现代学徒制课程标准基本框架

网络渗透与防御技术课程标准

企业：蓝盾信息安全技术股份有限公司

学校：广东工贸职业技术学院

一、课程名称

网络渗透与防御技术

二、适用专业及面向岗位

适用于信息安全管理专业，网络技术专业。面向渗透测试工程师、信息安全工程师、安全咨询服务工程师等工作岗位。可以具备具备一定的风险分析、防病毒和安全策略制定的能力，熟悉渗透测试的各类技术及方法，掌握各种渗透测试工具，安全知识技术技能和攻防手段，承担信息安全监控与防护工作。

三、课程性质

网络渗透与防御技术是高职信息安全技术专业的专业核心课程，也是一门重要的职业专门能力课程。其目标是培养学生掌握防护各种网络攻击的方法，技术和工具，具备解决现实环境中网络安全突发事故的应对能力。

信息安全攻击与防护的先修课程包括计算机网络基础、信息安全技术基础、网络互联设备配置，是网络安全综合项目训练、信息安全等级保护等课程的学习基础。本课程基于高职学生“双证书”要求，融合了全国信息技术水平考试“计算机网络信息安全工程师”相应的知识和技能。

本课程是一门实践性和应用性较强的课程。

四、课程设计

本课程是主要在机房内进行教学，通过模拟平台，着重体现理论和实践的结合，并根据现代学徒制的教学设计由企业与学校共同完成。

本课程遵循能力核心、系统培养，以行业专家分析的职业能力为逻辑起点，依据教育专家界定的职业能力设计课程内容，发挥校企结合优势，。

网络攻击与防护课程首先让学生对网络安全攻击与防护有初步的认识，其次从网络安全概述、信息收集技术、漏洞扫描技术、漏洞利用技术、权限提升技术、状态维持与隐藏技术、密码破解技术、网络攻击技术、蜜罐和密网技术、网络安全综合防范平台等方面，让学生分别了解和理解相应的网络攻防内容和运行机制，掌握网络渗透与防御的方法、工具和技能，培养增强网络安全的防护能力。

在教学过程中，采用项目式任务式，充分发挥教学平台的作用，以学生自主学习为主、教师辅导为辅。

将网络安全评估 1+X 证书相关考试内容融合到本课程中，鼓励学生考取证书。并组织学生参加省信息安全管理与评估等等比赛。

五、课程教学目标

1．方法能力目标

(1) 具备描述信息安全技术的交流表达能力；

(2) 具备解释信息安全攻击与防护原理的能力；

(3) 具备分析问题和解决问题的能力；

(4) 具备信息收集、分析与处理的能力；

2．社会能力目标

(1) 培养学生诚实、守信、坚忍不拔的性格；

(2) 培养学生的安全意识、责任意识与爱国情怀；

(3) 培养团队精神与合作能力；

(4) 培训学生勇于创新、爱岗敬业的工作作风；

3．专业能力目标

(1) 能描述常见的网络渗透攻击方式；

(2) 能运用工具实现信息收集、漏洞扫描；

(3) 能运用工具实现漏洞利用；

(4) 能运用工具软件实现权限提升；

(5) 能识别恶意木马及对恶意木马进行查杀

(6) 能运用工具软件实现网络身份的欺骗。

(7) 能对搭建网络安全综合防范平台。

六、参考学时与学分

课程共计 64 课时，其中实践课 32，学分 3.5。

七、课程结构

表 7-1 课程结构表

序号	学习任务（单元、模块）	对接典型工作任务及职业能力要求	知识、技能、态度要求	教学活动 设计（与工作任务相融合）	学时
1	网络安全概述	了解网络安全理论和现状，掌握常见的网络命令。 能描述常见的网络渗透攻击方式，培养学生的安全意识、责任意识，分析问题和解决问题的能力	掌握网络安全理论基础 了解网络安全现状 理解常见的网络命令 了解网络安全存在的威胁 黑客攻击五部曲介绍 重要知识点：常见网络命令	常见网络命令的使用 分析网络安全的威胁 实验录屏：常见网络命令的使用（ifconfig 等网络命令的使用、基本网络配置）	2 课时
2	信息收集技术	掌握信息收集的原理、作用方法，掌握常见工具的使用。	了解信息收集的作用 理解快速定位、信息枚举、定点	dnsenum，Fierce 工具的应用 nmap 工具的应用 Whois、dig 的应用 Dmitry 工具的应用	4 课时

		锻炼信息收集、分析与处理的能力，用工具实现信息收集能力，实、守信、坚忍不拔的性格，安全意识	挖掘、漏洞查询等信息收集的方法 了解信息收集的防范措施 重要知识点一：信息收集的作用与防范	dirbuster 工具的应用 pOf 工具的应用 实验录屏 1： dnsenum，Fierce 工具的应用 实验录屏 2：nmap 工具的应用 实验录屏 3：Whois、dig 的应用 实验录屏 4：Dmitry 工具的应用 实验录屏 5：dirbuster 工具的应用 实验录屏 6：pOf 工具的应用	
3	漏洞扫描技术	熟练掌握漏洞扫描的工具、方法和防范措施。 锻炼分析问题和解决问题的能力、运用工具实现信息收集、漏洞扫描能力、培养诚实、守信、勇于创新、爱岗敬业的精神。	了解漏洞扫描的常用方法 了解漏洞扫描工具及使用 理解漏洞扫描的防范措施 重要知识点一：漏洞扫描原理与防范	漏洞扫描工具 Nessus 的使用 漏洞扫描工 OWAS_ZAP 的使用 漏洞扫描工具 Nikto 的使用 实验录屏 1：漏洞扫描工具 Nessus 的使用 实验录屏 2：漏洞扫描工具 OWAS_ZAP 的使用 实验录屏 3：漏洞扫描工具 Nikto 的使用	4 课时
4	漏洞利用技术	熟练掌握漏洞利用的工具、方法和防范措施。 锻炼分析问题	了解漏洞利用的常用方法 了解漏洞利用工具及使用 理解漏洞利用的防范措施	Msfconsole 渗透攻击 MySQL 数据库、PostgreSQL 数据库服务 Msfconsole 渗透攻击 Tomcat 服务 Msfconsole 渗透攻击 Samba	8 课时

		和解决问题的能力、运用工具实现信息收集、漏洞利用能力、培养诚实、守信、勇于创新、爱岗敬业的精神。	重要知识点一：漏洞利用基础（漏洞利用常用方法介绍、防范措施 Metasploit 基础、Metasploitable 操作系统介绍） 重要知识点二：MSF 渗透测试框架的使用 重要知识点三：Windows 操作系统漏洞利用	服务 利用 borwser_autopwn 渗透模块攻击浏览器 微软操作系统漏洞利用 实验录屏 1：利用 MSFCONSOLE 进行渗透攻击 实验录屏 2：利用 Metasploit 的图形管理工具 Armitage 攻击目标系统 实验录屏 3：Msfconsole 渗透攻击 MySQL 数据库服务 、PostgreSQL 数据库服务 实验录屏 4：Msfconsole 渗透攻击 Samba 服务 实验录屏 5：Msfconsole 渗透攻击 Tomcat 服务 实验录屏 6：利用 borwser_autopwn 渗透模块攻击浏览器 实验录屏 7：MS08-067 漏洞渗透及利用 实验录屏 8：MS12-020 漏洞利用 实验录屏 9：MS17-010 漏洞渗透及利用	
5	权限提升技术	熟练掌握权限提升的过程、方法和防范措施。 锻炼分析问题和解决问题的能力、工具软件实现权限提升能力、培养诚实、守信、勇于创新、爱岗敬业的精	了解解权限提升的过程 理解权限提升的方法 理解权限提升的防范措施 重要知识点一：MS09-012 提权 实验录屏：MS09-012 提权 重要知识点二：	MS09-012 提权 字体库提权 Linux 提权 存储过程提权 实验录屏 1：Linux 提权 实验录屏 2：存储过程提权	4 课时

		神。	字体库提权 实验录屏：字体库提权 重要知识点三：Linux 提权 重要知识点四：存储过程提权		
6	状态维持与隐藏技术	掌握网络攻击和控制，木马的查杀和防御方法。 锻炼识别恶意木马及对恶意木马进行查杀的能力，分析问题和解决问题的能力、、培养诚实、守信、勇于创新、爱岗敬业的精神	网络攻击的介绍 网络痕迹的讲解 网站控制的维持（后门、木马） Rootkit 木马应用 木马的查杀与防御 重要知识点一：网站控制的维持 重要知识点二：Rootkit 木马应用 重要知识点三：木马查杀与防御	网站控制的维持 Rootkit 木马应用 木马查杀与防御 实验录屏 1：网站控制的维持 实验录屏 2：Rootkit 木马应用 实验录屏 3：木马查杀与防御	4 课时
7	密码破解技术	掌握密码破解和无线破解的过程。 锻学习能力、解决问题能力、新能力，提高安全意识。	密码破解介绍 密码破解演练 无线安全讲解--无线破解演示 重要知识点一：RAR 密码破解 重要知识点二：office 密码破解 重要知识点三：	密码破解演练 无线破解演示 实验录屏 1：RAR 密码破解 实验录屏 2：office 密码破解 实验录屏 3：操作系统密码破解 实验录屏 4：无线破解演示	4 课时

			操作系统密码破解 重要知识点四：无线破解演示		
8	网络攻击技术	掌握网络攻击技术 锻炼运用工具软件实现网络身份的欺骗开发能力、学习能力、解决问题能力、团队合作能力、创新能力，提高信息安全意识。	网络攻击介绍 ARP 欺骗演练 拒绝服务攻击原理 拒绝服务攻击实现手段 拒绝服务攻击攻防 重要知识点一：ARP 欺骗演练 重要知识点二：SYN flood 攻击 重要知识点三：CC 攻击	ARP 欺骗演练 SYN flood 攻击 CC 攻击 实验录屏 1：ARP 欺骗演练 实验录屏 2：SYN flood 攻击 实验录屏 3：CC 攻击	4 课时
9	蜜罐和密网技术	了解蜜罐蜜网，提高信息安全意识。	蜜罐和密网的介绍 蜜罐和密网部署方式介绍	理论教学	2 课时
10	网络安全综合防范平台	掌握网络安全综合防范平台的搭建和分析方法。 掌握搭建网络安全综合防范平台的能力，学习能力、解决问题能力、团队	网络安全综合防范平台作用的介绍 网络数据采集软件：Splunk 介绍 Splunk 的搭建与分析 重要知识点一：Splunk 的搭建与	Splunk 的搭建与分析 实验录屏：Splunk 的搭建与分析	4 课时

		合作能力、创新能力，提高信息安全意识。	分析		
11	综合项目实训	通过企业相关的实际案例实训，锻炼学生综合能力，自主学习能力、解决问题能力、团队合作能力、创新能力。	完成如下的实训项目： 1、主动侦查方法及工具应用 2、被动侦查的方法及工具应用 3 、 Nmap 和 Nessus 扫描工具的应用 4、Metasploit 漏洞利用框架学习 5、密码破解技术与应用 6、ARP DNS 中间人网络攻击应用 7、蜜罐和密网技术应用 8、权限提升技术 9、状态维持与隐藏技术	1、完成主动侦查方法及工具应用项目实训 2、完成被动侦查的方法及工具应用项目实训 3、完成 Nmap 和 Nessus 扫描工具的应用项目实训 4、完成 Metasploit 漏洞利用框架学习项目实训 5、完成密码破解技术与应用项目实训 6、完成 ARP DNS 中间人网络攻击应用项目实训 7、完成蜜罐和密网技术应用项目实训 8、完成权限提升技术项目实训 9、完成状态维持与隐藏技术项目实训	24 课时
合计					64 学时

八、资源开发与利用

（一）教材编写与使用

建议使用教材：

1、《Kali Linux 高级渗透测试》 ISBN:9787111593065 机械工业出版社

2、《从实践中学习 Kali Linux 渗透测试》 ISBN：9787111632580 机械工业出版社

教材选取过程中应满足以下要求：

1、教程需与本课程标匹配

2、教材应充分体现任务导向实践引领的课程设计思想，按照重要知识点和技能点的不同分解为不同的学习情景。

3、教程应能充分反映最新的企业实践新成果，吸纳更新重要知识点和技能点，使教材具有先进性，职业性和指导性。

4、教材内容，要强化技能点的培养和重要知识点的应用。

5、教材表达必须精炼准确，科学。

（二）数字化资源开发与利用

1、校企合作开发数字化资源平台：现代学徒制学习资源及测评综合管理系统

https://jsjxyxtz.gdgm.cn/static/pc/managesystem/dist/index.html#/login。

2、教师上课课件、视频、学习指南、PPT 讲稿、习题、测试资料

（三）企业岗位培养资源的开发与利用

1、充分利用我院和蓝盾信息安全技术股份有限公司合作企业的优势，在真实的工作环境中突出工学结合，选择典型的企业项目案例为实训任务，实现实训与生产相结合。

2、企业和学校的双导师相互配合，利用校企合作开发的资源平台，建立好课前-课中-课后的一系列教学服务，做好课前预习，课中讲解，课后跟踪的课内外指导和辅导，扩展课外教学形式。

3、利用蓝盾信息安全技术股份有限公司及其相关合作单位作为校外实训基地，发挥现代学徒制办学的优势，通过生产性实训提升学生的职业素养和职业能力。

4、通过多渠道的资源共享，为学生提供更加完备的参考资料。并组织校企老师协作，不断完善数字化资源平台。以网络课程为平台积极开发数字化教学资源

包括课程标准、课件、习题、案例库、实训环境构建、实训指导书等数字资源；教学视频、教学动画、微课等视频资源。并建立互动交流网络平台。

九、教学建议

建议本课程重视学生在校学习与实际工作的一致性，采取实际案例设计学习场景，采用任务驱动项目导向的教学模式。重视培养学生信息安全也意识、职业道德的培养和严肃认真的学习态度。通过本课程的学习，还应该使学生具备自主学习、持续学习的能力，关注新技术和行业发展，以便适应发展变化迅速的信息安全领域的需求。

十、课程实施条件

1、师资条件：具备一支优秀的校企结合教学团队，目前本专业的要求和现代学徒制教学的特点，需确保学习领域课程实施，保证教学质量。团队成员由校内专任教师和企业导师组成，专任教师需具备硕士学历、讲师以上职称；企业导师（师傅）由企业人员担任，需具备网络渗透的实际工作经验，并具备良好的授课沟通能力。

2、实训条件：本课程是一门实践性很强的操作课程，建议全部课程安排在机房上课。企业需要提供比较先进的校外实训基地，配置好模拟平台，氛围符合企业真实环境。

十一、教学评价

为了全面考核学生的知识与技能掌握情况，本课程主要通过以过程考核和成果评价考核相结合的方式，课程考核涵盖项目(学习情景)任务全过程，并着重于综合能力的检测。

注：各项目考核过程需要注意考核工作与职业操作，学习态度，团队合作精神，交流及表达能力，组织协调能力等内容。

撰稿人：蓝盾信息安全技术股份有限公司　胡韶峰

广东工贸职业技术学院　　高学勤