2022 公安部 HW 行动-培训大纲

- **第一周**
- **时长：5 天**

时间	模块	内容简介	培训目标	说明
第 1 天 上午	HW 第一课 HW 流程	了解网络安全及 HW，分享 HW 经验，了解 HW 流程	认识 HW，了解 HW	
第 1 天 下午	护网防守方工作流程 规划与总结 初识安全设备	介绍防守方工作，并接触安全设备	了解防守方工作，对安全设备有印象	
第 2 天 上午	操作系统：linux	操作系统基础 Linux 基础入门与系统 Linux 文件及目录管理命令基础 系统目录结构与重要文件	学习（复习）linux 系统相关知识	
第 2 天 下午	操作系统：linux	文件类型与文件属性 Linux 用户管理知识 操作系统基础 进程管理与软件管理		CVE-2017-3599 CVE-2016-6662
第 3 天 上午	操作系统：linux	操作系统基础 Linux 文件系统 操作系统-文本内容编辑 操作系统安全实践-Linux 系统配置安全		CVE-2020-15778 CVE-2018-15473
第 3 天 下午	操作系统 windows	Windows 指令基础 操作系统安全实践-Windows 配置安全 操作系统概述	学习（复习）windows 系统安全配置相关知识	CVE-2020-1938 CVE-2017-12615 CVE-2016-8735

第 4 天 上午	操作系统相关	shell 基础 操作系统安全问题-典型的安全问题。	一些其他的关于操作系统的知识	
第 4 天 下午	计算机网络概述	计算机网络概述 传输层协议简述 应用层协议简述 网络协议安全概述	学习（复习）计算机网络的相关知识	
第 5 天 上午	流量分析	wireshark&tcpdump 的介绍 流量分析题讲解	学习 wireshark 的使用，并学习进行流量分析	
第 5 天 下午	应急响应	应急响应实战讲解第一节 应急响应实战讲解第二节 应急响应实战讲解第三节。	掌握应急响应的方法	

- **第二周**
- **时长：5 天**

时间	模块	内容简介	培训目标	说明
第 1 天 上午	实战场景讲解	常见的攻击防守 常见安全事件与 Windows 日志分析 Linux 与 Windows 入侵与排查	掌握应急响应的方法	
第 1 天 下午	复习，学习安装 dvwa	为考试准备，并为后续的学习做好环境准备		
第 2 天 上午	理论知识测验	对之前学习的知识进行测验		
第 2 天 下午	认识 DVWA 平台 XSS 漏洞	首先在安装好的 dvwa 平台上进行 学习 XSS 漏洞利用方式，高中低难度	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 3 天 上午	文件上传漏洞	学习文件上传漏洞，学习使用一些常用的 webshell 管理工具	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 3 天 下午	Sql 注入漏洞	学习 SQL 注入漏洞的利用，以及自动化注入工具的使用	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 4 天 上午	SQL 盲注	学习 SQL 盲注漏洞的利用，以及自动化注入工具的使用	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	

第 4 天 下午	文件包含漏洞与命令注入漏洞	学习文件包含漏洞、命令执行漏洞的利用	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 5 天 上午	暴力破解漏洞，CSRF	学习文暴力破解漏洞的原理以及 burpsuite 的使用	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 5 天 下午	实操考核			

- **第三周**
- **时长：5 天**

时间	模块	内容简介	培训目标	说明
第 1 天 上午	中间件漏洞，安装 vulhub 靶场以及 kali			
第 1 天 下午	回顾之前 HW 行动中的漏洞	挑选一些有意义的曾经出现过的漏洞复现并讲解原理		
第 2 天 上午	Tomcat 系列漏洞	学习 tomcat 相关的一系列中间件漏洞	通过学习一些列的 tomcat 中间件漏洞，了解 tomcat 漏洞的利用，形成方式以及利用方法，能够给出修复意见	
第 2 天 下午	Tomcat 系列漏洞			
第 3 天 上午	Weblogic 漏洞	学习 weblogic 相关的一系列中间件漏洞	通过学习一些列的 weblogic 中间件漏洞，了解 webloic 漏洞的利用，形成方式以及利用方法，能够给出修复意见	
第 3 天 下午	Weblogic 漏洞			
第 4 天 上午	Strust2 漏洞	学习 Strust2 相关的一系列中间件漏洞	通过学习一些列的 strust2 中间件漏洞，了解 strust2 漏洞的利用，形成方式以及利用方法，能够给出修复意见	
第 4 天 下午	Strust2 漏洞			

第 5 天 上午	Fastjson 漏洞，shrio 漏洞	学习 Fastjson，shrio 相关的一系列中间件漏洞	认识了解相关漏洞的形成方式以及利用方法，能够给出修复意见	
第 5 天 下午	实操考核			

- **第四周**
- **时长：5 天**

时间	模块	内容简介	培训目标	说明
第 1 天	waf 使用练习	waf 各模块功能介绍 Top10 漏洞触发 waf 告警实践 查看 waf 告警页面，分析告警日志，判断是否误报及告警分析	通过实战掌握 waf 的功能及蓝队的使用方法	
第 2 天	IPS/IDS 使用练习	IPS 各模块功能介绍 常见攻击触发 IPS 告警实践 查看 IPS 告警页面，借助 IPS 分析攻击类型及攻击结果	通过实战掌握 IPS/IDS 的主要功能及蓝队的使用方法	
第 3 天	项目现场注意事项	详解项目现场应注意的事项，包括客户网络安全保障， 客户现场行为准则等，保证项目安全运行。	保证客户现场安全，也保证自己安全。	
第 4-5 天	攻防平台应急相应实战演习	在企业级内外网攻防平台上进行攻击队与防守队实战对抗 演练蓝队应急/研判组对攻击行为的处置过程 编写蓝队处置报告	通过实战掌握应急响应的流程	