CTF 预备队员培训计划

课程安排：

模块	时间	内容	备注
网络基础知识	第 1 天	网络基础	TCP/IP 模型 局域网和广域网原理 TCP\UDP\IP 原理 路由器与交换机原理 网络与信息系统架构
操作系统基础	第 2 天	Windows 操作系统	Windows 用户和组管理 Windows 文件系统 Windows 性能和日志管理
	第 3 天	Windows 操作系统	Windows 服务器配置之 DNS Windows 服务器配置之 IIS Windows 服务器配置之 AD
	第 4 天	Linux 操作系统	管理文件和目录 管理磁盘和文件系统 Linux 软件包管理 Linux 网络配置
	第 5 天	Linux 操作系统	Linux 用户和组管理 Linux 日志管理 Linux 服务器配置之 DNS Linux 服务器配置之 Web
数据库基础	第 6 天	SQL 基础 1	检索数据使用 SQL 语句 限制和排序数据 使用函数 多表查询 子查询
	第 7 天	SQL 基础 2	使用 DDL 建立与管理表 建立其他对象 操纵数据 高级子查询 报表高级分组函数 层次查询
中间件	第 8 天	中间件基础 1	Apache 安装使用 jboss 中间件安装配置 NGINX 安装使用 Tomcat 安装使用
	第 9 天	中间件基础 2	WebLogic Server 安装与配置 控制台管理

			命令行管理 配置 JDBC 配置 JMS
Web 应用漏洞	第 10 天	Web 安全基础	Web 服务器介绍 HTTP 协议详解 OEASP Top 10 介绍 对应 CTF 中 Web 试题解析 目录遍历漏洞
	第 11 天	文件上传漏洞	文件上传漏洞 js 绕过 文件上传漏洞 MINE-Type 绕过 文件上传漏洞扩展名绕过 文件上传漏洞 00 截断 文件上传漏洞修改文件头绕过
	第 12 天	SQL 注入	SQL 注入基础知识 SQL 注入实战演练 SQL 注入工具使用 SQL 注入防御措施
	第 13 天	命令执行漏洞	PHP 命令执行 PHP 代码执行 PHP 动态函数调用 PHP 函数代码执行漏洞
	第 14 天	提权	了解提权 简单提权 Mysql 提权 03/08 溢出提权
	第 15 天	XSS	XSS 介绍 XSS 类型 payload 构造 XSS filter 绕过 Cookie 的获取及使用 XSS 漏洞挖掘 XSS 防御
	第 16 天	文件包含漏洞	初识文件包含 本地文件包含 远程文件包含 PHP 伪协议 防御文件包含
逆向技术 PWN	第 17 天	二进制文件 汇编基础	从源代码到可执行文件 ELF 文件格式 静态链接 动态链接 CPU 架构与指令集 操作模式

	第 18 天	分析环境搭建 分析工具	虚拟机环境 Docker 环境 IDAPro104 Radare2 GDB 其他常用工具
	第 19 天	漏洞利用开发	hellcode 开发 Pwntools zio
		整数安全	计算机中的整数 整数安全漏洞
	第 20 天	格式化字符串	格式化输出函数 格式化字符串漏洞
		栈溢出与 ROP	栈溢出原理 返回导向编程
	第 21 天	堆利用	TCache 机制 fastbin 二次释放 houseofspirit 不安全的 unlink off-by-one houseofeinherjar overlappingchunks houseofforce unsortedbin 与 largebin 攻击
	第 22 天	Pwn 技巧	one-gadget 通用 gadget 及 Return-to-csu 劫持 hook 函数 利用 DynELF 泄露函数地址 SSPLeak 利用 environ 泄露栈地址 利用_IO_FILE 结构 利用 vsyscall
密码学	第 23 天	密码学	编码 古典密码 现代密码 真题解析
隐写术	第 24 天	隐写术上	文件操作与隐写 图片隐写
	第 25 天	隐写术下	压缩文件处理 流量取证技术
代码审计	第 26 天	PHP 编程基础	PHP 代码基础
	第 27 天	PHP 代码审计	PHP 代码审计

	第 28 天	JAVA 编程基础	JAVA 编程基础
	第 29 天	JAVA 代码审计	JAVA 代码审计
	第 30 天	Python 编程基础	Python 编程基础
	第 31 天	Python 代码审计	Python 代码审计