实战视角下的网络安全防御

教育部教育管理信息中心
祁 伟

2019.11.12 浙江●杭州

内容简介

- 分析网络攻击的特点，从安全防御的难点入手，梳理安全防护的思路，从实战中来，到实战中去。

网络安全防御的难点

- 网络安全的本质
  - 网络攻防是网络安全的本质
- 存在的问题
  - 识别攻击的确定性太低
  - 从确定到处置太慢

网络攻击的特点

- 攻击行为
  - 寻找网络路径
  - 控制主机节点
  - 建立隐秘通道
  - 获取敏感数据
- 攻击目标
  - 路由器等网络及网络安全设备
  - 主机-服务器和终端计算机
  - 数据库

防御技术与措施

- 数据流管控
  - 流量分流
    - 数据平面
    - 管理平面
    - 控制平面
  - 控制思路
    - 限制攻击面
    - 定位控制点

防御技术与措施

- 主机管控
  - 操作系统层管控
    - 用户权限
    - 文件系统
    - 服务进程
  - 控制思路
    - 管控粒度延伸至操作系统

防御技术与措施

- 数据库管控
  - 数据库层管控
    - 数据库对象级
    - 行为管控
    - 数据库防火墙
  - 控制思路
    - 管控粒度延伸至数据库级
    - 与应用服务器联动控制

防御技术与措施

- 经验总结
  - 网络防御策略
    - 由里向外
    - 化繁为简
    - 化整为零
  - 人才队伍建设

谢谢聆听！