**河南大学**

**大学生创新创业训练计划项目**

**进展报告**

**项目名称：**基于蜜罐的主动防御策略在信息安全建设中的应用

**项目级别：** 校级

**项目编号：** 20231012012

**项目负责人：** 王青松

**学 号：** 2112080140

**所在学院：** 计算机与信息工程学院

**年级专业：** 2021级 信息安全专业

**填写日期：** 2024.1.28

河南大学大学生创新创业训练计划工作领导组制

填写说明

一、项目进展报告要按照《河南大学创新性实验计划项目管理办法》的相关要求，逐项认真填写，填写内容必须实事求是，表达明确清晰。

二、**格式要求：**封面使用小三号字体，表格中使用五号字体，所填写的文字用宋体，数字及其他用Times New Roman，单倍行距。需签字部分须由相关人员用黑色钢笔或水笔签名。A4纸双面打印，左侧装订。

三、填写时根据需要，可另加附页。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | | 基于蜜罐的主动防御策略在信息安全建设中的应用 | | | | | | | | 立项年度 | | |  |
| 项目负责人 | | 王青松 | | 项目编号 | | | 20221015022 | 项目经费（元） | | | | 20000 | |
| 项目类别 | | 创新训练 | | | | | | | | | | | |
| 所属学院 | | 计算机与信息工程学院 | | | | 起止时间 | | 2023.6.1——2024.6.1 | | | | | |
| 项目组成员（含负责人） | | | | | | | | | | | | | |
| 姓名 | | 性别 | 学号 | | 所在学院、专业 | | | | 联系电话 | | E-mail | | |
| 1 | 王青松 | 男 | 2112080140 | | 计算机与信息工程学院信息安全专业 | | | | 15093605172 | | 2098781282@qq.com | | |
| 2 | 童勇超 | 男 | 2212080095 | | 计算机与信息工程学院信息安全专业 | | | | 15138210132 | | 3164647976@qq.com | | |
| 3 | 王俊豪 | 男 | 2212080174 | | 计算机与信息工程学院信息安全专业 | | | | 13262065923 | | 2381689468@qq.com | | |
| 4 | 杨仕佳 | 男 | 2212080049 | | 计算机与信息工程学院信息安全专业 | | | | 15716322763 | | s2676225006@outlook.com | | |
| 5 | 张丁 | 男 | 2212080197 | | 计算机与信息工程学院计算机科学与技术 | | | | 18135706196 | | 1501608414@qq.com | | |
| 第一指导教师 | | | | | | | | | | | | | |
| 姓名 | | 性别 | 职称 | | 所在学院 | | | | 联系电话 | | E-mail | | |
| 杨欣欣 | | 女 |  | | 计算机与信息工程学院 | | | | 15837864354 | | 359397993@qq.com | | |
| 1. **项目进展情况**（应具体阐述项目的进展程度，已完成的和未完成的具体工作、已经取得的阶段性成果等）   **已完成的工作：**  1、2023年6月份参加河南省开封市的网络安全应急演练，学会威胁情报的搜集；  2、2023年7月参加第七届“御网杯”网络安全应急演练比赛，体验基于蜜网攻击的防范技术；取得本次比赛的二等奖、三等奖若干；  3、2023年10月份参加河南大学网络安全应急演练，学会了搜集校园网的网络安全情报搜集；  4、设计和搭建了一个基于开源蜜罐软件（HFish）的实验环境，并进行了初步的功能测试；开展了一系列针对蜜罐系统的安全建设实践，包括网络配置、日志记录、警报机制等；分析和挖掘已收集到的威胁情报数据，发现攻击者的行为规律和攻击手段。  5、基于蜜罐技术对于全国各地的制定区域网站进行漏洞扫描，被横向课题“郑州赛欧思”公司所认可；  6、基于蜜罐技术的威胁情报的报告2份被“郑州赛欧思”公司所认可并接纳；  7、为了顺利搭建蜜罐的网络层搭建，同学们参加了11-12月份是“华为ICT“、”华三杯”计算机网络竞赛学习和竞赛并且取得省级奖励若干；  9、在12月份为了响应学校的学科竞赛，学院也举办了基于蜜罐技术的信息安全竞赛，本组同学取得奖项；  **未完成的工作：**   1. 蜜罐的防护能力、和利用能力需要进一步加强；   2、 分析网络安全威胁情报的能力需要进一步加强；  3、 基于蜜罐在校园网当中的应用实践需要进一步加强；  4、 学生组的论文尚未完成； | | | | | | | | | | | | | |
| **二、项目经费开支情况** | | | | | | | | | | | | | |
| **三、存在的问题及下一阶段工作安排**  存在的问题：  下一阶段工作安排：  进一步提升蜜罐系统的性能和可靠性，包括改善网络配置、加强日志分析和警报机制，以提高蜜罐系统的诱饵效果和威胁情报收集能力；  我们要深入分析已收集到的威胁情报数据，以发现更多关于攻击者的行为规律、攻击手段和攻击趋势；  针对已发现的攻击手段，我们需要进行相关的安全防御研究，并提出相应的对策和建议，以增强网络安全的防护能力；  我们计划进行针对蜜罐系统的攻防对抗演练，验证主动防御策略的有效性，并收集更多实战经验；  最后，我们将撰写论文并准备项目最终报告，总结研究成果和经验教训，提出未来的研究方向和建议。 | | | | | | | | | | | | | |
| **四、指导教师意见**  然本组同学积极参加本课题组织的相关各项活动和各阶段学习，也取得了阶段性成果，但是和我们预期的结果还有差距。尤其是我们很多基于威胁情报的大量实验是处于虚拟环境，下一步工作应该多做真实网络环境的实验。还有对于蜜罐技术的应用理解还是不够的到位，下面还需加强这一方面的学习和实践。对于威胁情报的发现能力有一定的发现技术，但是处理能力比较薄弱，还需要加强这一方面的技术。教师组的论文已经如期完成，而学生组的论文尚未成型，这仍然任重而道远。  指导教师签字： 年 月 日 | | | | | | | | | | | | | |
| **五、学院意见**  学院主管领导签字 年 月 日 学院盖章： | | | | | | | | | | | | | |