山东大学 网络空间安全 学院

《 网络攻击与防御实践 》实验课程教学大纲

编写人：李增鹏　　审定人：

编制时间：2021 年 8 月　　审定时间：

一、课程基本信息

课程名称	**网络攻击与防御实践**				
英文名称	**Network Engineering and Defense Practice**				
课程编码	**sd04630270**				
开课单位	**网络空间安全学院**				
实验类型	□专业基础实验　□专业实验　□综合实验 □创新实验　□开放实验				
课程性质	□必修　□选修				
实验类别	□独立设课 □非独立设课				
学分	2	总学时	64	实验学时	64
适用专业	网络空间安全、信息安全				
先修课程					
课程网站					

二、课程描述

（不超过 200 字，须提供中、英文对照描述）

以网络空间安全领域的时机工程应用为主线，要求学生亲自动手，着重提高学生的问题分析能力、动手实践能力、知识运用能力和独立解决问题能力，能力挖掘学生的创新创造能力。

Taking the actual engineering application in the field of network security as the main line, students are required to focus on improving students' problem analysis ability, hands-on practical ability, knowledge application ability and independent problem-solving ability, and strive to explore students' creative creativity.

三、课程性质和教学目标

【教学目标】

《网络攻击与防御实践》是网络空间安全专业的一门专业必须课，重点讲授以主机为中心的网络攻击与防御实践的基本思想、技术和方法。本课程的特色是透过网络空间的宏观安全体系去认识网络中的攻击与实践问题。同时，本课程之一体现网络环境对网络安全的影响及对网络空间安全的支撑。

本课程透过实际案例的剖析，洞察内部技术机制。注重基本概念和基本思想，通过对安全机制的考察把握系统安全的关键技术和方法。考察身份认证机制、基础安全机制、强制安全机制和可信性检查机制等安全机制，涉及操作系统和数据库系统等关键基础软件。

通过本课程的学习和实践，使学生能够比较系统和全面地掌握计算机网络攻击与防御的基本概念、原理及技术；了解计算机网络与信息攻击与防御的主

要方法、工具的技术特点、发展和实际应用；具备较强的构建安全信息安全网络应用的能力；为今后从事计算机网络安全方面的研究和实际工作与其它专业课程的学习打下一定基础。

教学目标 1: 使学生掌握网络攻击与防御的基本概念与知识、基本原理与方法、基本框架与协议，奠定应用相关知识、原理和方法对复杂网络攻击与防御问题进行分析与设计的基本能力和思维方法。

教学目标 2: 使学生了解网络攻击与防御的关键技术、网络攻击与防御应用实施方案等，具有将其应用于针对应用领域进行设计、开发网络攻击与防御系统应用方案和技术方案的能力。

教学目标 3: 使学生在网络攻击与防御项目建设中，了解网络攻击与防御系统工程知识与方法、熟知其总体架构与协议体系，具有专业领域的表达、分析、沟通的知识和能力，并将其应用于撰写报告和设计文稿中、对相关问题清晰表达或回应。

教学目标 4: 在解决网络攻击与防御问题的过程中，能基于网络攻击与防御的工程专业相关背景知识进行合理分析，能评价网络攻击与防御工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的贡献和影响，并积极探索合理利用专业知识降低负面影响的可能性。

【教学要求】

《网络攻击与防御实践》的教学要求是给学生讲授网络攻击与防御的统一知识体系，引导学生进入网络攻击与防御知识框架的整体概貌，掌握网络攻击与防御的基础和关键技术，为学生学习密码科学与技术/网络空间安全知识、掌握密码科学与技术/网络空间安全技术，解决密码科学与技术/网络空间安全问题，及从网络空间安全与隐私增强计算等方面充实网络攻击与防御方面的知识。

本课程通过基础理论讲解和案例剖析，掌握安全两方、多方计算和高阶隐私增强计算的关键技术和方法。具体教学要求如下：

根据所授课程教学目标，填写对应支撑的毕业要求（从毕业要求 12 条中选出 3-6 条）

毕业要求	指标点	课程教学目标
1. 工程知识	具有扎实的数学、自然科学知识，系统掌握网络空间安全基本理论、专业知识及工程基础，能够将其用于解决网络空间安全领域复杂工程问题。	1.掌握经典的算法设计思想与方法、主要的设计范式，同时加深对算法数学本质的理解. 2.掌握算法分析技术,包括算法的正确性证明和时空复杂度分析.
2. 问题分析	能够应用数学、自然科学和工程科学的基本原理，准确识别、表达、并通过文献研究分析网络空间安全相关领域的复杂工程问题，以获得有效结论。	2.掌握算法分析技术,包括算法的正确性证明和时空复杂度分析.
3.设计/开发解决方案	能够应用网络空间基础理论、密码学、网络安全、系统安全、软件安全等专业知识，设计针对网络空间安全及相关领域复杂工程问题的解决方案，设计、开发、实现满足特定需求的软硬件系统、模块，并能够在设计环节中	3、能够应用算法解决复杂的具体问题，掌握算法从理论到实践的全流程,即问题建模-算法设计-算法分析-编程实现.

	体现较强的创新意识，考虑社会、健康、安全、法律、文化以及环境等因素。	
4．研究	能够基于网络空间安全及相关领域的科学原理并采用科学方法对网络空间安全领域的复杂工程问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论。	3、能够应用算法解决复杂的具体问题，掌握算法从理论到实践的全流程,即问题建模-算法设计-算法分析-编程实现.
6.工程与社会	能够基于网络空间安全工程领域相关背景知识进行合理分析，评价网络空间安全专业工程实践和复杂工程问题解决方案对社会、健康、安全、法律以及文化的影响，并理解应承担的社会责任。	3、能够应用算法解决复杂的具体问题，掌握算法从理论到实践的全流程,即问题建模-算法设计-算法分析-编程实现. 4、能够严格遵守计算机行业法律法规与职业道德规范、具备强烈社会责任感、爱国精神及团队协作精神.
8．职业规范	具备良好的人文社会科学素养、社会责任感，了解网络空间安全领域相关法律法规，能够在工程实践中理解并遵守工程职业道德和规范，履行相应的责任。	3、能够应用算法解决复杂的具体问题，掌握算法从理论到实践的全流程,即问题建模-算法设计-算法分析-编程实现. 4、能够严格遵守计算机行业法律法规与职业道德规范、具备强烈社会责任感、爱国精神及团队协作精神.
9．个人和团队	具有团队协作精神，能够在多学科背景下的团队中承担个体、团队成员以及负责人的角色。	4、能够严格遵守计算机行业法律法规与职业道德规范、具备强烈社会责任感、爱国精神及团队协作精神.

参考教材

[1] 吴礼发,洪征,李华波. 网络攻防原理与技术(第 3 版). 机械工业出版社. 2021.
[2] 张玉清. 网络安全----技术与实践. 清华大学出版社. 2011.
[3] 诸葛建伟. 网络攻防技术与实践. 电子工业出版社. 2011.
[4] 李华峰. Kali Linux 2. 网络渗透测试实践指南. 人民邮电出版社. 2020.
[3] 李亚伟. Kali Linux 无线网络渗透测试详解. 清华大学出版社. 2020.

四、课程教学内容及学时分配

第 2 章 密码学基础知识

2.1 秘密共享协议实验

【教学目标和要求】

通过实验，让学生充分理解和掌握 Shamir 秘密共享协议。

【实验环境】

(1) 平台：Windows 或 Linux。

(2) 编程语言：C、C++、Python 任选一，建议由教师指定。

(3) RSA 加密、解密函数库（由教师提供，或要求学生从互联网上搜索下载）。

【实验要求】

实验的难点和重点、实验安全和环保要求等。

⑴编程实现 Shamir 秘密共享协议，并调试通过。
⑵利用 Shamir 秘密共享协议对某一数据文件进行单次分享和重构操作。
⑶界面简洁、友好，便于操作。

2.2 可验证秘密共享 VSS 协议与公开可验证秘密共享 PVSS 协议实验

【教学目标和要求】
通过实验，让学生充分理解和掌握 VSS 和 PVSS 协议。
【实验环境】
(1) 平台：Windows 或 Linux。
(2) 编程语言：C、C++、Python 任选一，建议由教师指定。
(3) RSA 加密、解密函数库（由教师提供，或要求学生从互联网上搜索下载）。
【实验要求】
实验的难点和重点、实验安全和环保要求等。
⑴编程实现 VSS 和 PVSS 协议，并调试通过。
⑵利用 VSS 和 PVSS 协议协议对某一数据文件进行单次分享和重构操作。
⑶界面简洁、友好，便于操作。

2.3 不经意伪随机函数 OPRF 与隐私集合求交 PSI 协议实验

【教学目标和要求】
通过实验，让学生充分理解和掌握不经意伪随机函数 OPRF 与隐私集合求交 PSI 协议。
【实验环境】
(1) 平台：Windows 或 Linux。
(2) 编程语言：C、C++、Python 任选一，建议由教师指定。
(3) RSA 加密、解密函数库（由教师提供，或要求学生从互联网上搜索下载）。
【实验要求】
实验的难点和重点、实验安全和环保要求等。
⑴编程实现不经意伪随机函数 OPRF 与隐私集合求交 PSI 协议，并调试通过。
⑵利用不经意伪随机函数 OPRF 与隐私集合求交 PSI 协议，对某一数据文件进行单次进行不泄漏消息的哈希运算和集合求交操作。
⑶界面简洁、友好，便于操作。

第 3 章 网络侦察技术

3.1 站点信息查询

【教学目标和要求】
培养学生综合运用搜索引擎、Whois 数据库、DNS、社会工程学等手段对目标站点进行侦察的能力，了解站点信息查询常用的信息源及搜索工具，熟悉掌握常见搜索工具的功能及使用技巧。
【实验环境】
(1) 互联网环境。
(2) 目标域名由教师指定，建议选择有一定影响力的商业公司门户网站的域名或使用本单位门户网站域名。
【实验要求】
(1) 获得目标站点的相关信息（尽可能包含所有项）：域名服务注册信息，包括：注册商名称及 IP 地址、注册时间、域名分配的 IP 地址（段）、注册人联系信息（姓名、邮箱、电话、办公地址）；相关 IP 地址信息，如 DNS、邮件服务器、网关的 IP 地址。
(2) 站点所属机构的相关信息（尽可能包含所有项）：业务信息、主要负责人信息（姓名、邮箱、电话、办公地址、简历等）、有合作关系的单位名称及网址。
(3) 所有查询输入及结果均需截图，并写入实验报告中。

3.2 联网设备查询

【教学目标和要求】

培养学生使用搜索引擎在互联网查找特定设备的能力，熟悉联网设备搜索引擎的功能，熟练掌握设备搜索引擎的使用方法。
【实验环境】
(1) 互联网环境。
(2) 搜索引擎 ZoomEye（或 Shodan）。
(3) 搜索地域（国家、城市、区、街道、经纬度等）由教师指定或学生自主确定。
【实验要求】
(1)查找指定地域内有弱口令、可匿名登录的网络设备（路由器、网关、Server 等），并返回其 IP 地址。
(2) 查找指定地域内网络摄像头，并返回其 IP 地址。
(3)实验过程中只允许浏览搜索结果。对搜索到的可远程控制的设备，应禁止学生对这些设备进行远程控制。
(4) 所有查询输入及结果均需截图，并写入实验报告中。

第 4 章网络扫描技术

4.1 主机扫描-1

【教学目标和要求】
了解主机扫描的作用，深入理解主机扫描原理，掌握 Nmap 的使用方法，学会分析主机扫描结果。
【实验环境】
(1) 实验室环境。
(2)最新版本的网络扫描软件 Nmap（Linux 或 Windows，下载地址：http://www.insecure.org）。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 实验按 2 人一组方式进行。
(2) 安装 nmap 工具。
(3) 每个小组组员之间使用 Nmap 工具互相扫描对方主机，进行端口扫描和操作系统识别。根据扫描结果分析主机开放的端口类型和对应的服务程序，查看主机的详细信息。通过“控制面板”的“管理工具”中的“服务”配置，尝试关闭或开放目标主机上的部分服务，重新扫描，观察扫描结果的变化。扫描过程中，要求至少更改 2 次 Nmap 扫描选项进行扫描，并观察不同选项下 Nmap 扫描结果的变化。
(4) 对整个网络进行主机发现和端口扫描。
(5) 所有扫描结果均需截图，并写入实验报告中。

4.2 主机扫描-2

【教学目标和要求】
了解主机扫描的作用，深入理解主机扫描原理，掌握 Nmap 的使用方法，学会分析主机扫描结果。
【实验环境】
(1) 实验室环境。
(2)最新版本的网络扫描软件 Nmap（Linux 或 Windows，下载地址：http://www.insecure.org）。
【实验要求】
练习 1 主机发现，包括 ARP 主机发现和 NetBIOS 主机发现
练习 2 端口扫描，包括 TCP、UDP 端口扫描；
练习 3 熟悉掌握端口扫描工具，1）SATAN；2）Nessus；3）Nmap；4）X-Scan。以 Nmap 为例，掌握 Nmap 的使用，实验可按照两人一组的方式进行，也可设置两台虚拟机进行，安装 Nmap 工具后，每个小组成员之间使用 Nmap 工具互相扫描对方的主机，进行端口扫描和操作系统识别。

参考资料：

[1] https://crayon-xin.github.io/

[2] 吴礼发,洪征,李华波. 网络攻防原理与技术(第 2 版). 机械工业出版社. （参考第四章第 4.3 节端口扫描和第 4.7 节实验，Page83）
[3] 诸葛建伟. 网络攻防技术与实践. 电子工业出版社. （参考第 3.3 节网络扫描与第 3.4 节网络查点）
[4] https://crayon-xin.github.io/2018/08/12/nmap%E8%B6%85%E8%AF%A6%E7%BB%86%E4%BD%BF%E7%94%A8%E6%8C%87%E5%8D%97/。

4.3 漏洞扫描

【教学目标和要求】
了解漏洞扫描的作用，理解漏洞扫描原理，掌握 Nessus 的使用方法，学会分析漏洞扫描结果。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Linux 或 Windows 操作系统（安装 Linux 虚拟机）。
(2) 网络中配置一台预设安全漏洞的服务器作为扫描目标。
(3) 最新版本的漏洞扫描软件 Nessus（Linux，下载地址：http://www.nessus.org）。有条件的实验室可使用 Metasploit 作为漏洞扫描软件。
【实验要求】
(1) 安装 Nessus 工具的服务器端、插件库和客户端，配置 Nessus 的服务器端，确保各个 Nessus 客户端都可以连接并使用服务器端的服务。
(2) 使用 Nessus 客户端对指定服务器或主机进行漏洞扫描，得到扫描报告。
(3) 详细分析扫描报告，分析服务器可能存在的漏洞。
(4) 所有扫描结果均需截图，并写入实验报告中。

第 5 章　拒绝服务攻击

5.1 编程实现 SYN Flood DDoS 攻击

【教学目标和要求】
通过编程实现 SYN Flood 拒绝服务攻击，深入理解 SYN Flood 拒绝服务攻击的原理及其实施过程，掌握 SYN Flood 拒绝服务攻击编程技术，了解 DDoS 攻击的识别、防御方法。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Windows。
(2) 实验室网络中配置一台 Web 服务器作为攻击目标。
(3) SYN Flood 源代码（见教材 5.3.2 节）。
(4) C 语言开发环境。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 调试通过 5.3.2 节 SYN Flood 攻击源代码，将攻击源代码中的被攻击 IP 设置成实验目标服务器的 IP 地址。
(2)所有实验成员向攻击目标发起 SYN Flood 攻击。
(3) 用 Sniffer 监视攻击程序发出的数据包，观察结果。
(4) 当攻击发起后和攻击停止后，尝试访问 Web 服务器，对比观察结果。
(5) 将 Sniffer 监视结果截图，并写入实验报告中。

5.2 编程实现 NTP 反射式拒绝服务攻击

【教学目标和要求】
通过编程实现，深入理解 NTP 反射式拒绝服务攻击的原理及其实施过程，掌握 NTP 反射式拒绝服务攻击编程技术，了解 DDoS 攻击的识别、防御方法。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Windows。

(2) 实验室网络中配置一台 Web 服务器作为攻击目标，配置 2 台 NTP 服务器作为反射源（将实验学生分成两组，每组各使用一台 NTP 服务器作为反射源），并开放 monlist 请求。
(3) 编程语言自定（建议使用 Python，互联网上可查到用 Python 语言编写的 NTP 反射式拒绝服务攻击示例程序作参考）。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 编程实现 NTP 反射式 DDoS 攻击程序，并调试通过。程序的攻击目标为实验室 Web 服务器，反射源为实验室内网中指定的 NTP 服务器。
(2) 所有实验成员向攻击目标发起 NTP 反射式拒绝服务攻击。
(3) 用 Sniffer 监视攻击程序发出的数据包，观察结果。
(4) 当攻击发起后和攻击停止后，尝试访问 Web 服务器，对比观察结果。
(5) 将 Sniffer 监视结果截图，并写入实验报告中。

第 6 章 特洛伊木马

6.1 远程控制型木马的使用

【教学目标和要求】
通过实验理解远程控制型木马（或者远程控制软件）的基本原理及防范方法，掌握计算机木马（如冰河）或者远程控制软件（Quasar）的安装与使用方法。
【实验环境】
（1）实验室环境：实验主机需禁用杀毒软件和防火墙。建议在虚拟机中进行实验。
（2）开源远程控制软件 Quasar(https://github.com/quasar/Quasar)，也可以使用冰河木马进行实验（冰河木马参考实验 6.4）。
【实验要求】实验的难点和重点、实验安全和环保要求等。
（1）按 2 人一组方式组织，双方将自己的住家座位对方的控制目标（感染主机）。
（2）关闭杀毒软件和防火墙后，启动木马控制端（冰河或 Quasar）。
（3）使用木马控制端对木马程序进行配置，主要是通信配置（控制端 IP 地址和端口）、安装目录、木马功能（如键盘监听）等，然后将配置好的木马程序发送或者拷贝给对方，并让对方启动木马。
（4）启动木马控制端，并在指定网络端口上监听，在界面上观察木马上线情况。
（5）使用控制端对感染木马的主机实施远程控制，在感染主机上执行限制系统功能（如远程关机、远程重启计算机、锁定鼠标、锁定系统热键、锁定注册表等）、远程文件操作（创建、上传、下载、复制、删除文件或者目录）、注册表操作（对主键的浏览、增删、复制、重命名和对键值的读书操作等），监视感染主机屏幕、键盘输入等。
（6）清除木马，恢复杀毒软件和防火墙功能。

6.2 编程实现键盘记录功能

【教学目标和要求】
掌握木马的键盘记录功能的编程实现技术。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Windows，并安装 Python 开发环以及 Python 第三方库 PyHook。
(2) 7.2.6 节 keylogger.py 源程序。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 调试 7.2.6 节给出的 keylogger.py 程序。
(2) 运行 keylogger.py 程序。
(3) 修改 Windows 用户口令，观察 keylogger.py 程序的记录结果。
(4) 所有结果均需截图，并写入实验报告中。

6.3 编程实现截屏功能

【教学目标和要求】
掌握木马的截屏功能的编程实现技术。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Windows，并安装 Python 开发环境以及 Python 第三方库 PyWin32。
(2) 7.2.6 节 screenshot.py 源程序。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 调试 7.2.6 节给出的 screenshot.py 程序。
(2) 运行 screenshot.py 程序。
(3) 打开 C 盘根目录下的 screen.bmp，观察结果。
(4) 修改 screenshot.py，以实现实验者自定功能。
(5) 所有结果均需截图，并写入实验报告中。

6.4 远程控制型木马的使用
【教学目标和要求】
熟悉利用远程控制型木马进行网络入侵的基本步骤，分析冰河木马的工作原理，掌握常见木马的清除方法，学会使用冰河陷阱。
【实验环境】
(1) 实验室环境，所有主机需禁用杀毒软件。
(2) 冰河木马客户端程序 G_Client.exe，冰河木马服务器程序 G_Server.exe，冰河陷阱。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 实验按 2 人一组方式组织，各自实验主机作为对方的控制目标。
(2) 使用冰河客户端 G_Client.exe 对冰河服务器程序 G_Server.exe 进行配置，然后感染局域网中的某台主机。
(3) 在感染冰河木马的主机上进行检查，判断对木马的配置是否生效；主要检查项包括：木马的监听端口是否为所设置的端口；木马的安装路径是否为所设置的路径；木马进程在进程列表中所显示的名称是否与设置相符；如果为木马设置了访问口令，是否必须通过设定的口令才能够对木马实施远程控制。
(4) 在感染主机上验证冰河的文件关联功能，将木马主程序删除，打开关联的文件类型，查看木马主程序是否会被恢复。
(5) 使用冰河客户端对感染冰河的主机实施远程控制，在感染主机上执行限制系统功能（如远程关机、远程重启计算机、锁定鼠标、锁定系统热键、锁定注册表等）、远程文件操作（创建、上传、下载、复制、删除文件或目录）以及注册表操作（对主键的浏览、增删、复制、重命名和对键值的读写操作等）。
(6) 采用手工方法删除冰河木马，主要步骤包括：①检查系统文件，删除 C:\Windows\system 下的 Kernel32.exe 和 Sysexplr.exe 文件。②如果冰河木马启用开机自启动，那么会在注册表项 HKEY_LOCAL_MACHINE/software/ microsoft/windows/ CurrentVersion/Run 中扎根。检查该注册表项，如果服务器程序的名称为 KERNEL32.EXE，则存在键值 C:/windows/system/Kernel32.exe，删除该键值。③检查注册表项 HKEY_LOCAL_MACHINE/software/microsoft/ windows/CurrentVersion/Runservices，如果存在键值 C:/windows/system/ Kernel32.exe 的，也要删除。④如果木马设置了与文件相关联，例如与文本文件相关联，需要修改注册表 HKEY_CLASSES_ROOT/txtfile/shell/open/command 下的默认值，由感染木马后的值：C:/windows/system/Sysexplr.exe %1 改为正常情况下的值：C:/windows/notepad.exe %1，即可恢复 TXT 文件关联功能。完成以上步骤后，依据端口和进程判断木马是否清除。
(7) 使用冰河陷阱清除冰河木马，在此基础上，利用冰河陷阱的伪装功能来诱捕入侵者。运行冰河陷阱后，使主机系统完全模拟真正的冰河服务器程序对攻击者的控制命令进行响应，使攻击者认为感染机器仍处于他的控制之下，进而观察攻击者在主机上所进行的攻击操作。

6.5 网页木马
包括（1）木马生成、植入与功能；（2）木马删除；4 木马捆绑与隐藏；木马免杀

第 7 章 口令攻击技术

7.1 Windows 口令破解

【教学目标和要求】掌握 Windows 口令文件 SAM 的获取方法，掌握利用口令破解软件破解 Windows 口令文件的方法，深入理解口令破解原理，体会弱口令的脆弱性。

【实验环境】

(1)实验室环境，实验用机的操作系统为 Windows，实验时使用管理员帐号登录。

(2)口令破解软件 L0phtCrack5。

(3)Windows PE 启动光盘。

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1)安装口令破解软件 L0phtCrack5。

(2)破解本地主机帐户口令。

(3)破解远程主机帐户口令（可以两人一组，各自主机作为对方远程破解时的目标主机）。

(4)用 WindowsPE 启动光盘启动系统，拷出本地主机的 SAM 文件，然后正常启动系统并使用 L0phtCrack5 进行破解。

(5)将所有破解结果截图，并写入实验报告中。

7.2 文件口令破解

【教学目标和要求】

掌握 Office 文档、压缩文档、PDF 文档口令破解软件的功能及使用方法。

【实验环境】

(1)实验室环境，实验用机的操作系统为 Windows。

(2) Office 文档口令破解软件 Advanced Office Password Recovery。

(3) 压缩文档口令破解软件 Advanced Archive Password Recovery。

(4) PDF 文档口令破解软件 Advanced PDF Password Recovery。

(5) 带加密口令的 MicrosoftWord、PowerPoint、Excel 文件、RAR 文档、PDF 文件（由老师提供或学生自主创建）。

【实验要求】

实验的难点和重点、实验安全和环保要求等。

(1)分别安装口令破解软件 Advanced Office Password Recovery、Advanced Archive Password Recovery、Advanced PDF Password Recovery。

(2)破解指定 Office 文档的加密口令，要求使用破解软件提供的多种破解选项进行破解，比较不同破解方法的优劣。

(3)破解指定 RAR 文档的加密口令，要求使用破解软件提供的多种破解选项进行破解，比较不同破解方法的优劣。

(4)破解指定 PDF 文档的加密口令，要求使用破解软件提供的多种破解选项进行破解，比较不同破解方法的优劣。

(5)将所有破解结果截图，并写入实验报告中。

7.3 加密口令值破解

【教学目标和要求】

熟悉掌握在线破解网站或离线破解软件破解加密口令值的方法。

【实验环境】

(1)实验室环境，实验用机的操作系统为 Windows，可接入互联网。

(2) MD5 和 SHA1 散列值在线破解的网站 cmd5（http://www.cmd5.com/）。

(3)离线 MD5 密码暴力破解软件 MD5Crack（http://md5crack.adintr.com）。

(4)命令行版本的 SHA1 密码破解工具 Bulk SHA1（http://securityxploded.com/ bulk-sha1-password-cracker.php）。

(5)一个或多个待破解的 MD5 和 SHA1 加密口令值（老师提供或学生自主从系统的 SAM 文件中获取）。

【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 接入互联网，访问在线破解网站 cmd5，破解指定的 MD5 和 SHA1 加密口令值。
(2) 安装 MD5 密码暴力破解软件 MD5Crack，并破解指定的 MD5 加密口令值。
(3) 弹出命令窗口运行 Bulk SHA1 破解指定 SHA1 加密口令值。
(4) 将所有破解结果截图，并写入实验报告中。

7.4 在Kali中破解散列值和无线WIFI口令（802.1X和EAP协议）

【教学目标和要求】
熟悉掌握散列值和 WIFI 口令的破解方法。
【实验环境】
Kali操作系统
【实验要求】实验的难点和重点、实验安全和环保要求等。参考
1 https://blog.csdn.net/weixin_43134675/article/details/82833613
2 https://blog.csdn.net/weixin_44545251/article/details/100279827

7.5 WPA密钥破解实验（WPA/PSK无线破解原理与方法）

【教学目标和要求】
熟悉掌握 WPA 密钥破解实验。
【实验环境】
Kali操作系统
【实验要求】实验的难点和重点、实验安全和环保要求等。参考
参考 https://wenku.baidu.com/view/384d111004a1b0717ed5dd95.html

第 8 章 网络监听技术（网络嗅探与攻防对抗实践）

8.1 Wireshark 的安装与使用

【教学目标和要求】
了解 Wireshark 软件的监听原理，掌握 Wireshark 软件的使用方法，学会使用 Wireshark 软件进行数据包和协议分析。
【实验环境】
(1) 实验室环境，实验用机的操作系统为 Windows。
(2) 最新版本的 Wireshark 软件。
(3) 飞秋即时通信软件。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 安装 Wireshark、飞秋软件。
(2) 学习使用 Wireshark 软件，包含各功能菜单的作用，选项的设置等。
(3) 二人（A 和 B）一组，组员 A 和 B 启动 Wireshark 软件，设置好捕获选项，并开始捕获。注意根据情况设置好过滤器，使得尽量只捕获自己想要的那些数据包，进行以下实验过程：

a)启动飞秋，不使用飞秋进行任何操作，通过分析 Wireshark 捕获的数据包判断飞秋是否会定时发送数据包，如果发送，采用的是何种协议、何种方式？

b)组员 B 使用飞秋向组员 A 发送消息。

c)组员 A 和 B 截获数据包后，分析飞秋发送消息使用的传输层协议（UDP/TCP），并分析使用飞秋发送一条消息时的通信机制。

d)组员 B 使用飞秋的刷新功能进行刷新。

e)组员 A 和 B 截获数据包后，分析飞秋刷新时使用的传输层协议，并分析使用飞秋刷新时的通信机制。

f)组员 B 使用飞秋向组员 A 发送文件。

组员 A 和 B 截获数据包后，分析飞秋发送文件时使用的传输层协议，并分析使用飞秋发送文件时的通信机制。

(4) 将观察结果截图，并写入实验报告中。

8.2 Wireshark 工具的使用与 TCP 数据包分析

【教学目标和要求】

了解 Wireshark 软件的监听原理，掌握 Wireshark 软件的使用方法，学会使用 Wireshark 软件进行数据包和协议分析。

【实验环境】

(1) 实验室环境，实验用机的操作系统为 Windows。

(2) 最新版本的 Wireshark 软件。

(3) 飞秋即时通信软件。

【实验要求】实验的难点和重点、实验安全和环保要求等。

（1）攻击方使用 Nmap 扫描达到特定的目的。

（2）防守方使用 tcpdump 嗅探。

（3）用 Wireshark 分析，并分析出供给方的扫描目的以及每次使用的 Nmap 命令。

（4）撰写实验报告。

第 8 章 ARP 攻击部分，与网络安全实验课程重复，故不再设置实验课程。

第 9 章缓冲区溢出攻击和第 10 章 Web 网站攻击技术，与其他课程重复，故不设置实验课程。补充基于 Kali Linux 的社会工程学工具包 SET 的使用

第 9、10 章 社会工程学包及使用社会工程学包实施攻击

【教学目标和要求】

社会工程学包（Social Engineering Toolkit，SET）是一个开会员的、Python 驱动的社会工程学渗透测试工具。这套工具包由 David Kenned 设计，而且已经成为业界部署实施社会工程学攻击的标准。SET 利用人们的好奇心、信任、贪婪及一些愚蠢的错误，攻击人们自身存在的弱点。使用 SET 可以传递攻击载荷到目标系统，收集目标系统数据，创建持久后门，进行中间人攻击等。了解 SET 的原理及其重要意义，学习 SET 的配置方法，掌握 SET 实现攻击的全过程。

【实验环境】

Kali Linux

【实验要求】实验的难点和重点、实验安全和环保要求等。

1 社会工程学包启用

（1）启动社会工程学工具包

（2）传递攻击载荷 Payload 给目标系统

（3）收集目标系统的数据

（4）清除踪迹

（5）创建持久后门

2 使用 SET 实施攻击

（1）针对性钓鱼攻击向量

（2）Web 攻击向量

第 11 章　认证技术与认证协议

11.1 使用 Kerberos 实现网络身份认证

【教学目标和要求】

了解身份认证的原理及其重要意义，学习 Kerberos 的安装和配置方法，掌握和了解 Kerberos 的工作原理和实现原理，使用 Kerberos 实现身份认证的全过程。学会在 Linux 环境下配置 Kerberos 身份认证系统。并掌握在 Windows 系统中实施 Kerberos 的方法。

【实验环境】

两台安装了 Ubuntu 的主机，Kerberos 等软件。

【实验要求】实验的难点和重点、实验安全和环保要求等。

（1）安装 Kerberos，包括 NTP 安装及配置

https://github.com/whua3/Kerberos-authentication

（2）Kerberos 认证实验

（https://blog.csdn.net/w1781806162/article/details/46388387）
（3）练习基于 Kerberos 认证的 TCP 通信
（https://blog.csdn.net/eyoulc123/article/details/78542761）

11.2 Windows 认证中心的构建实验
【教学目标和要求】
了解身份认证的原理及其重要意义，掌握 Windows 2008 Server 操作系统下证书服务的设置方法，深入理解 PKI 和数字证书的工作原理。
【实验环境】实验用机的操作系统为 Windows 2008 Server。
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1) 在 Windows 2008 Server 中启用并配置证书服务。
(2) 向证书服务申请并安装数据证书。
(3) 将相关配置和申请界面截图并写入实验报告中。

11.3 使用 SSL 协议实现安全的 FTP 数据传输
【教学目标和要求】
信息一般以明文的形式在网络中传输，使用抓包软件可以成功地监听一次 FTP 登录的所有数据包，其中可以看到铭文的用户名和密码。有时需要一个安全的 FTP 访问。为此，一种通用的方法是加密 FTP 服务器和用户至今传输的数据，本实验采用 SSL 安全协议来实现数据传输的目的。
【实验环境】Windows 系统和 VMware 虚拟机下的 FTP 服务器
【实验要求】实验的难点和重点、实验安全和环保要求等。
（1）首先在虚拟机上安装 FTP 服务器软件，如 server-U。
（2）在本机上安装抓包软件 Ethereal，然后使其运行起来。
（3）使用客户端浏览器，如 IE 浏览器来访问虚拟机中的 FTP 服务器，然后用抓包软件进行查看登陆过程。
（4）我们再在本季配置成支持 SSL 的客户端，另一方配置成支持 SSL 的 FTP 服务器，然后用抓包软件进行查看登录过程。
（5）写出相近的实验报告和体会。

11.4 安全协议
【教学目标和要求】
了解身份认证的原理及其重要意义，深入理身份认证协议、密钥交换协议在网络协议中的作用。了解 SSL-安全套接层协议、SSL 记录和握手协议等安全协议，掌握这些身份认证协议的配置方法。
【实验环境】
Linux 或者 Windows
【实验要求】实验的难点和重点、实验安全和环保要求等。
（1）练习 Openssl实现单向及双向认证教程（服务端代码+客户端代码+证书生成）
https://www.cnblogs.com/Anker/p/6018032.html
https://www.cnblogs.com/lsdb/p/9391979.html

（2）练习 SSL/TLS认证的实现
参考 https://blog.csdn.net/vip97yigang/article/details/84721027?depth_1-utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-8&utm_source=distribute.pc_relevant.none-task-blog-BlogCommendFromBaidu-8

（3）练习口令认证协议 Secure Remote Protocol

（4）练习WPA3蜻蜓(Dragonfly)密钥交换协议分析
参考 https://www.anquanke.com/post/id/161793#h3-5

（5）练习OPAQUE 口令认证密钥交换协议实验

原始论文：https://eprint.iacr.org/2018/163.pdf

标准化文档：https://tools.ietf.org/html/draft-krawczyk-cfrg-opaque-00

简单说明：

https://eprint.iacr.org/eprint-bin/getfile.pl?entry=2018/163&version=20190628:192253&file=163.pdf （Page 29，Fig 9）

第 12 章 访问控制技术

12.1 Windows 访问控制策略配置实验

【教学目标和要求】

掌握 Windows 10 操作系统下不同层次访问控制策略的设置方法，理解访问控制的工作原理。

【实验环境】实验室环境，实验用机的操作系统为 Windows 7。

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1) 配置用户、用户组的访问控制策略并验证策略的有效性。

(2) 配置目录、文件的访问控制策略并验证策略的有效性。要求验证父目录、子目录、文件三层访问控制权限不一致情况下，Windows 的访问控制策略是如何处理的。

(3) 将相关配置及验证结果界面截图并写入实验报告中。

第 13 章 网络防火墙技术

13.1 Windows 内置防火墙配置实验

【教学目标和要求】

掌握 Windows 7 操作系统内置防火墙的配置方法，加深对防火墙工作原理的理解。

【实验环境】实验室环境，实验用机的操作系统为 Windows 7。有条件的学校建议使用专业防火墙进行实验。

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1) 配置 Windows 防火墙的安全策略并进行验证，要求多次变更安全策略，分析比较不同安全策略下的防护效果。

(2) 将相关配置及验证结果界面截图并写入实验报告中。

第 14 章 入侵检测技术

14.1 snort 的安装与使用

【教学目标和要求】

通过实验深入理解入侵检测系统的原理和工作方式，熟悉入侵检测工具 Snort 在 Windows 操作系统中的安装、配置及使用方法。

【实验环境】

(1) 实验室环境，实验用机的操作系统为 Windows。

(2) Windows 版本的 Snort 软件（http://www.snort.org/downloads）。

(3) WinPcap 软件（http://www.winpcap.org/install/bin/）。

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1) 安装 WinPcap 软件。

(2) 安装 snort 软件。

(3) 完善 snort 配置文件 snort.conf，包括：设置 snort 的内、外网检测范围；设置监测包含的规则。

(4) 配置 snort 规则。

(5) 尝试一些简单攻击，使用控制台查看检测结果。

(6) 将每种攻击的攻击界面、snort 检测结果截图写入实验报告中。

14.2 Metasploit 的安装与使用

【教学目标和要求】

通过实验深入理解入侵检测系统的原理和工作方式，熟悉入侵检测工具 Metasploit 在 kali Linux 的适应，以及在 Windows 操作系统中的安装、配置及使用方法。

【实验环境】实验室环境，实验用机的操作系统为 Windows。

VMware 虚拟机，Kali Linux

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1) 使用 Metasploit 进行 Windows 远程渗透攻击，如选择具有漏洞 MS08-067 的 Windows Metasploitable 靶机，或其他 MSRPC over SMB 中的漏洞

步骤 1: 启动 Metasploit 软件，根据个人喜好使用 msfconsole、msfgui、msfweb 之一；

步骤 2: 使用 exploit：windows/smb/ms08_067_netapi 渗透攻击模块；

步骤 3: 选择攻击 PAYLOAD 为远程 shell，（正向或反向连接均可）；

步骤 4: 设置渗透攻击参数（RHOST，LHOST，TARGET 等）；

步骤 5: 执行渗透攻击；

步骤 6: 查看是否正确得到 Shell，并查看获得的权限

(2)使用 Metasploit 进行 Linux 远程渗透攻击，攻击 Linux 靶机上的 Samba 服务 usermap_script 安全漏洞，获取目标 Linux 靶机的主机访问权限

步骤 1: 启动 Metasploit 软件，根据个人喜好使用 msfconsole、msfgui、msfweb 之一；

步骤 2: 使用 exploit：exploit/multi/samba/usermap_script 渗透攻击模块；

步骤 3: 选择攻击 PAYLOAD 为远程 shell，（正向或反向连接均可）；

步骤 4: 设置渗透攻击参数（RHOST，LHOST，TARGET 等）；

步骤 5: 执行渗透攻击；

步骤 6: 查看是否正确得到 Shell，并查看获得的权限

(3)使用 Metasploit 对操作系统进行攻击

(4)使用 Metasploit 对软件发起攻击

(5)使用 Metasploit 对客户端发起攻击

(6)使用 Metasploit 对 web 应用的攻击

第 15 章 高阶网络攻防练习

15.1 无线安全渗透测试

【教学目标和要求】通过实验深入理解入侵检测系统的原理和工作方式，熟悉无线安全渗透测试工具的使用。

【实验环境】

实验室环境，实验用机的操作系统为 Windows。

VMware 虚拟机，Kali Linux

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1)对路由器进行渗透测试

(2)扫描出可连接的无线网络

(3)使用 Wireshark 捕获无线信号

(4)使用 Kismet 进行网络审计

15.2 无线渗透软件练习和测试

【教学目标和要求】

通过实验深入理解入侵检测系统的原理和工作方式，熟悉无线安全渗透测试工具的使用。

【实验环境】实验室环境，实验用机的操作系统为 Windows。

VMware 虚拟机，Kali Linux

【实验要求】实验的难点和重点、实验安全和环保要求等。

(1)练习 Kismet 的使用

(2)练习 Aircrack-ng 的使用

(3)练习 Gerix wifi cracker 的使用

(4)练习 Wifite 的使用
(5)练习 Easy-Creds 的使用

15.3 数据恢复与安全删除
【教学目标和要求】
通过实验深入理解数据恢复与安全删除的原理和工作方式，熟悉数据恢复与安全删除工具的使用。
【实验环境】
实验室环境，实验用机的操作系统为 Windows。
VMware 虚拟机，Kali Linux
【实验要求】实验的难点和重点、实验安全和环保要求等。
练习使用 EasyRecovery 工具恢复已删除的文件实验
练习使用 WinHex 恢复已删除文件实验
练习使用 Eraser 安全删除文件实验

15.4 PGP 实现安全邮件通信
【教学目标和要求】
通过实验深入理解 PGP 的原理和工作方式，练习 PGP 软件的安装和配置，熟悉 PGP 在安全邮件通信等方面的使用。
【实验环境】
实验室环境，实验用机的操作系统为 Windows。
VMware 虚拟机，Kali Linux
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1)使用 PGP 软件对邮件等进行加密和签名
https://www.codenong.com/cs109088267/ /https://www.codenong.com/cs110941749/

15.5 SSH 实验
【教学目标和要求】
通过实验深入理解 SSH 的原理和工作方式，练习 PGP 软件的安装和配置，熟悉 SSH 等方面的使用。学习 OpenSSH 的相关命令及应用，了解和体验 Windows 及 Linux 环境下 SSH 的应用。
【实验环境】
SSH 服务器：Linux，装有 openSSH，wireshark，telnet，ftp
SSH 客户端：Windows 10，装有 Xshell；Linux，装有 openSSH，wireshark，telnet，ftp
【实验要求】实验的难点和重点、实验安全和环保要求等。
(1)实验准备，服务器和客户端 IP 确认，账号新增
(2)SSH 登录，Linux 下口令登录&密钥登录，Windows 下口令登录&密钥登录
(3)SSH 应用，端口转发，比较分析

五、每年更新实验项目

（按照教育部实验教学要求，每年实验教学更新项目不少于 20%）

六、实验教学要求对应关系

	教学要求 1	教学要求 2	教学要求 3		
实验 1	X		X		
实验 2		X			
实验 3			X		
实验 4	X		X		

实验 5		X			
实验 6			X		
实验 7	X		X		
实验 8		X			
实验 9			X		
实验 10	X		X		
实验 11		X			
实验 12			X		
实验 13	X		X		
实验 14		X			
实验 15			X		

七、考核及成绩评定方式

【考核内容】预习+操作+结果+报告+期末考试（理论考试+操作考试）
【成绩评定】日常实验占 50%，实验报告占 50%.

八、教材及参考书目

【教材】编著者，教材名，出版社，出版年，教材类别（是否规划、获奖教材？）
[1]吴礼发，洪征，李华波编著.网络攻防原理与技术（第 2 版），机械工业出版社，2017 年，十三五国家重点出版物出版规划项目
[2]张玉清. 网络攻击与防御技术. 清华大学出版社，2014，普通高等教育“十一五”国家级规划教材
[3] 王群. 网络攻击与防御技术.清华大学出版社。
【参考书】3-5 本相关的教材或者专著、杂志或网络资源
[1]网络安全中机器学习大合集 https://github.com/jivoi/awesome-ml-for-cybersecurity
[2] 李华峰. Kali Linux 2. 网络渗透测试实践指南. 人民邮电出版社. 2020.
[3] 李亚伟. Kali Linux 无线网络渗透测试详解. 清华大学出版社. 2020.