“综合实践三”课设总结报告

**.**

**班 级：xxxxxxxx.**

**姓名：**　 **xxxx** 　.

**学号：**　 **xxxxx** 　　 　.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **项目** | **流量** | **逆向** | **内核** | **补丁** | **总分** |
| 分值 | 25 | 25 | 25 | 25 | **100** |
| 评分 |  |  |  |  |  |

# 流量分析

本实验分为两部分，即渗透测试和流量分析。

渗透测试主要是利用metasploit渗透测试框架，利用漏洞对靶机进行攻击，从而获得靶机的root权限的shell，拷贝/etc/shadow文件内容。并且，通过hashcat破解密文，获得msfadmin账号和root账号的密码。

流量分析主要是利用wireshark软件，对课堂提供的某一渗透测试过程中的攻击流量包进行分析，从而获得攻击主机的信息、攻击步骤，包括利用的漏洞，以及从攻击流量包中获得shadow文件，进而破解出root用户的密码。

通过本次实验，我掌握了渗透测试的基本思路，特别是后渗透测试-shell持久化，可以实现对靶机的持久化控制。此外，进一步提升了流量分析的能力。通过分析攻击流量包，可以获得攻击主机信息，实现流量取证。

1. **逆向分析**

本实验主要是学习使用IDA Pro对可执行程序进行逆向分析，通过栈溢出漏洞攻击程序。

先学习了对样例程序的分析，主要是熟练掌握IDA Pro的用法，包括如何加载可执行程序、设置断点、远程调试等技巧。利用IDA Pro强大的反编译功能，获得样例程序源码，找出栈溢出漏洞，即strcy函数调用处，紧接着精心构造输入文件，达到攻击目的。

接着尝试分析实验程序，主要的难点在于花指令和动态生成字符串。花指令需要人工纠正汇编代码，从而让IDA Pro正确反编译得到源码。无法直接获得“Success”字符串，转而获取“flag”字符串，并不断回溯，找到栈溢出需要跳转的目的代码段。

通过本次实验，明显增强了我对IDA Pro工具的使用能力，并加深了我对栈溢出漏洞利用原理的理解。

1. **内核安全**

本实验主要是Linux内核漏洞的分析与利用。

借助QEMU启动重新编译的Linux内核，并通过ssh、scp等脚本远程连接内核、给内核传送文件。

先是利用内核的“释放后使用漏洞”来完成权限提升，并通过C语言程序和内核进行交互。权限提升的核心原理是prepare\_kernel\_cred函数在参数为NULL（0）的时候，会准备root权限的结构体。通过commit\_creds函数提交，会更换原本程序的creds结构体而获得权限提升（root）。

接着利用内核的“空指针漏洞”，编写 C 语言通过空指针漏洞使内核崩溃。

最后，在前面基础上，结合空指针引用漏洞、零地址空间漏洞，以另一种方式实现权限提升。

通过本次实验，我初步学习了Linux内核漏洞的相关知识，并动手实践了释放后使用、空指针引用、零地址空间等漏洞的利用过程。

1. **补丁**

本实验主要是学习打冷补丁，通过IDA Pro修改静态二进制可执行文件，弥补程序缺陷。

首先是修复程序的逻辑漏洞，使用IDA Pro的插件keypatch，nop另一个打印性别的代码段，即可修复。

接着是修复程序的栈溢出漏洞，程序的缓冲区接收不超过10个字符，却未对输入长度进行检查。在eh\_frame段，编写汇编指令，调用syscall中的read读取10个字节，替换原有的gets函数。同时，把原有call \_gets替换为jmp语句。这样，无论输入多长的字符串均不会导致程序崩溃。

实际场景中，可能需要在程序运行时动态修补安全漏洞，这就是热补丁技术，这种修补不需要重启操作系统或应用程序。

通过本次实验，我初步学习了冷补丁、热补丁技术的相关知识，并动手实践了打冷补丁，加深了自身对程序运行机制的理解。