网络扫描原理

网络扫描作用：双刃剑（看使用对象和目的），入侵者利用扫描收集信息，管理员用来防范入侵，保障系统安全。

网络扫描步骤：

1.扫描目标主机识别工作状态（开/关机）

2.识别目标主机端口状态（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

下面按步骤给出一些技术需求，也作为学习步骤

1、主机扫描技术

确定目标主机是否可到达，方法是 ping 扫描（基于 ICMP 协议的扫描）

1.ICMP Echo 扫描

发送一个 ICMP ECHO REQUEST（ICMP type 8）包，等待是否收到 ICMP ECHO REPLY(ICMP type 0)

特点：简单实现，但容易被防火墙限制

2.Non-Echo 扫描

发送一个 ICMP TIMESTAMP REQUEST(type 13)或者 ICMP ADDRESS MASK REQUEST(type 13)，看是否响应

特点：可以突破防火墙

1.1 端口扫描技术

1.TCP 扫描

先来说下正常情况下 TCP 的三次握手

1）客户端发一个 SYN 包，带目的端口

2）观察下返回的包：

返回 SYN/ACK 包，说明端口打开在监听；返回 RST/ACK 包，说明端口关闭，连接重置。

3）若返回 SYN/ACK，客户端发一个 ACK,完成这次连接

下面是 TCP 扫描的几种形式

①开放扫描

1:TCP Connect 扫描

与目的主机建立一次 TCP 连接，此时目的主机会将这次连接记录到 log 中

方法：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。

2:TCP 反向 ident 扫描:需要建立完整的 TCP 连接

方法：ident 协议允许(rfc1413)看到通过 TCP 连接的任何进程的拥有者的用户名，

即使这个连接不是由这个进程开始的。

开放扫描特点：产生大量审计数据，容易被发现和屏蔽，但可靠性高

②半开放扫描

1：TCP SYN 扫描：发送 SYN 包，当收到 SYN/ACK 包时，不回 ACK 包给目的主机，立刻发送 RST 包来终止连接，

那么一般很少会被记录，但构造 SYN 包需要较高权限

2.间接扫描：通过第三方 IP（欺骗主机）

半开放特点：隐蔽性和可靠性在①③之间

③隐蔽扫描

又可分为 SYN/ACK 扫描，FIN 扫描，XMAS 扫描，NULL 扫描，TCP ftp proxy 扫描,分段扫描等。SYN/ACK 和 FIN 扫描都直接绕过连接第一步，目的主机会发 RST 来拆除连接，就得到了需要信息。

FIN 原理：当一个 FIN 数据包到达一个关闭端口时候，返回一个 RST，否则就会被简单丢弃不返回，XMAS 和 NULL 扫描相反，XMAS 将 6 个标志位（URG,ACK,RST,PSH,SYN,FIN）全 1，NULL 全 0。

特点：能有效的避免对方入侵检测系统和防火墙的检测，但这种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。

2.UDP 扫描

构造一个空的 UDP 数据包发送，如果目的端口有服务在等待，会返回错误消息，如果关闭，返回 ICMP 端口不可达信息。扫描速度慢，还会丢包，结果也不大准确。

1.2 操作系统探测

目的：得到 OS 信息，以及提供服务的计算机程序的信息

1.二进制信息探测

最简单方式，OS 自动返回

2.HTTP 响应分析

送 HTTP 连接后，分析响应包获得

3.栈指纹分析

不同 OS 和系统架构的多样性，使得协议栈具体实现不同，对错误包响应，默认值等都能提供 OS 依据

1）主动栈指纹探测

主动向主机发起连接，分析收到响应来确定 OS 类型。

方法：FIN 探测，Bogus 标志探测，统计 ICMP ERROR 报文，ICMP ERROR 报文引用。

2）被动栈指纹探测

在网络监听中，分析系统流量，用默认值来猜测 OS 类型，包括 TCP 初始窗口尺寸，Do not Frafment 位，

TCP ISN（初始序列号）采样。

1.3 漏洞扫描

针对某一特定操作系统的特定服务，主要有基于弱点数据库和基于插件两种。