.65 Buffer Overflow 漏洞，在目标主机上添加一个用户。按照如下步骤进行：

（1）检测漏洞的存在。

（2）构造能够实现在目标主机上添加用户的 Shellcode。

（3）获取缓冲区的大小并定位溢出点 Ret 的位置。

（4）改变程序的流程使 War-ftp 在溢出之后执行 Shellcode。

（5）选择一种编程语言实现漏洞利用程序。

## 实验要求

（1）在实验报告中写明利用该缓冲区溢出漏洞的主要步骤、关键代码段。

（2）提出解决漏洞的方案。

（3）总结缓冲区溢出漏洞攻击的原理和防范思路。