|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 武汉大学国家网络安全学院教学实验报告 | | | | | |
| 课程名称 | 网络对抗演练 | | 实验日期 | | 2024/5/31 |
| 实验名称 | PWN-二进制 | | 实验周次 | | 第3周 |
| 姓名 | 学号 | | 专业 | | 班级 |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  |  | |  | |  |
| 实验目的、实验要求以及实验内容  （要求：写明本次实验目的以及要求掌握的知识技能；实验内容包含必要的原理分析。） | | | | | |
| **本次实验采取以最终结果为目标，开放式解题。评分依据不唯一，例如可以将学习到的漏洞利用方式，从环境配置搭建中遇到的问题以及自己借助互联网资源进行解决的方法，以及所获取到的相关结果进行归纳总结，综合得分。**  **实验1 实验2 实验3，三选一，根据小组情况自行选择。**  **实验1** 完成32位目标程序axb\_2019\_fmt32的利用。  **实验目的：**   * + 学会32位格式化字符串漏洞利用方法，结合pwntools编写利用脚本，得到本地shell [粘贴脚本截图和shell截图]   + 掌握格式化字符串任意地址读   + 掌握格式化字符串任意地址写   + 掌握one\_gadget的使用方法   **实验题目：**   1. 完成axb\_2019\_fmt32题目，通过格式化字符串漏洞任意地址读写，拿到本地shell。   **实验2** 完成目标程序pb的利用。  **实验目的：**   * + 学会非栈上格式化字符串漏洞利用方法，结合pwntools编写利用脚本，得到本地shell [粘贴脚本截图和shell截图]   + 学会通过多级指针完成任意地址写   + 掌握one\_gadget的使用方法   **实验题目：**   1. 完成pb题目，通过非栈上格式化字符串利用方式，获取本地shell。   **实验3** 利用IDA插件keypatch完成对AWD文件夹下format、gets、pwn的程序修补。  **实验目的：**   * + 学会漏洞程序的修复。 [粘贴修补截图]   + 掌握格式化字符串漏洞修复   + 掌握栈溢出漏洞修复   **实验题目：**  1、完成AWD目录下三个题目修复，保证程序正常运行情况下，使攻击脚本无法再获取shell。 | | | | | |
| 1. 实验步骤   （要求：详细写明实验步骤和方法，关键部分需截图。没做出的题目可写思路和想法。） | | | | | |
|  | | | | | |
| 1. 实验过程分析   （要求：记录实验过程中遇到问题，进行问题分析，说明问题解决过程及方法。） | | | | | |
|  | | | | | |
| 1. 实验结果总结   （要求：写明实验的完成情况，所遇到的难点，对实验的修改建议。） | | | | | |
|  | | | | | |
| 1. 各人实验贡献与体会   （要求：每人各自撰写，每人在实验中所做的贡献度与体会。） | | | | | |
|  | | | | | |
| 1. 教师评语 | | | | | |
|  | | | | | |
| **教师评分（请填写好姓名、学号）** | | | | | |
| 姓名 | | 学号 | | 分数 | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
|  | |  | |  | |
| 教师签名：  2024年 5月 日 | | | | | |