课程名称：网络安全攻防 2021

课程目标：

CTF 百度-夺旗赛 CTF(Capture The Flag)中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF 起源于 1996 年 DEFCON 全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013 年全球举办了超过五十场国际性 CTF 赛事。而 DEFCON 作为 CTF 赛制的发源地，DEFCON CTF 也成为了目前全球最高技术水平和影响力的 CTF 竞赛，类似于 CTF 赛场中的"世界杯" 。CTF 是一种流行的信息安全竞赛形式，其英文名可直译为"夺得 Flag"，也可意译为"夺旗赛"。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。为了方便称呼，我们把这样的内容称之为"Flag"。

本课程将全面介绍现有网络信息安全防范措施，以网络协议的发展为主线，结合病毒的发展过程来综合分析。在分析工具上，将介绍多种网络监测工具、常用分析软件安，注重理论与实践相结合，每介绍一种类型安全攻防，**超过 30 个操作案例**的网络课程。

适用学员：从事 WEB 机房维护工程师、网络安全工程师、服务器运维工程师、后台支撑（市场、后台、增值服务等线条）。

课程设计：

课程编号：	20210729005
授课课时:	2-10 天
授课条件：	学员必须具有基本的通信技术基础知识
内容摘要：	**壹、 CTF 概述** ◇ CTF 赛制介绍 ◇ 参赛工具介绍 ◇ Kali Linux 基础 ◇ 配置 apt 命令 ◇ Kali 本地网络配置 **案例：被动收集——DNS 域名解析** **案例：被动收集——Maltego 收集域名信息** **案例：被动收集——使用 Shodan 暗黑谷歌搜索引擎**

弐、 主动扫描

- ◇ 列举远程机器开放的端口
- ◇ 识别目标主机的服务印记
- ◇ 发现局域网中在线主机
- ◇ 端口探测技巧
- ◇ NSE 脚本使用
- ◇ 使用特定网卡进行探测
- ◇ 对比扫描结果 ndiff
- ◇ 可视化 Nmap 的使用
- ◇ Nmap 指定网卡补充

案例：使用 scapt 定制数据包进行高级扫描

案例：僵尸扫描

案例：分布式集群执行大量扫描任务

案例：NESSUS 漏洞检测

参、 Wireshark 网络抓包

- ◇ 抓包原理与设置
- ◇ 抓包及快速定位数据包技巧

案例：对常用协议抓包并分析原理

案例：解决服务器被黑后 无法联网问题

- ◇ 基于 TCP 协议收集主机信息
- ◇ 基于 SNMP 协议收集主机信息
- ◇ 基于 SMB 协议收集信息
- ◇ 基于 SSH 协议收集信息
- ◇ 基于 FTP 协议收集信息
- ◇ 通过 IP 地址定位客户端位置

四、 终端渗透

- ◇ 终端渗透原理

案例：制作 WIN 系统软件获取目标客户 SHELL

案例：制作 Linux 系统获取目标客户 SHELL

案例：制作后门 BUG

案例：利用 0day 漏洞获取 SHELL

案例：基于 JAVA 环境的漏洞利用获取

案例：安卓客户端渗透

伍、 burpsuite 抓包拦截应用

掌握重要网路安全应用工具，包括认证协议原理、电子邮件安全原理、WEB 安全原理，了解 IP 安全和网络 SNMP 管理

- 安装
- Proxy 代理设置
- 抓取手机 APP 流量
- 绕过 JS 文件上传认证
- Target 介绍
- 站点地图

案例：爬虫

案例：漏洞扫描

案例：暴力破解 WEB 用户密码

案例：跨站请求伪造

案例：命令行注入

案例：反射型跨站脚本攻击

案例：存贮型跨站脚本攻击

案例：SQL 注入

案例：文件包含

六、 防火墙

掌握防火墙技术原理，了解恶意软件的威胁和应对。

- TCP/IP 64 位基础

- 防火墙原理
- 防火墙技术发展
- 常用防火墙设置技巧

七、 系统安全

掌握重要的系统安全级问题，包括入侵原理和检测技术原理

- 入侵原理
- 口令管理
- 蠕虫与溢出

案例：利用 Unicode 漏洞

案例：使用 Ping 探测服务器存活

八、 木马病毒

- 木马技术揭露
- 木马程序的安装
- 木马的隐藏技术分析
- 木马清除方法

案例：使用 ms17-010 永恒之蓝漏洞对 WIN7 进行渗透

案例：linux 无文件木马程序

案例：使用脚本自动创建后门

案例：系统日志清理

授课语言：	中文