四川大学
国家示范性软件学院
SCU Software college

端口扫描程序

2012-10

课程内容

- 端口扫描回顾
- Connect 端口扫描程序工作原理

端口扫描回顾

- 定义：所谓端口扫描就是发送数据包给被探测端，根据被探测端的响应信息确定被探测端开启了那些端口。
- 作用：确定有哪些端口正处于监听状态是一个非常重要的攻击步骤，攻击者不仅可以了解到远程系统上都运行着哪些服务，还可以准确地探测出目标系统所使用的操作系统和应用程序的类型和版本

端口扫描回顾

分类

- 开放扫描 (Open Scanning)
- 半开放扫描 (Half-Open Scanning)
- 秘密扫描 (Stealth Scanning)

试验题目

- 利用 socket 中的 sock_stream 套接字实现一个 TCP 公开扫描程序，要求：
  - 输入
    1. 用户可以通过程序可以设定扫描目的的地址；
    2. 用户可以设定扫描端口的范围；
  - 输出
    1. 显示扫描目标开启了那些端口；
  - 程序的验证：
    - 在 shell 下输入命令“ netstat -ltn”, 对比自己程序的输出结果

试验题目提示-端口扫描程序工作流程

服务名的获取

- Struct servent *getservbyport(port,proto)

- Struct servenet{
  char * s_name;
  char** s_aliases;
  int s_port;
  char* s_proto;
  }