**IP网络扫描技术的研究与实践总结**

1. **网络扫描技术**

基于ICMP/TCP/UDP协议进行目标主机扫描，以判断指定网段主机的存在性、端口的开闭性等信息，通过对这些信息的统计分析可以得到目标用户主机的潜在风险，为相关人员规避漏洞和管理主机提供技术支持。

1. **网络扫描技术的原理**

通过端口扫描向目标主机的 TCP/IP 服务端口发送探测数据包，并记录目标主机的响应。通过分析响应来判断服务端口是打开还是关闭，就可以得知端口提供的服务或信息。端口扫描也可以通过捕获本地主机或服务器的流入流出 IP 数据包来监视本地主机的运行情况，它仅能对接收到的数据进行分析，帮助我们发现目标主机的某些内在的弱点。即：

* 1. 扫描目标主机识别其**工作状态**（开/关机）
  2. 识别目标主机的端口状态（监听/关闭）
  3. 识别目标主机系统及服务程序的类型和版本
  4. 根据已知漏洞信息，分析系统脆弱点
  5. 生成扫描结果报告以供分析

1. **常见扫描技术**

* ICMP协议（主机扫描）

网际控制报文协议（Internet Control Message Protocol），是IP的一部分，在IP协议栈中必须实现。主机扫描的目的是确定在目标网络上的主机是否可达。

用途：网关或者目标机器利用ICMP与源通讯；当出现问题时提供反馈信息用于报告错误

特点：不保证可靠性；不用来反映ICMP报文的传输情况

传统技术：ICMP Echo扫描、ICMP Sweep扫描、Broadcast ICMP扫描、Non-Echo ICMP扫描

高级技术：构造IP包

* ICMP Echo扫描：

原理：Ping的实现机制，在判断在一个网络上主机是否开机时非常有用。向目标主机发送ICMP Echo Request数据（type8），等待回复的ICMP Echo Reply包type 0）。如果能收到，则表明目标系统达，否则表明目标系统已经不可达或发送的包被对方的设备过滤掉。

优点：简单、系统支持

  缺点：容易被防火墙限制 （如不响应PING）

* ICMP Sweep扫描：

在ICMP Echo基础上，通过并行发送，同时探测多个目标主机，以提高探测效率。（看作多线程的ICMP Echo）

* Broadcast ICMP扫描：

原理：将ICMP请求包的目标地址设为广播地址或网络地址，则可以探测广播域或整个网络范围内的主机。

缺点：1.只适用于UNIX/Linux系统，Windows会忽略这种请求

2.容易引起广播风暴。

* Non-Echo ICMP扫描：

原理： 利用ICMP协议中非ICMP ECHO的ICMP查询信息类型实现主机扫描，如Timestamp和Timestamp Reply 、Information Request和Information Reply 、Address Mask Request 和Address Mask Reply等。

* 构造IP包：

原理：向目标主机发送构造的IP包，探测对方返回的信息。第三层攻击。

* **TCP协议（端口扫描）** 传输控制协议TCP（Transmission Control Protocol），位于运输层，提供面向连接的服务，在传送数据之前必须先建立连接，数据传送结束后要释放连接。扫描器主要利用TCP协议的三次握手和四次挥手、标志位实现端口扫描。

### TCP标志位

### 

当确定了目标主机可达后，就可以使用端口扫描技术，发现目标主机的开放端口，包括网络协议和各种应用监听的端口

端口扫描技术主要包括以下三类：

* 1. 开放扫描：会产生大量的审计数据，容易被对方发现，但可靠性高。
  2. 隐蔽扫描：能有效避免对方入侵检测系统和防火墙的检测，但这样扫描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。
  3. 半开放扫描：隐蔽性和可靠性介于两者之间。
* 开放扫描技术：主要是TCP Connect扫描

TCP Connect扫描：原理:通过调用socket函数connect()连接到目标计算机上，完成一次完整的三次握手过程。如果端口处于侦听状态，那么connect()就能成功返回。否则，这个端口不可用，即没有提供服务。

优点：稳定可靠，不需要特殊的权限。

缺点：扫描方式不隐蔽，服务器日志会记录下大量密集的连接和错误记录，并容易被防火墙发现和屏蔽。（防火墙发现机制：短时间内某固定的IP地址建立了大量的连接）

* 半开放扫描技术

TCP SYN扫描

原理：扫描器想目标主机发送SYN包。如果应答是RST包，那么说明端口是关闭的；如果应答中包含SYN和ACK包，说明目标端口属于监听状态，在传送一个RST包给目标主机从而停止建立连接。由于SYN扫描事，全连接尚未建立，所以这种技术通常被称为半连接扫描。

优点：隐蔽性比全连接扫描好，一般系统对这种半扫描很少记录。

缺点：通常构造SYN数据包需要超级用户或者授权用户访问专门的系统调用。

TCP间接扫描

原理：利用第三方的IP（欺骗主机）来隐藏真正扫描者的IP。由于扫描主机会对欺骗主机发送回应信息，所以必须监控欺骗主机的IP行为，从而获得原始的扫描结果。扫描主机通过伪造第三方主机IP地址向目标主机发起SYN扫描，并通过观察其IP序列号的增长规律获取端口的状态。

优点：隐蔽性好

缺点：对第三方主机要求较高。

* 隐蔽扫描： 1、TCP FIN扫描 2、TCP Xmas扫描 3、TCP Null扫描 4、TCP ftp proxy扫描 5、分段扫描

**四、实现方案**

* C语言

优势：库比较齐全，有大量模板，实现方便

缺点：单线程效率低下，多线程实现复杂

* Go语言

优势：性能优越**，**兼容性好**，**跨平台编译

缺点：没有相关库及模板，不支持图形化界

目前我想采用go语言，原因是更有挑战，不拘泥于以往C毕设论文的模板，也能通工毕设提高自己网络知识与go编程能力。

目前完成一个测试demo，如下



