马士兵教育
www.mashibing.com

网络安全大师课 2.0版

2022年最新课程简章

V2022.2

复合全能人才培养 / 一站式知识服务提供商 / 品牌保障

第一部分：基础与准备

1.1. 网络安全行业与法规

- 网络安全是什么?
- 信息系统安全三要素
- 网络空间安全
- 网络安全常用术语介绍
- 网络安全实施威胁地图
- 网络安全事件分类
- 2021年安全大事件盘点
- 网络安全与各行各业的关系
- 中国网络安全行业全景
- 中国网络安全人才需求
- 中国知名网络安全公司
- 网络安全就业岗位与薪资
- 《计算机信息系统安全保护条例》（147号令）
- 《国际联网安全保护管理办法》
- 《网络安全法》
- 《网络安全审查办法》
- 《密码法》
- 《数据安全法》
- 《互联网安全产品漏洞管理规定》
- 《个人信息保护法》
- 网络安全国家标准与行业标准
- 课程设计思路
- 官网学习平台功能（学习、提问、靶场）介绍
- 如何高效地学习网络安全课程

1.2. Linux操作系统

- 操作系统发展历史与Linux
- 安装VMWare软件
- VMWare常用操作
- VMWare克隆和快照功能
- 安装和配置CentOS 7
- 为虚拟机配置静态IP

- CentOS安装软件的方式
- Linux操作系统目录结构
- Linux命令格式
- Linux文件和目录操作命令
- Linux用户和用户组操作命令
- Linux查看和操作文件内容命令
- Linux文件压缩和解压缩命令
- Linux网络管理命令
- Linux磁盘管理和系统状态命令
- Linux安装软件
- Linux安全加固

1.3. 计算机网络基础

- 计算机网络在信息时代中的作用
- 因特网发展的三个阶段
- 因特网边缘部分介绍
- 因特网核心部分介绍
- 计算机网络的分类之按照作用范围分类
- 计算机网络的分类之按线路结构进行分类
- 网络性能指标之速率
- 网络性能指标之带宽和吞吐量
- 网络性能指标之时延
- 网络性能指标之往返时间
- 网络性能指标之利用率和丢包率
- 常用的计算机网络体系结构
- 物理层
- 数据链路层在网络体系结构中所处的地位
- 封装成帧
- 透明传输
- 差错检测
- 以太网的基本概念
- MAC地址
- MAC地址的识别
- 以太网交换机自学习和转发帧的流程
- 以太网交换机的生成树协议STP
- 虚拟局域网VLAN
- 网络层概述
- IPv4地址概述

- IPv4地址的分类
- IP地址习题讲解
- 子网的划分方法
- IP协议概述
- IP数据报的发送和转发过程
- 路由表概述
- 路由表的类型
- 思科gest登陆方式
- 路由表实验
- ARP高速缓存表
- 特殊IP地址
- 运输层概述
- 端口号
- TCP协议的首部
- TCP连接的建立
- TCP 四次挥手
- TCP 可靠性传输的实现
- 用数据报协议UDP概述
- TCP和UDP的区别
- 应用层概述
- 万维网概述
- HTTP协议
- Wireshark的基本使用
- Wireshark过滤器
- 使用Wireshark分析TCP三次握手

1.4. HTML基础

- HTML简介和发展史
- 开发工具的使用
- HTML5骨架
- HTML基本语法
- HTML常用标签
- HTML标签的基本使用（有序和无序列表）
- HTML标签的基本使用-表格
- HTML标签的基本使用-form表单
- HTML布局常用标签-div和span

1.5. JavaScript基础

- JavaScript简介
- JavaScript用途
- JavaScript组成
- 数字类型字面量
- 变量基本使用
- 变量提升
- 类型检测
- 数学运算
- 比较运算
- 逻辑运算
- if语句
- switch基础应用
- 嵌套循环
- break，continue while do while
- 函数认知
- 函数基本使用
- 局部变量
- 作用域
- return关键字
- 函数实战应用
- 回调
- 递归
- 函数自执行
- 数组
- 堆栈空间
- 正则表达式概述
- 正则使用技巧
- 正则字符集
- 正则边界符
- arguments
- 闭包
- DOM认识
- DOM方法
- 操作节点属性
- 操作节点样式
- 节点事件

1.6. PHP入门

- PHP简介与开发环境搭建
- PHP基本语法
- PHP变量与变量作用域
- 常量与数据类型
- 数据类型之复合类型
- 数据类型之特殊类型
- PHP运算符
- PHP流程控制
- superglobals 超全局变量
- PHP+Bootstrap 实现表单校验功能
- PHP+MySQL实现用户登录和注册功能

1.7. MySQL基础

- 数据库介绍：分类、安装、配置、登录、连接等
- 数据库基本操作：创建、查看、选中、查库表、删除数据库等相关命令行操作
- 数据字段操作：创建调整字段顺序排序删除等字段命令行操作
- 数据库表操作：创建选中删除数据库表等相关个命令行操作
- 数据类型：整型、浮点、字符、时间、符合型等
- 增删改查之更新记录、数据库权限操作
- 函数、分组查询、多表关联查询、子查询
- 索引、外键、约束、事务、存储过程、触发器

1.8. Python编程

- Python 介绍以及应用场景
- Python的安装
- 第一个Python程序
- PyCharm的安装
- Python入门
- 变量练习题
- 字符串
- 分支语句
- 字符串分支语句练习题
- 列表
- 循环
- 元组

- 数组循环练习题
- 字典
- 函数
- 包和模块
- 类和对象

第二部分：渗透与攻防

2.1. SQL注入漏洞的渗透与防御

- 数据库基础
- 什么是SQL注入
- 产生SQL注入的原理
- SQL注入带来的危害有哪些
- GET型SQL注入漏洞是什么
- GET型SQL注入演示
- 工具以及靶场介绍
- POST注入是什么
- POST注入演示
- 判断SQL注入点
- 回归测试
- 注入类型
- Time-based基于时间的盲注
- Time-based基于时间的盲注注入手工演示
- Time-based基于时间的盲注注入脚本演示
- Time-based基于时间的盲注注入练习
- 基于User-Agent注入
- 基于User-Agent注入演示
- 基于User-Agent注入练习
- Error-based基于报错注入
- Error-based floor()基于报错注入演示
- Error-based extractvalue()基于报错注入演示
- 配合Burp Suite注入演示
- stacked queries基于堆叠注入
- stacked queries基于堆叠注入演示
- Bypass混淆绕过
- Bypass WAF绕过
- sqlmap的使用
- sqlmap原理以及源码阅读
- sqlmap实战1-COOKIE注入
- sqlmap实战2-USER-AGENT注入
- sqlmap实战3-手动注入与sqlmap对比
- sqlmap实战4-脱库

- sqlmap高级应用
- 如何防御SQL注入

2.2. XSS漏洞相关渗透与防御

- HTTP协议回顾
- Cookie和Session的作用
- XSS基本概念和原理介绍
- 反射型XSS和储存型XSS
- XSS获取Cookie
- XSS钓鱼获取用户密码
- XSS获取键盘记录
- XSS平台搭建xss-platform
- Kali beef-xss
- XSS漏洞检测和利用
- XSS防御与绕过
- XSS小游戏靶场解题思路

2.3. 文件上传漏洞渗透与防御

- 文件上传代码实现
- 文件上传常见场景
- 文件上传漏洞原理
- Webshell介绍
- 网站控制工具：蚁剑、冰蝎、哥斯拉
- 漏洞带来的危害有哪些
- 工具以及靶场安装介绍
- 上传文件代码函数原理&上传图片拦截
- 后缀客户端验证-JS禁用&BURP改包&本地提交
- 后缀黑名单验证-大小写&加空格&符号点&::$DATA
- 后缀白名单验证-MIME修改&%00截断&0X00截断
- 文件头变异验证-验证MIME
- 二次渲染
- 代码逻辑&&条件竞争
- 如何挖掘和利用文件上传漏洞
- 如何防御文件上传漏洞

2.4. 文件包含漏洞渗透与防御

- 为什么要包含文件
- 文件包含漏洞概述及分类演示
- CVE实际漏洞案例
- PHP相关函数和伪协议
- DVWA靶场案例演示
- CTF题目案例
- 中间日志包含绕过
- PHP包含读写文件
- STRREPLACE函数绕过
- 包含截断绕过FNM_TBH函数绕过
- 文件包含漏洞挖掘与利用
- 文件包含漏洞修复方案

2.5. CSRF漏洞渗透与防御

- CSRF漏洞概述及原理
- CSRF案例分析：Gmail、Weibo CSRF漏洞
- CSRF漏洞危害
- CSRF和XSS的区别
- CSRF常见payload写法
- CSRF漏洞挖掘与自动化工具
- CSRF漏洞防御之Referer、Token、二次验证

2.6. SSRF漏洞渗透与防御

- SSRF漏洞概述和演示
- PHP SSRF相关函数和协议
- SSRF常见场景
- SSRF CTF题目分析
- 如何检测、挖掘SSRF漏洞
- 如何防御SSRF漏洞

2.7. XXE漏洞渗透与防御

- XML基础知识之外部实体
- XXE 危害：读取任意文件、探测内网端口、执行命令、DoS
- 微信支付XXE漏洞分析

- XXE 漏洞发现和利用
- XXE 漏洞修复：禁用外部实体、过滤XML内容、WAF

2.8. 远程代码执行漏洞渗透与防御

- 远程代码执行原理介绍
- CVE实际漏洞分析
- Log4j RCE复现与原理详解
- PHP远程代码执行涉及函数
- pikachu和DVWA靶场案例分析
- CTF题目分析：eval执行、命令注入、过滤CAT、过滤空格、过滤目录符号
- 远程代码执行漏洞防御方法

2.9. 反序列化漏洞渗透与防御

- PHP类与对象回顾
- PHP Magic函数介绍
- 什么是PHP对象反序列化操作
- 为什么会出现安全漏洞
- CTF题目分析：攻防世界 unserialize3
- CVE-2016-7124漏洞利用
- Typecho CMS反序列化漏洞复现
- PHP反序列化漏洞如何修复
- Java序列化和反序列化
- Apache Commons Collections反序列化漏洞
- Aalibaba Fastjson反序列化漏洞
- Apache Shiro反序列化漏洞

2.10. 逻辑漏洞渗透与防御

- 网络黑产事件与法律
- 逻辑漏洞挖掘必备技能
- 用户名遍历漏洞
- 恶意注册
- 未授权访问漏洞
- Session和Cookie伪造
- 验证码突破
- 密码找回漏洞
- 越权漏洞

- 短信轰炸漏洞
- 业务一致性相关漏洞
- 重定向漏洞

2.11. 暴力猜解与防御

- 密码安全概述
- 什么样的密码是不安全的
- 密码猜解思路
- Python代码实现暴力破解
- Burp Suite Intruder实现暴力破解
- Hydra爆破SSH密码
- Medusa暴力破解SSH密码
- msf破解SSH密码
- wfuzz爆破web密码
- 密码暴力破解防御手段
- 用户如何提升密码安全性

2.12. Redis未授权访问漏洞

- Redis服务器被挖矿案例
- Redis常见用途
- Redis环境安装
- Redis持久化机制
- Redis动态修改配置
- Webshell提权案例
- 定时任务+Bash反弹连接提权案例
- SSH Key提权案例
- Redis安全加固分析

2.13. AWVS漏洞扫描

- AWVS介绍
- Windows安装AWVS
- Kali安装AWVS
- 小皮面板安装
- 扫描靶场数据库部署
- 部署靶场网站
- 用户名密码登录扫描

- 录制登录序列进行扫描
- 定制cookies绕过登录扫描
- 扫描报告分析
- Goby简介
- Goby安装
- npcap安装
- Goby+AWVS联动扫描

2.14. Appscan漏洞扫描

- AppSacn介绍
- AppSacn扫流程和扫描方式介绍
- AppSacn安装与激活
- 环境搭建
- 扫描web应用程序
- 扫描环境准备
- 外置设备手工扫描
- 内置浏览器手工扫描
- 证书安装
- 外部设备扫描绕过登录
- 自定义扫描策略，扫描针对性漏洞
- 加载扫描结果
- 领导查看的报告解读
- 其他类型的报告解读

2.15. Nessus漏洞扫描

- Nessus工具介绍
- Nessus工具安装
- Nessus离线激活
- Nessus解除16次扫描的限制
- Nessus使用过程中遇到坑以及解决方案
- Nessus Host Discovery
- Nessus高级扫描
- Nessus Web应用程序扫描
- Nessus扫描log4J环境搭建
- Nessus扫描log4Jshell
- Nessus扫描log4Jshell漏洞生态系统

2.16. MSF-Metasploit Framework

- Metasploit 发展史
- Linux安装Metasploit
- Kali更新Metasploit
- Windows安装Metasploit
- Metasploit图形界面Viper
- Metasploit 目录结构
- msf核心模块与功能
- msfvenom常用命令参数上
- msfvenom 常用命令参数下
- msfconsole漏洞利用流程上
- msfconsole漏洞利用流程下
- meterpereter功能介绍
- PHP后门反弹连接演示
- CVE-2017-0144 “永恒之蓝”漏洞演示
- CVE-2017-8464 “震网三代” 反弹shell演示
- CVE-2020-0796 “永恒之黑”漏洞攻击蓝屏演示
- 生成木马反弹shell（Windows）
- 生成木马反弹shell（Linux）
- 生成木马反弹shell（Android ）
- 后渗透之访问文件系统
- 后渗透之上传下载文件
- 后渗透之屏幕截图（Windows）
- 后渗透之键盘记录（Windows）
- 后0渗透之创建账号（Windows）
- 后渗透之调用音频设备录制
- 后渗透之提权（Windows）
- 后渗透之获取登录密码（Windows）
- 后渗透之远程监控（Windows）
- 后渗透之调用摄像头
- msf Auxiliary辅助模块
- msf编码免杀
- msf清除事件日志

2.17. CS-CobaltStrike

- Cobalt Strike介绍和环境配置
- Cobalt Strike 服务器启动
- Cobalt Strike 客户端链接到团队服务（linux）
- Cobalt Strike 客户端链接到团队服务（Windows）
- Cobalt Strike 功能按钮介绍
- Cobalt Strike 快速创建监听器
- Cobalt Strike Beacon分类
- DNS Beacon
- HTTP 和 HTTPS Beacon
- SMB Beacon
- TCP Beacon
- Cobalt Strik 目标主机信息收集
- Cobalt Strik 克隆网页并挂马
- Cobalt Strik 邮件钓鱼
- Cobalt Strik注入MSF会话

2.18. Burp Suite从入门到实战

- Burp Suite基本介绍
- Burp Suite版本区别
- Burp Suite参考资料
- Burp Suite下载
- Burp Suite启动激活
- Burp Suite配置
- Burp Suite界面布局
- Burp Suite模块总体介绍
- 浏览器代理设置
- Burp Suite代理设置
- Burp Suite拦截HTTPS数据
- Burp Suite拦截手机App数据
- Target模块的作用
- Target设置目标域
- 站点地图Sitemap
- Target结果操作
- Scanner模块
- Intruder模块

- Repeater模块
- Burp常用插件

2.19. ARP渗透与防御

- ARP原理
- ARP断网攻击
- ARP流量分析
- kali数据包转发
- dsniff工具介绍
- url流量分析过程讲解
- ARP-wireshark获取用户数据
- wireshark工具介绍
- ARP攻击截获用户信息步骤
- wireshark过滤命令讲解
- Ettercap工具介绍
- Ettercap界面操作攻击
- Ettercap功能讲解
- Ettercap命令行攻击
- ARP网速限制
- TC工具介绍
- TC命令介绍
- ARP攻击限制网速的具体步骤
- 限速原理讲解
- ARP-DNS欺骗
- ARP-DNS原理和劫持概念讲解
- ARP-DNS常用命令讲解
- ARP-DNS攻击步骤01
- ARP-DNS攻击步骤02
- ARP-DNS攻击课堂小结
- ARP防御方法介绍
- ARP防火墙防护ARP攻击
- ARP设置临时绑定网关MAC地址为静态
- ARP设置永久绑定网关mac地址
- linux防御ARP攻击
- 网关或者路由器防御ARP攻击
- web服务器防御ARP攻击

2.20. DOS与DDOS渗透与防御

- SYN+FLOOD攻防还原
- IP地址欺骗攻防
- DNS放大攻击攻防还原
- SNMP放大攻击攻防还原
- NTP放大攻击攻防还原
- 应用层CC攻防攻防还原
- 其它类型压力测试
- DDOS安全防范

2.21. 内网相关渗透与防御

- 内网信息收集
- 隐藏通道隧道技术
- 权限提升分析与防御
- 域内横向移动分析及防御
- 域控制器安全
- 跨域攻击分析及防御
- 权限维持分析及防御

2.22. 无线相关渗透与防御

- :环境准备
- 协议补充
- wifi协议
- AP和客户端介绍
- Ap专业术语介绍
- 网卡工作模式
- wifi渗透环境搭建
- 字典概念介绍
- 亦思社会工程学密码生成器
- 真空密码生成器
- safe6密码生成器
- Crunch密码生成器
- 千万常用密码
- windows扫描附近的wifi
- windows-ntesh探索WiFi密码
- 章节4:熟悉kismet

- kismet软件介绍
- kismet嗅探wifi
- WEP介绍
- 认证类型讲解
- 加密算法介绍
- WEP加密和解密
- Aircrack-ng 常用工具包
- Aireplay-ng 的 6 种攻击模式
- WEP wifi探索步骤-1
- WEP wifi探索步骤-2
- 遇到错误的处理方式
- gerix-wifi-cracker环境准备
- gerix-wifi-cracker探索步骤讲解
- gerix-wifi-cracker探索实操讲解
- wifite工具介绍
- wifite扫描讲解
- wifite渗透步骤讲解
- Hirte介绍
- Hirte渗透姿势1
- Hirte渗透姿势2
- WPA概念介绍
- WPA工作原理
- wifi设置讲解
- WPA专属字典打造
- WPA渗透步骤讲解
- WAP渗透家用路由器
- hashcat介绍
- 渗透姿势讲解
- Cowpatty介绍
- cowpatty渗透
- hast-table加速渗透
- WPA-自动化渗透WPA加密
- WPA渗透-windows下GPU跑包加速
- EWSA安装教程
- pyrit介绍
- pyrit安装
- GPU加速渗透
- GPU加速渗透流程

- WPA渗透-使用airolib-ng创建彩虹表加速

2.23. 系统权限提升渗透与防御

- WINDOWS 提权常用命令
- WINDOWS 提权实战、提权防范
- WINDOWS 提权后期密码安全性测试
- LINUX 权限提升以及提权必备的命令学习
- LINUX 脏牛提权以及 SUID 提权

2.24. 社会工程学

- 社工学之交流模型概述
- 社工学之通过交流方式收集渗透信息
- 社工学之“香农”-“韦弗”模型概述
- 社工学 香农-韦弗模型基础
- 社工学 香农-韦弗模型分层
- SMCR通信模型
- SMCR通信模型规则
- 制定交流模型
- 真实钓鱼邮件案例解说
- 工具-诱导篇
- 工具-诱导含义
- 工具-诱导交谈的步骤
- 工具-成功诱导的条件和技巧
- 工具-提问的艺术

2.25. CVE漏洞复现

- CVE-2021-44228 Log4j2远程代码执行漏洞
- CVE-2022-22947 Spring Cloud Gateway RCE漏洞
- CVE-2022-22965 Spring Bean RCE漏洞
- ……

2.26. vulnhub靶场实战系列

- 靶场实战平台介绍
- prime1
- breach1

- dc9
- Kioptrix_Level_1
- Kioptrix Level 2
- pWnOS v2.0

2.27. 挖漏洞项目实战

- 信息收集-在线站点
- 挖漏洞-信息收集-工具
- 漏洞挖掘-fuzz
- 漏洞挖掘-SQL注入
- 漏洞挖掘-XSS
- 漏洞挖掘-越权漏洞
- 漏洞挖掘-LFI-CSRF
- 漏洞挖掘-SSRF
- 漏洞挖掘-文件上传漏洞、RCE
- 漏洞挖掘-综合实战

2.28. 免杀-反杀毒技术

- 从思维角度上改变免杀的认识
- 安全软件分析思维导向
- 从源码角度解决RAT免杀问题
- 渗透过程中白+黑利用方式
- 开发高级版shellcode加载器
- 改壳免杀高级技巧
- 高级免杀壳开发原理
- 从源码角度加密输入表
- 打造自己独立的红蓝对抗RAT后门shell
- 巧过360全家桶方法
- 迷你方式过卡巴全家桶
- 冲锋方式过管家系列
- 免杀office相关APT组合
- 奇淫技巧之主动防御绕过
- 偷梁换柱之奇怪的免杀方法
- 云沙盘绕过方法

2.29. Windows逆向进阶版

- 汇编与C的关系
- 从逆向角度看C++
- 动态调试基础
- IDA动静分析基础
- PE文件结构基础
- Windows系统安全基础
- 脚本类恶意程序的快速分析技巧
- 文档类恶意程序的快速分析技巧
- PE类恶意程序的快速分析技巧（DLL篇）
- PE类恶意程序的快速分析技巧（EXE篇）
- APT攻击链恶意样本分析
- 勒索病毒类型快速分析
- 白+黑类型样本快速分析
- 恶意样本加壳基础
- 恶意软件脱壳基础
- 游戏反外挂基础
- 游戏加密协议基础
- 游戏功能函数分析
- 外服CABAL脱机辅助开发原理
- nProtect GameGuard漏洞分析
- 游戏检测绕过与防护
- 游戏插件开发原理与查杀
- 游戏截包工具开发基础
- 游戏资源文件解密
- MIR4 区块链游戏的对抗方式
- 流量溯源的起源
- 流量溯源的信息探索
- 流量溯源的溯源画像模板
- 流量中攻击链的形成
- 流量中攻击链的基础溯源
- 社交网络部署蜜罐进行溯源分析
- 从逆向维度溯源扫描器框架
- 从逆向维度挖掘线索中的价值
- 暗藏在钓鱼邮件背后的流量攻击
- C&C通讯模块的溯源分析
- DDOS溯源分析

- DDOS攻击流量中域名溯源分析
- DDOS攻击流量中关键ServerConnectClishell函数分析
- DDOS攻击流量中关键DNS解密函数分析
- 恶意流量之完整的精准溯源流程
- 恶意流量之开源C&C平台源码分析
- 恶意流量之完整的精准溯源流程
- 羊毛党的世界
- 羊毛党的黑产分析
- 恶意流量之检测C&C RAT通讯流量
- 恶意流量之源码 ghost通讯协议分析
- SIM token合约代码自动化薅羊毛攻击还原
- 区块链 token 的自动化薅羊毛攻击分析
- 风控模式下的对抗薅羊毛各种方式
- 薅羊毛App软件以及功能分类
- 薅羊毛APP软件功能分析
- 薅羊毛黑产工具原理
- 薅羊毛灰色产业链结构
- 薅羊毛之群控的原理

2.30. 安卓逆向

-
- 安卓逆向概述
- Linux-mac设置jdk
- Windows设置jdk
- 安装Android-studio
- 配置Android-sdk与代理的使用
- 配置开发设备虚拟机
- 配置开发设备-实体机
- Java语法概述
- Java语法hello例子
- Java语法-class-method-member
- Java语法-循环和条件判断
- Java语法try-catch
- Java语法总结
- 创建项目并运行
- 页面之间跳转
- 发起http请求
- 解析http结果

- AndroidManifest
- service与运行-调试
- Android studio的急速入门
- gradle极速入门
- Android_应用
- adb-push-pull
- adb-使用root设备
- Linux极速入门
- 虚拟机与实体机
- 普通发布的过程
- 为什么要加固加密
- 加密加固的多种阶段
- 加密加固的多种方案
- 安卓逆向基础-基本路径&基本用法
- jd-gui的基本用法
- apk-to-smali路径
- Burp Suite的安装与基本使用
- Burp Suite的基本配置
- 使用Burp Suite抓包https-web
- 安卓设备安装证书
- 为什么root与root原理
- 设备的选择
- 小米账户的绑定与设备解锁
- 刷机
- 刷机后的验证
- 钩子Hook介绍
- 钩子方法
- frida-server-client的安装与注意事项
- frida-安卓例子
- 判断是否存在代码层面的证书校验
- 脱壳并使用frida绕过ssl证书校验
- apk反编译成smali再重新打包成apk

第三部分：工程与实战

3.1. 等级保护

1）为什么要学习等保

- 什么是等级保护
- 什么是信息系统
- 什么是信息系统安全
- 等保的发展历程
- 等保的关注对象
- 等保的实施流程
- 等保的参与角色
- 课程学习目标

2）等保常见问题解答

- 哪些行业需要等级保护？
- 不做等级保护可以吗？
- 等保是按单位实施还是按系统实施？
- 系统部署在阿里云，需要做等保吗？
- 内网系统需要做等保吗？
- 做等级保护测评需要多久？
- 等保测评是一次测评，终身有效吗？
- 做等级保护要多少钱？
- 是不是定级越低越好？
- 等级保护测评的难点有哪些？

3）等级保护相关概念介绍

- 第三方测评机构
- 等保测评师岗位
- 安全产品服务和厂商
- 关保：关键信息基础设施保护
- 分保：涉及国家秘密的信息系统分级保护管理办法
- 重保：重要时期安全保障服务
- ISO27000体系

- 风险评估

4）等保2.0解读

- 等级保护发展历程
- 等级保护与网络安全法
- 等保2.0修订背景
- 等保2.0变化内容
- 等保2.0标准体系

5）等保2.0通用要求解读

- 安全框架
- 安全通用要求
- 控制类和控制项
- 2.0网络拓扑结构设计
- 安全设备配置建议
- 2.0扩展要求解读

6）等保实施流程

- 定级备案
- 风险评估、差距分析
- 安全规划设计
- 建设整改
- 等级测评
- 监督检查

7）等保案例分析

3.2. 应急响应

- 企业安全应急响应流程
- 木马实战演练
- Linux服务器入侵实战演练
- Windows系统入侵实战演练
- DNS&DHCP实战演练
- ARP欺骗攻击实战演练
- DDOS实战演练

3.3. 代码审计

- 代码安全测试介绍
- 代码安全测试方法
- 代码审计的通用思路
- 漏洞产生的原因
- 漏洞挖掘流程分析
- 手工代码审计实例分析
- SEAY源代码审计系统使用
- 工具局限性

3.4. 风险评估

- 项目准备
- 实施申请
- 培训事项
- 物理环境
- 网络结构
- 硬软件资产
- 信息系统
- 数据资产
- 服务器资产
- 安全管理
- 安全措施

1）脆弱性评估

- 网络设备脆弱性评估、交换机、路由器、安全设备
- 数据库脆弱性评估MySQL、MSSQL、Oracle
- 中间件脆弱性评估
- 主机璀错性评估
- 安全渗透测试

2）信息系统风险控制规划

- 安全技术控制规划
- 安全管理控制规划

3) 报告输出

- 信息系统脆弱性评估报告
- 信息系统威胁评估报告
- 信息系统资产评估报告
- 信息系统风险评估综合报告

3.5. 安全巡检

- 漏洞扫描(绿盟、安恒、启明及开源漏洞扫描器在企业中应用,同时完成漏洞扫描之后如何编写漏洞扫描报告
- 实战案例:策略检查(交换机、路由器、安全设备、操作系统、数据库、应用安全配置等进行策略检查)
- 实战案例:日志审计(分别通过安全日志分析工具及手工方式对攻击日志进行分析)
- 实战案例:监控分析(系统监控、态势感知、WAF设备等监控分析)
- 行业巡检(金融、教育、医疗行业等安全巡检)
- 巡检总体汇总报告

3.6. 数据安全

- 数据安全的基本认识
- 企业部署MySQL的准备工作
- MySQL企业上线要求
- MySQL 8.0生产落地实战
- Oracle部署准备
- Oracle上线准备
- Oracle生产落地实战
- 等保中对MySQL版本的要求
- 等保中对MySQL用户相关要求
- 等保中对MySQL用户相关操作
- 等保中对MySQL权限方面要求
- 等保中对MySQL SQL审核要求
- Yearning SQL审核平台应用
- Yearning SQL审核平台配置
- Yearning SQL审核平台-SQL审核操作
- 数据安全保护-数据损坏的场景
- 数据安全保护-数据备份的职责
- 数据安全保护-备份工具介绍

- 数据安全保护-mysqldump进行数据损坏恢复
- 数据安全保护物理备份工具PXB全备恢复应用
- 数据安全保护-物理备份工具PXB增量备份恢复
- 数据安全保护-使用ClonePlugin本地克隆
- 数据安全保护-使用ClonePlugin远程克隆
- 数据安全保护-架构设计及容灾能力
- 数据安全保护-ORCH容灾能力测试

第四部分：开发与提升

4.1. 密码学

- 剖析基本概念
- 什么是加密与解密
- 寻找银弹
- 入门加密与解密
- 数据完整性
- 对称密码
- 公钥密码
- 公钥密码
- 非对称密钥生成器
- 密钥规范管理
- 数字签名
- 数字证书相关管理
- 安全套接字
- 简单并常用的BASE64
- 文件校验
- 打破出口限制
- 编码转化辅助工具

4.2. Java入门

- Java入门
- 数据类型
- 运算符
- 流程控制
- 方法的定义、调用、重载
- 数组
- IDEA开发工具
- Java面向对象
- 注解、反射、JDK新特性

4.3. C语言

- C语言开篇

- 数据类型
- C语言输入和输出
- 运算符和表达式
- 流程控制
- 数组
- 函数
- C语言预处理
- 指针
- 复合数据类型
- C程序的组成

4.4. C++编程

- C++概述
- C++对C的拓展
- 类和对象
- 继承
- 多态
- 异常
- 强制类型转换
- 泛型编程

4.5. Shell编程

- 编程入门技能
- 变量概念介绍
- 特殊变量进阶
- 数值计算实践
- 条件测试比较
- 条件判断语句
- 流程控制语句
- 循环语句应用
- 循环控制语句
- 函数知识精讲
- 数组知识精讲
- 开发环境规范
- 调试优化实践
- 自动化实战项目

4.6. 汇编语言程序设计

- 为什么要学习汇编
- 计算机语言发展历史
- 编程语言分类
- 机器语言
- 汇编语言
- 寄存器的概念
- 字的存储
- 物理地址与段地址
- CS和IP
- DOS的安装与使用
- 段的分类
- 一个源程序从写出到执行的过程
- 源程序
- 编译
- 连接
- 程序执行过程的跟踪
- 数据传输指令
- 算术运算指令
- 位运算指令
- 串操作指令
- 控制转移指令
- 处理机控制指令及伪指令

4.7. CTF夺旗赛

1) CTF-WEB题型

- CTF-WEB 题型[GKCTF2021]HACKME
- CTF-WEB 题型[GKCTF2021]EASYNODE
- CTF-WEB 题型[GKCTF2021]EASYCMS
- CTF-WEB 题型[GKCTF2021]CHECKBOT
- CTF-WEB 题型[GKCTF2021]BABYCAT

2) CTF-REVERSE题型

- CTF-REVERSE 题型[GKCTF2021\]SOMUCHCODE]
- CTF-REVERSE 题型[GKCTF2021]QQQQT

- CTF-REVERSE 题型[GKCTF2021]KILLERAID
- CTF-REVERSE 题型[GKCTF2021]CRASH
- CTF-REVERSE 题型[GKCTF2021]APP-DEBUG

3) CTF-PWN题型

- CTF-PWN 题型[GKCTF2021]ESAPESH
- CTF-PWN 题型[GKCTF2021]DEMO_CATROOM
- CTF-PWN 题型[GKCTF2021]CHECKIN
- CTF-PWN 题型 YCB_2020_MIPSPWN
- CTF-PWN 题型 YCB_2020_REPWN

4) CTF-CRYPTO题型

- CTF-CRYPTO 题型[GKCTF2021]XOR
- CTF-CRYPTO 题型[GKCTF2021]RRRRSA
- CTF-CRYPTO 题型[GKCTF2021]RANDOM
- CTF-CRYPTO 题型[羊城杯 2020]GMC
- CTF-CRYPTO 题型[羊城杯 2020]RRRRRRRSA

5) CTF-MOBILE

- CTF-MOBILE 题型[ISCC2021]1A2B
- CTF-MOBILE 题型[ISCC2021]LOCKK
- CTF-MOBILE 题型[ISCC2021]MOBILEEASY
- CTF-MOBILE 题型[ISCC2021]MOBILENORMAL
- CTF-MOBILE 题型[ISCC2021]OHHH

6) CTF-MISC

- CTF-MISC 题型[GKCTF2021]FIREFOXFORENSICS
- CTF-MISC 题型[GKCTF2021]EXCEL 骚操作
- CTF-MISC 题型[GKCTF2021]银杏岛の奇妙冒险
- CTF-MISC 题型[GKCTF2021]签到
- CTF-MISC 题型[GKCTF2021]你知道 APNG 吗