渗透测试工程师技术实战课

课程介绍

教学目标

★ 能够理解渗透测试是什么

★ 能够理解渗透测试流程的基本步骤

◆ 为什么要学习web渗透测试

网络战

“一个民族国家为了造成损害或破坏而渗透另一个国家的计算机或网络的行动”

网络战其作为国家整体军事战略的一个组成部分已经成为趋势

◆ 为什么要学习web渗透测试

★ 业务数据对组织的重要性使得组织必须关注业务连续性

★ 可遵循的资产保护

有什么

用来做什么

需要保护他们吗

◆ 为什么要学习web渗透测试

从个人角度而言，这不仅仅是一个技术问题，还是一个社会问题、法律问题以及道德问题。

- 隐私保护
- 社会工程学
- 个人资产安全

个人信息资产问题思考

- 哪些信息资产被恶意利用后会形成人身的损害?
- 哪些信息资产被恶意利用后会形成财务的损失?
- 哪些信息资产被恶意利用后会形成法律责任?

◆ 为什么要学习web渗透测试

分层思想的优劣：每个人看到的系统不同；

只追求功能的实现；

最大的威胁是?

安全目标

先于攻击者发现和防止漏洞出现

01

攻击型安全

使用攻击手段发现系统中的漏洞

02

防御型安全

将不必要的端口和服务关掉，降低攻击面

渗透测试

尝试挫败安全防御机制，发现系统安全弱点

从攻击者的角度思考，测量安全防护有效性

证明安全问题的存在，而非破坏

道德黑客

法律

渗透测试的标准流程

侦察

目标测试

漏洞利用

提高权限

保持访问

google、whois…

nmap、DirBuster…

Metasploit,sqlmap…

Meterpreter…

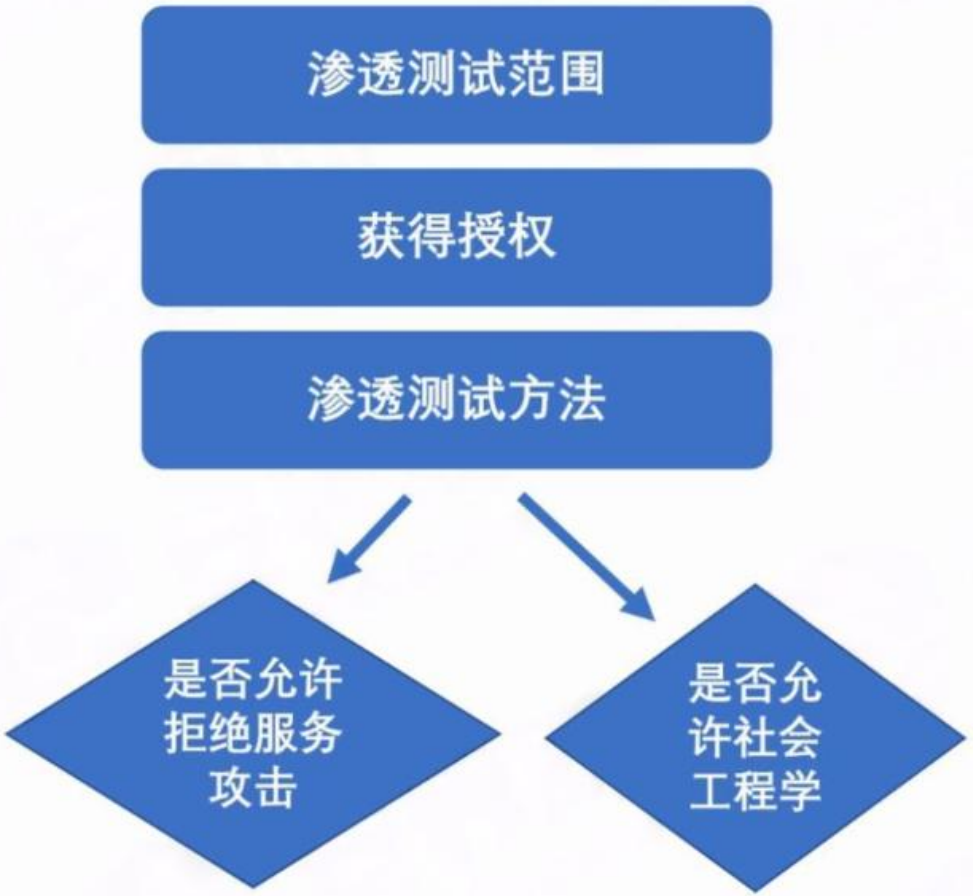
Meterpreter…

渗透测试的标准流程

渗透测试流程

前期交互阶段	确定参透测试范围、目标、限制条件以及服务合同细节
情报收集阶段	获取目标网络拓扑、系统配置、安全防御措施等信息
威胁建模阶段	根据收集到的信息，确定最有效，最有可能成功的攻击途径
漏洞分析阶段	综合分析汇总的情报信息、从漏扫结果、服务查点信息等，找出可实施攻击的点
渗透攻击阶段	并不像想你中那么顺利，目标系统 有防护系统
后渗透攻击阶段	你以为一台被渗透机器为跳板，进一步渗透整个系统
报告阶段	向客户和其他同事证明系统可以被控制，描述发现、利用过程，以及如何解决

渗透测试的标准流程



渗透测试的误区

- 扫描器就是一切
- 忽视业务逻辑的漏洞
- 人和工具

谢谢观赏