- 扫描与防御技术
  - 主机扫描技术
    - 传统技术
      - ICMP Echo
        - Ping的实现机制，发送ICMP Echo Request （type 8）数据包，等待ICMP Echo Reply（type 0）。收到表示可达。
        - 简单、系统支持，但容易被防火墙限制
      - ICMP Sweep
        - 使用ICMP Echo 轮询多个主机
      - Broadcast ICMP
        - 将ICMP请求包的目标地址设为广播地址或者网络地址，则可以探测广播域或整个网络访问内的主机。
        - 只适用于Unix/Linux系统，Windows会忽略这种包，容易引起广播风暴。
      - Non-Echo ICMP
        - 一些其他类型的ICMP类型包，也可以用于判断目的主机状态。
          - Stamp Request（Type 13）
          - Reply （Type 14）
          - Information Request（Type 15）
          - Reply （Type 16）
          - Address Mask Request （Type 17）
          - Reply （Type 18）
    - 高级技术
      - 突破防火墙的限制
      - 异常的IP包头
      - 在IP头中设置无效的字段值
      - 错误的数据分片
      - 通过超长包探测内部路由器
      - 反向映射探测
    - 目的
      - 确认在目标网络上的主机是否可达
  - 端口扫描技术
    - 互联网上的通信，不仅需要知道对方的IP地址，也需要知道通信程序的端口号。
    - 端口号（2的16次方）
      - 0 ~ 1023
        - 熟知端口号，被提供给特定服务使用
      - 1024 ~ 49151
        - 注册端口
      - 49152 ~ 65535
        - 动态端口或者专用端口
    - 全扫描
      - 会产生大量的审计数据，容易被对方发现，但可靠性高。
      - 过程
        - 1.Client 发送 SYN
        - 2.Server 返回 SYN/ACK 表明端口开放
          - 2.Server 放回 RST/ACK 表示端口关闭
        - 3.Client 返回 ACK 表示连接以及建立
          - 3.Client 发送 RST，表示知道 Server 端口关闭
        - 4.Client 主动断开连接
    - 半扫描
      - 隐蔽性和可靠性结余全扫描与秘密扫描之间
      - 过程
        - 1. Client 发送 SYN
        - 2. Server 返回 SYN/ACK
          - 2.Server 返回 RST/ACK 表示端口关闭
        - 3. Client 发送 RST 断开连接
    - 秘密扫描
      - 能有效的避免对方入侵检测系统和防火墙的检测，但使用的数据包在通过网络时容易被丢弃从而产生错误的探测信息
      - 原理
        - 当一个FIN到达一个关闭的端口，数据包被丢弃，返回一个RST数据包
        - 当一个FIN到达一个打开的端口，数据包被丢弃。（不返回RST数据包）
      - 过程
        - 1. Client 发送 FIN（无返回表示端口打开）
        - 2. Server 返回 RST （表示端口关闭）
      - 变种
        - Xmax
          - 打开所有标记（ACK、FIN、RST、SYN、URG、PSH）
          - 过程
            - Client 发送 XMAX（all flags）（无放回表示端口打开）
            - Server 放回 RST （表示端口关闭）
        - Null
          - 关闭了所有标记，将所有标记置空，发送给目标主机。
          - 过程
            - Client 发送 Null （no flags）（无放回表示端口打开）
            - Server 放回 RST （表示端口关闭）
    - 认证扫描
      - 需要建立完整的TCP连接
      - 定义
        - 服务器要求验证客户端的身份，由服务器向客户端的113端口发起认证连接
      - 过程
        - 服务器向客户端TCP 113 端口发起连接，询问客户端该进程的拥有者名称，服务器并写下日志，某某某连接上我的机器，再建立通信。
    - FTP代理扫描
      - 隐蔽性好，难以追踪。但收到服务器设置的限制。
      - 原理
        - 允许数据连接位与控制连接位在不同的机器上，并支持代理FTP连接。
      - 过程
        - 扫描程序首先在本地与一个支持代理的FTP服务器建立控制连接，然后使用PORT命令向FTP服务器声明欲扫描的目的主机的IP地址和端口号，并发送LIST命令。这是FTP服务器会尝试向目标主机指定端口发起数据连接请求。成功会放回150和225，错误会返回425。
    - 远程主机OS指纹识别
      - 是入侵或者安全检测需要手机的重要信息，是分析漏洞和各种安全隐患的基础。
      - 类型
        - 主动协议栈指纹识别
          - 由于TCP/IP协议栈技术标准在RFC文档中描述，但各个公司实现OS不同，通过对比为差异来判断OS类型。
          - 主要技术
            - FIN探测
              - 向目标端口发送FIN，WinNT、CISCO IOS、HP/UX、IRIX的TCP/IP协议栈实现将返回Reset
            - ISN采样探测
              - 寻找初始化序列长度模板与特定OS的匹配方法，如，早些的Unix的是64K长度，新的Unix系统是随机增加长度
            - Dont’t Fragment 位探测
              - 一些操作系统会设置IP头部“Dont’s Fragment”以改善性能，这样可以判断区分远程OS。
            - TCP初始窗口的大小检测
              - AIX 的是 0x3F25
              - NT 和 BSD 是 0x402E 等
            - ACK值探测
              - 有些OS发回所确认的TCP包的序列号
              - 另外一些返回确认序列号加1
            - ICMP出错消息抑制
              - 限制 ICMP出错消息的速率
            - ICMP出错消息回射完整性
              - 返回ICMP出错消息的时候会修改所引用的IP头。
            - TOS服务类型
              - 多数OS会是0
            - 片段处理
              - 对重叠的片段处理上有差异
        - 被动协议栈指纹识别
          - 原理跟主动类似，但从不主动发送数据包，只是被动捕获远程主机返回的包来分析其OS版本
          - 4个方面
            - TTL
            - Windows Size
            - DF（分片位）
            - TOS
  - 端口扫描技术
    - 原理
      - 确认主机是否存活
      - 通过向目的计算机发送ICMP报文，并监听返回，校验与目的计算机的连接。
    - 参数
      - -a
        - 将目标的机器标识转换为IP地址
      - -t
        - 不中断，就一直Ping
      - -d
        - 使用套接字打开调试状态
      - -f
        - 指定flag
      - -c
        - 发送的报文数量
      - -4
        - 强制使用IPv4协议
      - -6
        - 强制使用IPv6协议
      - -p
        - 只打印开始和结束的一些信息
      - -l
        - 指定长度
  - ICMP
    - 用途
      - 网关或者目标机器利用ICMP与源通信
      - 当出现问题时，提供反馈信息用于报告错误
    - 特点
      - 其控制能力并不用于保证运输的可靠性
      - 它本身也不是可靠的
      - 并不用来反应ICMP报文的传输情况
  - Socket
    - 写扫描器，必学技能
      - 网络层的“IP地址”可以唯一标识网络中的主机，而传输层的“协议+端口”可以唯一标识主机中的进程。
      - 三元组（IP地址，协议，端口）就可以标识网络的进程了。
      - TCP/IP协议的应用程序通常使用应用程序接口，UNIX BSD的套接字（Socket）来实现网络进程之间的通信。
    - 在Windows中称为WinSock
    - 基本模式
      - Open
      - Write/Read
      - Close
    - 应用程序通常通过Socket向网络发出请求或者应答网络请求
  - Net use
    - net use \\192.168.1.34\ipc$ password /user:username
      - 以username为用户名，password为密码登陆192.168.1.34
    - net use o: \\192.168.1.34\c$
      - 将远程计算机的C盘映射到本地的O盘
    - net use \\192.168.1.34\ipc$ /delete
      - 删除IPC$连接
    - net use o: /delete
      - 删除共享映射
  - TCP控制位
    - URG
      - 紧急数据标准，为1，表示数据包中有紧急数据。
    - ACK
      - 确认标志位
    - PSH
      - 如果置位，接收端应尽快把数据传送给应用层
    - RST
      - 用来复位一个连接。
    - SYN
      - 建立连接，让连接双方同步序列号。
    - FIN
      - 表示发送端已经没有数据要求传输了，释放连接。
  - 扫描的防御技术
    - 反扫描技术
      - 主动扫描
        - 减少开发端口，做好系统防护
        - 实施检测扫描，及时作出告警
        - 伪装知名端口，进行信息欺骗
      - 被动扫描
        - 信息欺骗
          - 比如返回自定义的banner信息或者伪装知名端口
    - 端口扫描检测工具
      - 蜜罐系统
      - 工具
        - ProtectX
        - Winetd和DTK
        - PortSentry
    - 防火墙技术
      - ZoneAlarm Pro
      - Black ICE
      - Norton Personal Firewall
      - 天网
    - 审计技术
    - 其他防御技术
  - 扫描三部曲
    - 发现目标主机或网络
    - 发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务以及服务软件的版本等。
    - 根据收集到的信息判断或者进一步测试系统是否存在安全漏洞
  - 漏洞扫描
    - 基于漏洞库的特征匹配
      - CGI漏洞
      - POP3漏洞
      - FTP漏洞
      - SSH漏洞
      - HTTP漏洞
    - 基于模拟攻击
      - Unicode遍历目录漏洞探测
      - FTP弱密码探测
      - OPENRelay邮件转发漏洞探测
    - 常用工具
      - SATAN
      - Nmap
      - Nessus
      - X-san
  - Traceroute
    - 参数
      - 指定一个初始 TTL
        - -f
      - 指定一个最大TTL
        - -m
      - 设置目的主机的端口号
        - -p
      - 每次发送探测数据包的个数
        - -q
      - 指定超时的时间
        - -w
  - 网络漏洞
    - 系统软、硬件在安全方面的脆弱性
  - 扫描器
    - 定义
      - 自动检测远程或本地主机安全性弱点的程序
    - 双刃剑
      - 安全评估工具
      - 网络漏洞扫描器
    - 功能
      - 扫描目标主机识别其工作状态
      - 识别目标主机端口的状态
      - 识别目标主机操作系统的类型和版本
      - 识别目标主机服务程序的类型和版本
      - 分析目标主机、目标网络的漏洞
      - 生成扫描结果报告
    - 对计算机网络系统或网络设备进行安全相关简介，找出安全隐患和可被黑客利用的漏洞