**附件1：**

**“网络安全与数据恢复学习”培训班课程大纲**

|  |  |  |  |
| --- | --- | --- | --- |
| 时间 | 课程 | 内容 | 演示和实验 |
| 第一天上午 | 信息安全背景与发展态势 | * 2014.2.27国家信息安全领导小组
* 2015.315晚会与绵羊墙？
* APT与0day
* AET高级逃逸技术
* 云、大数据、物联网、工控、移动安全挑战
* 信息安全的背景、概念和特性
* 2014典型安全事件与安全漏洞总结
* 网络攻击的步骤和典型的攻击方式
* 各类典型攻防技术概述
* 黑客各种网络踩点特征分析和防范措施
* 端口扫描技术
* 漏洞扫描技术
* 渗透测试实践
* 虚拟机的使用技巧
 | * 心脏出血的演示与修复
* 破壳漏洞、贵宾犬漏洞、幽灵漏洞介绍
* 虚拟机的使用
* 攻防常用命令
* 信息获取，Banner识别
* 网段探测，IpScan
* 端口扫描，Nmap、SuperScan
* 漏洞扫描，Nessus、OpenVAS
 |
| 第一天下午 | 网络安全常见威胁和防御措施 | * 各类口令破解技术与应对措施
* 缓冲区溢出攻击与防御
* 提权的艺术
* 嗅探和欺骗技术解析
* ARP欺骗、ARP病毒、DNS域名劫持、DNS欺骗等攻击
* 网络钓鱼原理和检测分析
* DDOS攻击原理与防御
* 社会工程学—欺骗的艺术
 | * 密码生成器与字典生成器
* 被忽视的隐私--缓存密码
* Windows、Unix系统口令安全
* 神器Mimikatz
* Office、rar、pdf等文档安全
* 第三方应用口令安全，比如FTP、foxmail、思科设备密码
* 散列的破解
* 数据库口令安全
* 系统溢出，Linux内核溢出
* 第三方应用溢出
* 系统漏洞提权
* Serv-U提权
 |
| 第二天上午 | 计算机病毒木马的威胁与防治 | * 计算机病毒机制与组成结构
* 恶意代码传播和入侵手段全面汇总
* 恶意代码传播和感染发现手段
* 高隐藏性植入代码的检测机制
* 深入监测恶意代码行为的方法
* 病毒的高级手工查杀技术和思路
* 检测监控恶意代码的异常手段汇总
* 病毒传播和扩散最新技术分析
* 杀毒软件无法查杀的病毒原理分析
* 自毁灭木马痕迹的发现技术
 | * 盗号程序、后门账号、Shift后门、注册表后门、NTFS文件流
* 键盘记录、U盘小偷
* 病毒感染与手动清除实验，灰鸽子和Gh0st木马，文件夹病毒的清除
* 借助工具软件进行病毒的分析及排查（涉及的工具软件：IceSword、Rootkit Unhooker、Xuetr、ProcessExplorer）
 |
| 第二天下午 | Web安全 | * OWASP TOP 10介绍
* 常见Web安全漏洞
* SQL注入的原理和对策
* XSS跨站脚本攻击与cookie欺骗
* CSRF攻击介绍
* 网页挂马与WebShell
* 上传漏洞
* Web后台的爆破
* 旁注等其他Web攻击方式
* Web安全工具演示
* Web安全防御措施
 | * 典型Web漏洞的利用
* 利用SQL注入进入Web后台
* 注入点和Web后台的扫描
* 修复SQL注入漏洞
* 利用XSS获取管理员权限
* 利用CSRF修改管理员口令
* Webshell的上传
* 利用IE漏洞挂马
* 最小后门--一句话木马
* 爆破海蜘蛛软路由的后台
* 旁注演示
* Web安全类工具演示
 |
| 第三天上午 | 主机操作系统和应用服务器安全加固 | * Windows Server 2008安全
* Windows备份和还原
* II7安全配置
* 用户账户控制UAC
* ServerCore内核模式
* RODC只读域控制器
* 网络访问保护NAP实践
* 网络策略服务器
* 微软补丁服务器WSUS
* 微软基准安全分析器MBSA实践
* SpotLight服务器性能监视
 | * UAC用户权限控制
* Windows备份与还原
* IIS7安全加固
* 安装ServerCore内核
* 配置RODC
* NAP架构NAP的原理
* IPSEC和802.1x的NAP
* 微软WSUS实践
* MBSA基线安全扫描
* Spotlight监视服务器性能
 |
| 第三天上午 | 网络安全架构设计和网络安全设备的部署 | * 网络架构安全基础
* 网络安全规划实践
* 路由交换等设备安全
* 安全架构的设计与安全产品的部署
* 漏洞扫描设备的配置与部署
* 内网安全监控和审计系统的配置
* 网络安全设备部署
* 防火墙、防水墙、WEB防火墙部署
* 入侵检测、入侵防御、防病毒部署
* 统一威胁管理UTM部署
* 安全运营中心SOC
 | * 网络安全规划实践
* 路由安全和交换安全，模拟环境：PacketTracer或GNS3
* 发动DTP的攻击、DTP攻击的防范
* ARP攻击、防范交换机上ARP的攻击
* 防火墙部署
* IDS、IPS部署实例
* UTM、SOC等网络安全设备的部署实例
 |
| 第三天下午 | 灾难备份与业务连续性、风险评估方法与工具以及应急响应 | * ISO27001管理体系实践
* 企业ISO27001建立过程与策略
* 业务连续性管理的特点
* 业务连续性管理程序
* 业务连续性和影响分析
* 编写和实施连续性计划
* 业务连续性计划的检查维护重新分析
* ITIL V3概述
* 建立企业总体应急预案及部门预案
* 等级保护概述
 | * 风险评估软件安全检测操作
* MBSA&MRAST评估小型企业安全案例
* 某OA系统风险评估实例
* 风险评估等级保护实例演示
 |
| 第三天下午 | 无线安全 | * 无线安全的背景
* WLAN技术和802.11标准
* 无线网络的五大安全隐患
* WEP和WPA的原理与缺陷
* 无线网络如何做安全加固
* 实验---破解无线网络密码，针对WEP和WPA/WPA2两种情况进行演示
* 实验---加固无线AP
 | * 无线AP的加固实验
* 破解WEP加密的无线网络
* 破解WPA/WPA2加密的无线网络
 |
| 第三天下午 | 恢复丢失的数据，数据恢复实例 | * 数据恢复的前提条件和恢复的概率
* 恢复已格式化的分区
* 手工恢复FAT和NTFS磁盘格式的文件
* 利用工具恢复已经删除的文件
* 分析处理因文件系统被破坏造成的数据损坏
* 常见文件系统被破坏的现象原因与处理方法
 | * 格式化分区的数据恢复
* NTFS文件系统的删除及格式化原理及恢复方法
* 使用Easy recovery、Final data、R-Studio找回丢失的数据
* Diskgen找回丢失的分区
* Winhex恢复删除FAT分区
 |
| 附加课程 | DNS安全个人日常安全泄密途径灾难备份与业务持续性管理应急响应 | * DNS协议原理、协议安全、bind部署与安全加固、DNS欺骗、DNS放大攻击等
* 个人PC的加固、提升员工自我安全意识
* 总结出的九大泄密途径，有针对性的进行网络安全加固
* 灾备
* 应急响应
 | * 根据学员实际情况和时间灵活调整内容
 |

**附件2：**

**“网络安全与数据恢复学习”培训班报名回执表**

|  |  |
| --- | --- |
| 单位名称 |  |
| 详细地址 |  | 联系人 |  |
| 电话 |  |  传真 |  | 邮箱 |  |
| 姓名 | 性别 | 部门/职务 | 电话 | 手机 | 邮箱 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 户 名：软博时代（北京）科技有限公司开 户 行：招商银行北京陶然亭支行帐 号：110914587710501户 名：中联软博（北京）科技有限公司开 户 行：中国工商银行北京中关村支行账 号：0200095609200088230 | 参会单位签字或盖章 |

请于9月30日前发送邮件至协会秘书处，开班前一周我们将发送报到通知，届时请注意查收。

联系人：叶馨，电话：66311548，传真：020-66311543，邮箱：gzhea@vip.163.com。