2021 年春季学期《信息安全综合实验》课程要求

崔宝江
cuibj@bupt.edu.cn
13611330827

信息安全综合实验是综合性的创新性的综合设计类实验，主要目的是使学生将三年所学内容融会贯通，学会信息安全类知识的综合运用。并且，希望学生在自己有兴趣和擅长的信息安全领域，能够自己设计并完成相应实验。

一．实验任务要求

本次综合性实验， 6-10 人为一组分组协同完成，每组任务可从如下 4 个实验中任选其一，完成实验任务要求。

（一）高安全性的私有云平台综合实验

1）参考现有云平台环境，针对安全机制的不足和缺陷，完成高安全性的私有云平台设计和搭建，使租户访问云服务时获得高安全性保障。

2）完成私有云环境的服务层、容器层、虚拟化层和 OS 层的高安全性设计，完成租户对云服务的安全登录认证、传输、信息存储的加密认证机制设计，设计高安全性的密钥交互协议、认证协议和加密存储机制。

3）收集或编写平台多类安全缺陷的检测脚本，开展安全缺陷的扫描和检测；扫描和检测高安全性的私有云平台环境，利用发现的拒绝服务类或其它类安全缺陷或漏洞，实现对安全加密认证云平台的攻击和破坏。

4）收集云服务与租户之间的流量，对加密流量进行智能检测分析，识别和分析加密流量中正常和异常流量。

5）在云平台和网络边界中部署各种安全防护和检测工具，采用行为检测拦截技术和网络流量检测拦截技术，对各类攻击进行检测，从多角度发现攻击行为，实现全面检测和清除入侵行为。

（二）智能自动渗透和攻防对抗综合实验

1）近似真实企业网络拓扑设计，搭建物理隔离的内网云环境，不少于 6 台

服务器（不同类型），不少于 2 层网络，不少于 3 层次安全环境。

2）利用多种攻击工具的组合应用，考虑物理隔离内网的突破方式，并开展内网不同安全层级服务器的智能化自动扩散和渗透，考虑自动扫描、智能扩散、攻击渗透、隐藏回传，考虑攻击行为隐藏的长期性。

3）设计内网渗透过程中的智能选择模型和算法，实现对最优攻击路径和最优渗透结果的智能选择。

4）设计全方位攻击行为检测分析工具应用和防护检测模型，实现对内网安全性的自动感知，自动识别薄弱环节，对内网中攻击行为感知后的智能自动化对抗。

（三）全功能蜜罐机制与多蜜罐管理系统综合实验

1）设计并配置支持 linux 和 windows 的蜜罐和多蜜罐管理系统，攻击者打到蜜罐，安全防护人员就能检测到攻击者 IP 与攻击者的各种动作。为减少攻击者检测到可能处于蜜罐状态，考虑高交互和仿真性以假乱真的蜜罐机制来捕获攻击者的动作与行踪。

2）蜜罐可记录任何与蜜罐访问通讯的 IP，当使用其他机器连接蜜罐，在控制系统上能看到连接蜜罐的 IP。蜜罐在空闲时能自动恢复攻击前状态，并记录蜜罐从内向外通讯的域名与 IP，具有方便易用且用户友好的控制界面。

3）探索 socks(5)代理中的 RDP/SSH 中间人攻击技术，监听流量与操作行为。通过 socks(5)代理机制，蜜罐可录制并记录 RDP 连接操作与 SSH 连接操作，通过 RDP 或 SSH 连接蜜罐进行操作并退出后，在控制系统上能有相应的操作记录。

4）设计配置一套可将多个蜜罐攻击情况进行汇总的多蜜罐控制管理系统 ，当打开多个蜜罐进行测试时，该控制管理系统可同时看到多个蜜罐的记录。

5）可参考 jtesta/ssh-mitm、GoSecure/pyrdp 等网络资料。

（四）文件和日志保护机制综合实验

1）针对多种 APT 攻击，设计和构建对文件访问和日志信息进行全面防护和收集保护的安全环境。

2）Windows 平台下，记录文件被访问时的相关信息，包括但不仅限于：时间、访问文件的进程、进程所属用户。实现打开一个文件，可对该文件的访问

记录进行详细的收集和展示（注：鼠标选中文件时也会存在访问记录)。

3）Windows 平台下，对包括 system 的不同用户的文件访问均可做到访问信息的审计和记录。建立文件访问的用户或进程黑白名单限制机制，如禁止/只允许在某用户或进程权限下才可访问。

4）设计和构建 SIEM（Security information and event management）框架，可提供对应用程序和网络硬件生成的安全日志警报的实时分析。可根据已有的 SIEM 框架(如 ELK Endpoint Security 或其他开源框架)，构建出日志信息收集和分析完整环境，包括搭建、规则设置到最后的服务器和客户端部署。要求客户端需要支持 Windows、Linux 环境，可实现日志信息的收集。在客户端所在的系统中存在风险操作时，在日志分析系统能够检测和分析。可通过自行模拟登录密码爆破等在 ATT&CK 中出现的操作，展示攻击之后在日志分析系统中可看到的相应记录。

5）可参考 AdvanceRun、apriorit/file-system-filter、EaseFilter、Elastic Security、elk-docker、ELK Endpoint Security 等网络资源。

二．实验报告要求

每组组长提交 1 个总实验报告，组长要发挥实际组织作用，并且和组员一同负责答辩。

实验报告内容要求包括以下内容：目录，小组人员分工，实验环境平台设计、关键实验技术、实验过程和实验测试结果、实验总结。

实验报告提交包含的文档：word 和 ppt 的实验报告、搭建的服务器或平台环境程序（可用下载地址代替）、安全攻防工具（可用下载地址代替）或自己编写的检测程序（含代码）、实验平台和演示的录像等。

实验演示和报告部分综合考核学生掌握基础知识、对课题分析与设计、解决复杂工程问题、方案设计与验证、团队协作与组织、课题答辩与演示等方面的能力。根据实验成果演示的成功与否，实验方案设计和实现的合理性和可行性，实验报告内容的条例性、清晰程度，实验技术的难度和功能完善性，实验方法和技术的先进性，实验的创新性，团队合理组织等方面进行评分。其中，现场演示答辩 50%，实验报告 50%。

三．实验说明

时间：2021 年 7 月 5 日—7 月 9 日

大家周一上午自行完成分组，可跨班组成组，分组名单报给各班学委，各班学委建个群接龙，最后一个班的学委汇总后发给我最终分组名单（包括序号、组长姓名学号班级、组员姓名学号班级、所选题目）。最迟可周二把分组名单发给授课老师 cuibj@bupt.edu.cn，当跨班组建组时，该组在组长所在班里显示所有组员。

组建课程群（课后建立），供大家讨论、开发、完成报告。

实验汇报时间：7 月 9 日周五上午 8：00 开始，按照 2018211801-2018211806 班,2018661801 班的顺序，按照组长学号的先后顺序介绍。每组准备约 10-20 分钟的 PPT 和相关演示。

交报告要求：详细的实验报告（电子版）周五下午每组组长 17 点前提交各班学委，各班学委 17 点前提交 cuibj@bupt.edu.cn。

实验指导老师崔宝江的联系电话：13611330827

注意：不可对实验课程中所配置的服务器之外的任何计算机进行渗透测试。

中国移动 4G 7:56

群二维码名片

2021年信息安全综合实验群

该二维码7天内(7月12日前)有效，重新进入将更新