《网络空间安全导论实践》活动要求

一、目的

本实践旨在通过第一学期网络空间安全导论课程知识的学习，掌握利用相关工具及资源，设计网络安全场景类实验，自主实验活动，以激发学生的创新实践意识，培养初步动手实现能力。

二、要求

本实践采用推荐命题与开放式自主命题相结合的方式，学生可以选择推荐命题，也可以自命题，不影响评判结果。学生需要自己搭建环境实现，不能在公网上实施攻击。

题目：

1、选取漏洞库 3 个漏洞，了解其漏洞利用原理，并还原漏洞利用场景（复杂 APT 攻击漏洞可只选择一个场景案例；如果自己挖掘的 0day 漏洞也 1 个即可，提供漏洞证书）；

2、了解 Vmware 搭建虚拟机的实现原理与使用方式，搭建 kali linux 并尝试使用其中 3 种工具。

3、了解并安装 Metasploit，学习其使用流程，利用其中的漏洞完成一次远程攻击。

4、了解网络数据包传输原理，利用 Wireshark 等抓包软件，实现某一类异常攻击数据包的抓取与分析。

5、了解数据库，SQL 语言相关应用场景，并完成一次 SQL 注入攻击。

6、了解 DNS 解析相关原理，搭建环境实现一次 DNS 劫持攻击。如可搭建一个虚假 WIFI 热点，实现虚假 DNS 解析功能或中间人攻击功能。

7、了解无线局域网 Wifi 的安全加密协议原理与流程，并尝试实现针对 WiFi 的密码分析。

8、了解二进制漏洞以及操作系统的防御手段，尝试进行一次缓冲区溢出攻击。

9、了解密码学相关概念，选择一种国产加密方式（如 SM 系列算法），以及一段需要加密的信息，完成加密与解密；或者采用数字签名算法进行签名和验签。

10、 搭建私有云实验环境，尝试复现针对虚拟机逃逸、多租户隔离等的相关的安全漏洞利用与攻击；

11、 了解网络空间安全黑产相关概念与手段，实现一次密码撞库或暴力破解攻击或密码字典生成。

12、 了解网络安全竞赛的相关种类，完成 3 道 CTF 赛题的实验环境复现、赛题分析与解答。

13、 尝试针对选定的物联网应用场景，如监控音视频摄像头、无线传感器、RFID 等，复现相应的漏洞利用；

14、 搭建一套区块链系统，并实施一种针对区块链的攻击。

15、 针对现有的某一类人工智能算法，尝试实现对抗样本攻击效果，如抗图像识别检测等。

16、 针对大语言模型进行提示注入攻击，例如目标劫持攻击、提示泄露攻击、越狱攻击等，可针对不同大语言模型进行安全测试。

17、 自主命题：自主选取与网络安全相关场景的命题并进行技术复现或设计并实现某一安全功能的工具或系统。

三、 提交形式

学生可以分组完成（每组 1-2 人），需要提交**设计报告**、**汇报 PPT** 和**展板彩页**各 1 份！

第 13-16 周（5.24 开始）安排分别进行作品汇报路演，可进行演示！

所有文件打包后统一命名，文档命名方式为：网安导论实践-姓名-题目-学号-日期（如 20240627）.doc

如为软件设计，还需提供程序源代码（请规范注释）、演示程序等；

如为场景类设计，还需提供演示视频（内容包含原理说明、环境拓扑、场景还原展示、实现效果等），视频文件控制在 10M 以内（文件过大减分）。

必要时可提供实物演示。

四、 时间要求

请于 2024 年 6 月 23 日前将作品相关材料发送到朱老师邮箱：zhuhongliang@bupt.edu.cn，如收到均会回复。若未收到回复，请联系重发。若有实物演示请提前联系予以安排。

五、评判依据

评判结果主要依据规范性（15%）、工作量（45%）、设计难度（40%）等方面。

规范性主要依据文档命名规范、文档版式（排版、布局、字体等）、认真态度等；

工作量主要依据实现的功能复杂度、代码量或场景复杂度；

设计难度主要依据新颖性、创新性、实现难度等方面。