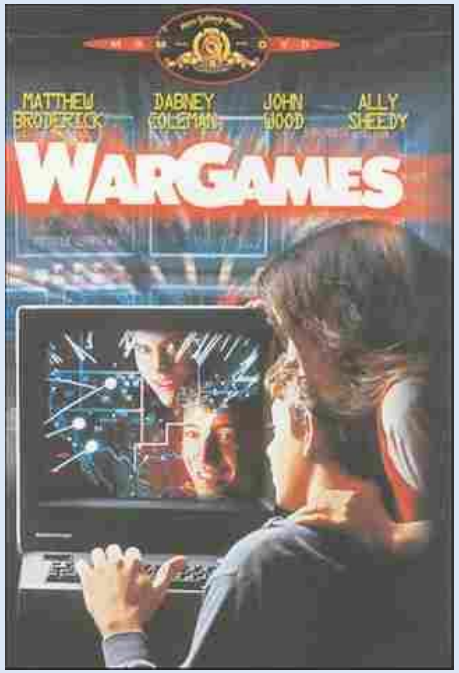
学习目标

黑客概述及目标系统的探测

2.1 概述

2.2 信息收集

2.1 概述



- 凯文•米特尼克是美国20世纪最著名的黑客之一，他是《社会工程学》的创始人
- 《欺骗的艺术》
- 史上5大最危险的黑客
- http://www.bilibili.com/video/av2149309/
- 电影：骇客追缉令

凯文•米特尼克

2.1 概述

黑客

黑客是一个中文词语，皆源自英文hacker，随着灰鸽子的出现，灰鸽子成为了很多假借黑客名义控制他人电脑的黑客技术，于是出现了“骇客”与"黑客"分家。2012年电影频道节目中心出品的电影《骇客（Hacker）》也已经开始使用骇客一词，显示出中文使用习惯的趋同。

实际上，黑客（或骇客）与英文原文Hacker、Cracker等含义不能够达到完全对译，这是中英文语言词汇各自发展中形成的差异。Hacker一词，最初曾指热心于计算机技术、水平高超的电脑高手，尤其是程序设计人员，逐渐区分为白帽、灰帽、黑帽等，其中黑帽（black hat）实际就是cracker。

2.1 概述

网络攻击发展趋势

01

攻击组织化

02

手段体系化

03

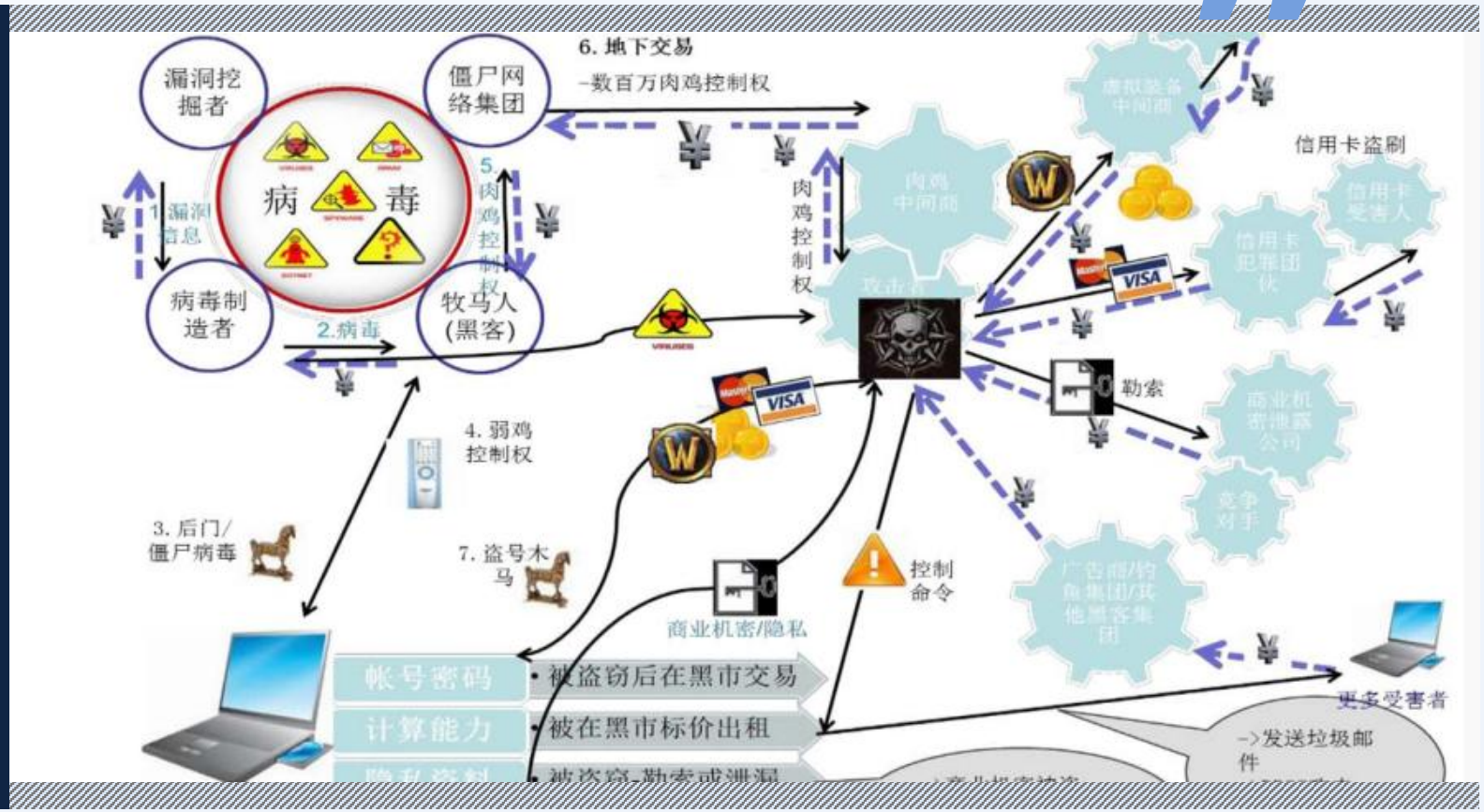
动机利益化

2.1 概述

	传统	现在
动机	对技术的兴趣	政治、经济利益
手段	渗透入侵	木马僵尸网络
危害	拒绝服务	信息泄露

2.1 概述

攻击从个人作战向组织犯罪转变

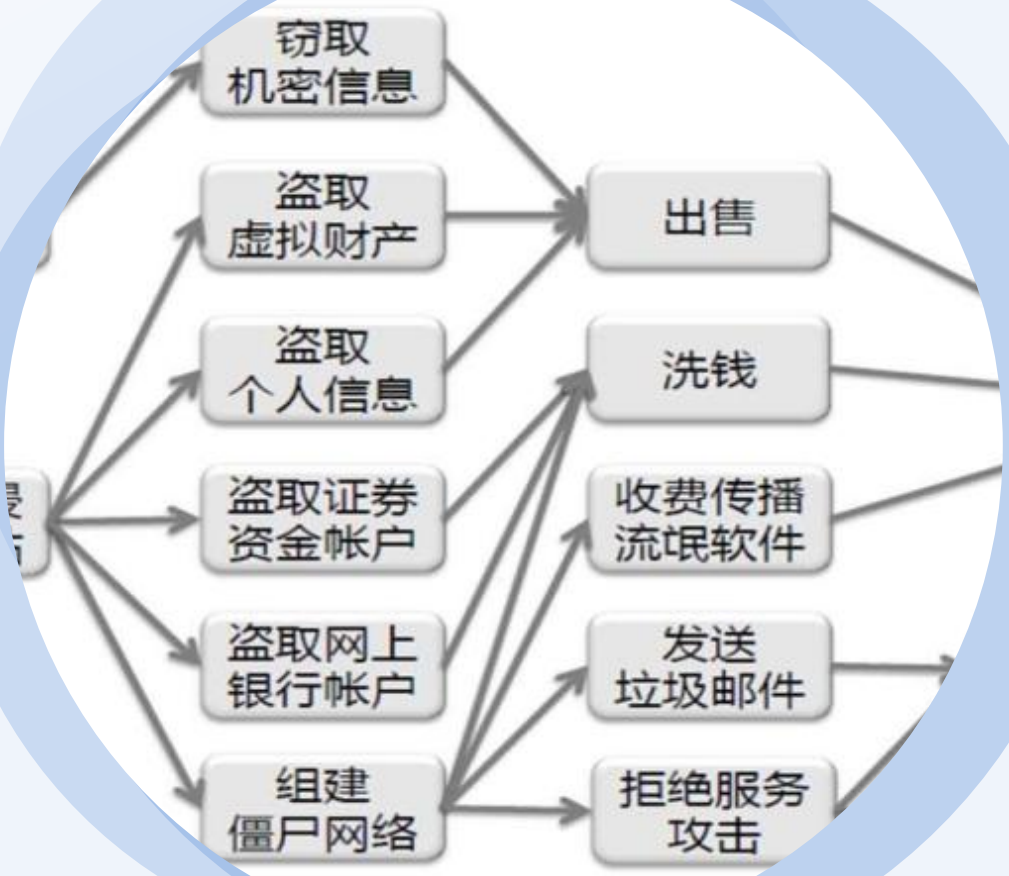


2.1 概述

攻击手段体系化

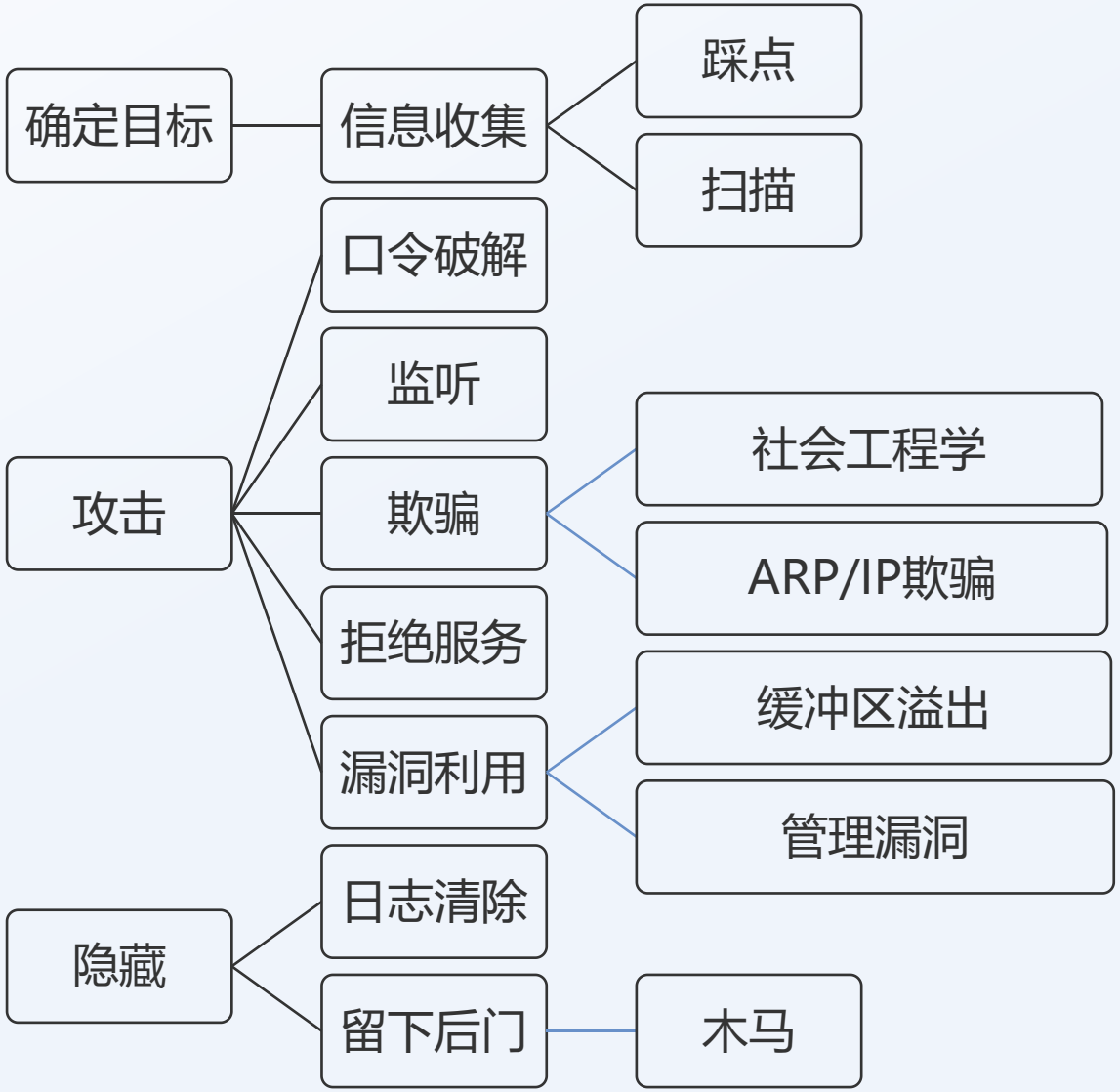
2.1 概述

动机利益化

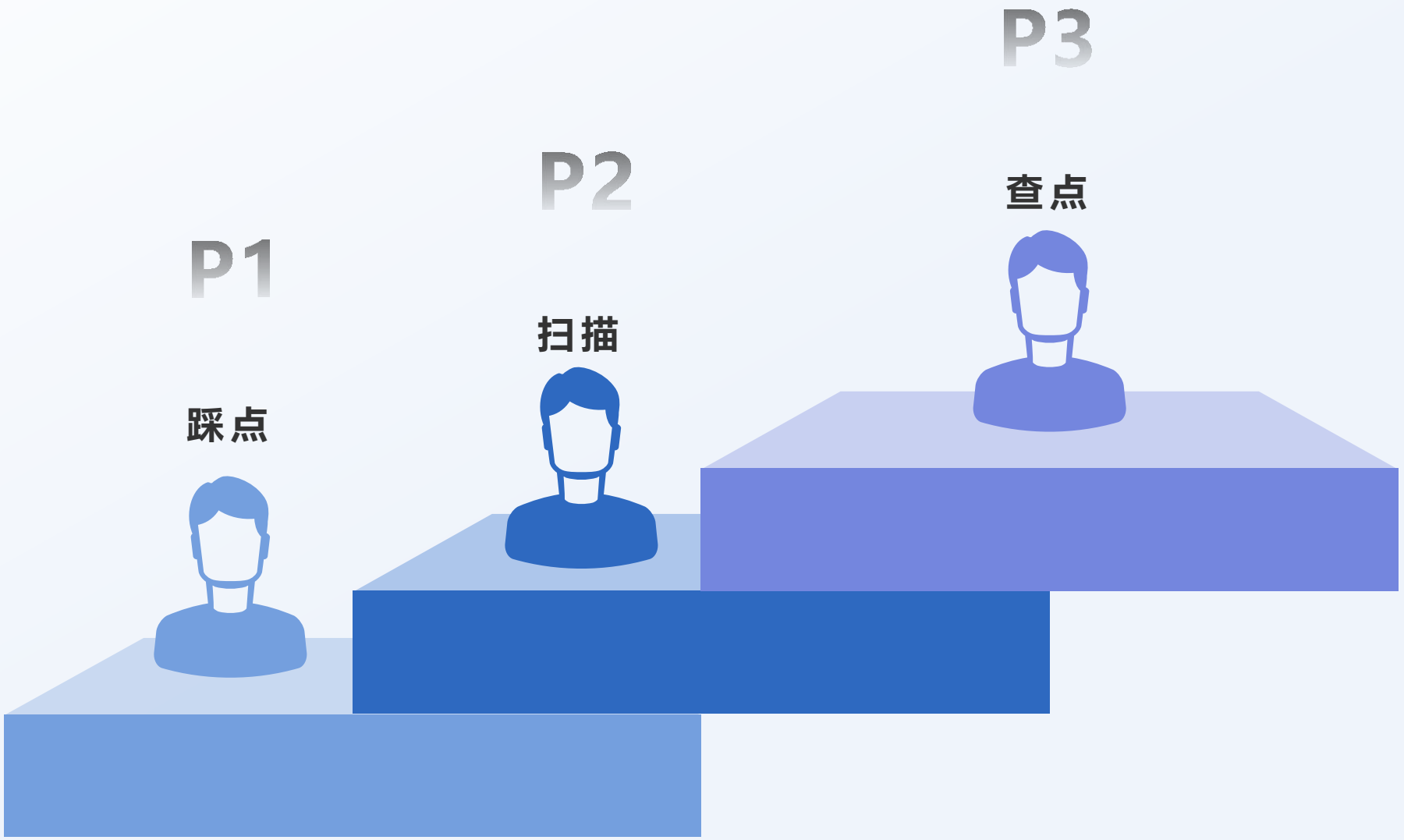

窃取
机密信息
盗取
虚拟财产
盗取
个人信息
盗取证券
资金帐户
盗取网上
银行帐户
组建
僵尸网络
出售
洗钱
收费传播
流氓软件
发送
垃圾邮件
拒绝服务
攻击

2.1 概述

黑客攻击的一般过程



2.2 信息收集



2.2 信息收集

01 网络踩点（footprinting）

OPTION

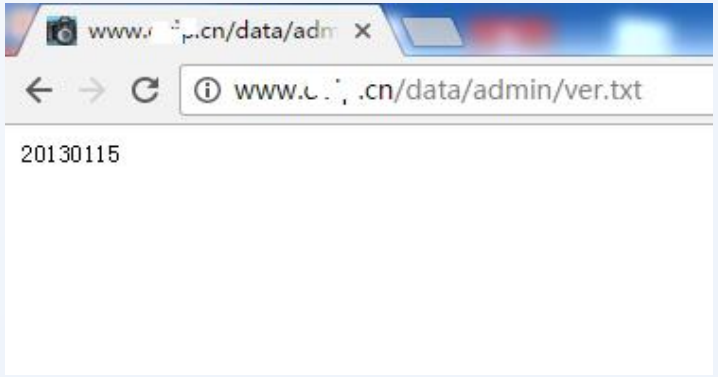
- 瑞典1973 年就颁布了《数据法》， 这是世界上首部直接涉及计算机安全问题的法规。
- 1983年美国公布了可信计算机系统评价准则（TCSEC）简称橙皮书。

02 环境安全

OPTION

- 主机扫描;
- 端口扫描;
- 系统类型探查;
- 漏洞扫描

2.2 信息收集



敏感信息

标题包含Index of：暴露网站的内容细节

网站地址中有data/admin/ver.txt：织梦CMS，暴露过大量漏洞

2.2 信息收集

01 02 03 04

Intitle

搜索范围限定在网页标题

Site

搜索范围限定在特定站点中

Inurl

搜索范围限定在url链接中

Filetype

搜索范围限定在指定文档格式

2.2 信息收集

百度的高级搜索

- 精准匹配，需要加上双引号，不加双引号搜索的结果中关键词可能会被拆分。例如：Windows server “Windows server ”
- 不包含指定关键词的搜索，是通过一个减号（-）来实现的，它的使用语法是前一个关键词与后一个关键词之间用减号连接，且减号的左边是空格，例子： 期末 -考试
- 包含指定关键词的搜索，是通过一个加号（+）来实现的，它的使用语法是前一个关键词与后一个关键词之间用加号连接，且加号的左边是空格，例子： 期末 +考试
- 并行搜索，是通过符号（|）连接关键词的，使用语法是A|B，搜索的结果显示是A 或B，例子：语言|文学

2.2 信息收集

组合应用：intitle:考试 inurl：edu

2.2 信息收集

WHOIS反查

使用邮箱、电话等反查获得更多关联域名信息

域名WHOIS查询

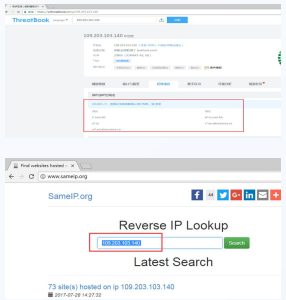
注册人、电话、邮箱、DNS、地址

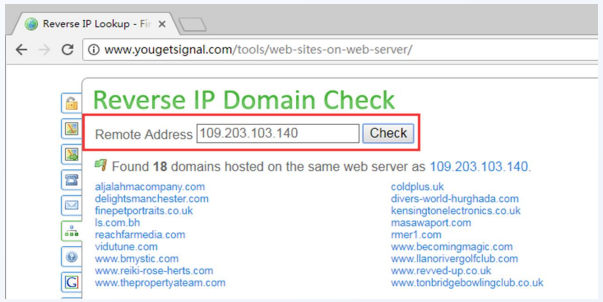
WHOIS查询

IP地址WHOIS查询

网段所属网络名称、国家、地区、管理员

2.2 信息收集





IP地址查询

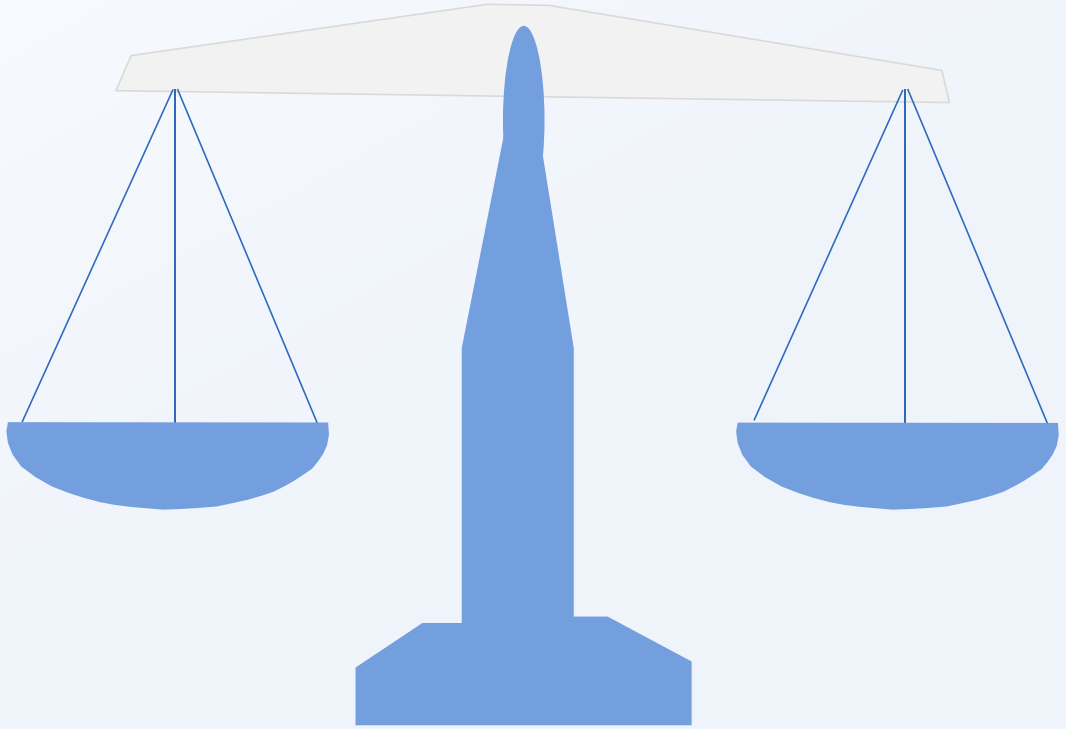
- http://www.sameip.org
- http://www.yougetsignal.com
- http://s.tool.chinaz.com
- https://x.threatbook.cn
- http://www.webscan.cc

2.2 信息收集

扫描器概念

概念

扫描器是检测本地或远程主机（设备）安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。



原理

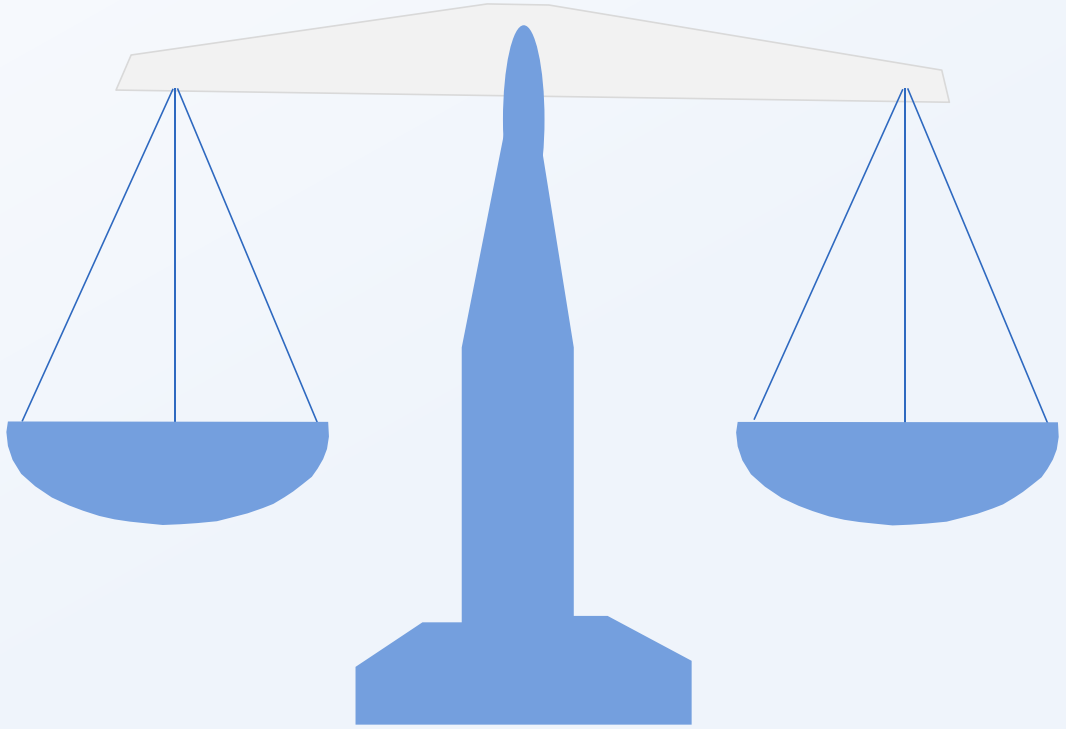
扫描器向目标计算机发送数据包，然后根据对方反馈的信息来判断对方的操作系统类型、开发端口、提供的服务等敏感信息。

2.2 信息收集

漏洞概念

概念

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。



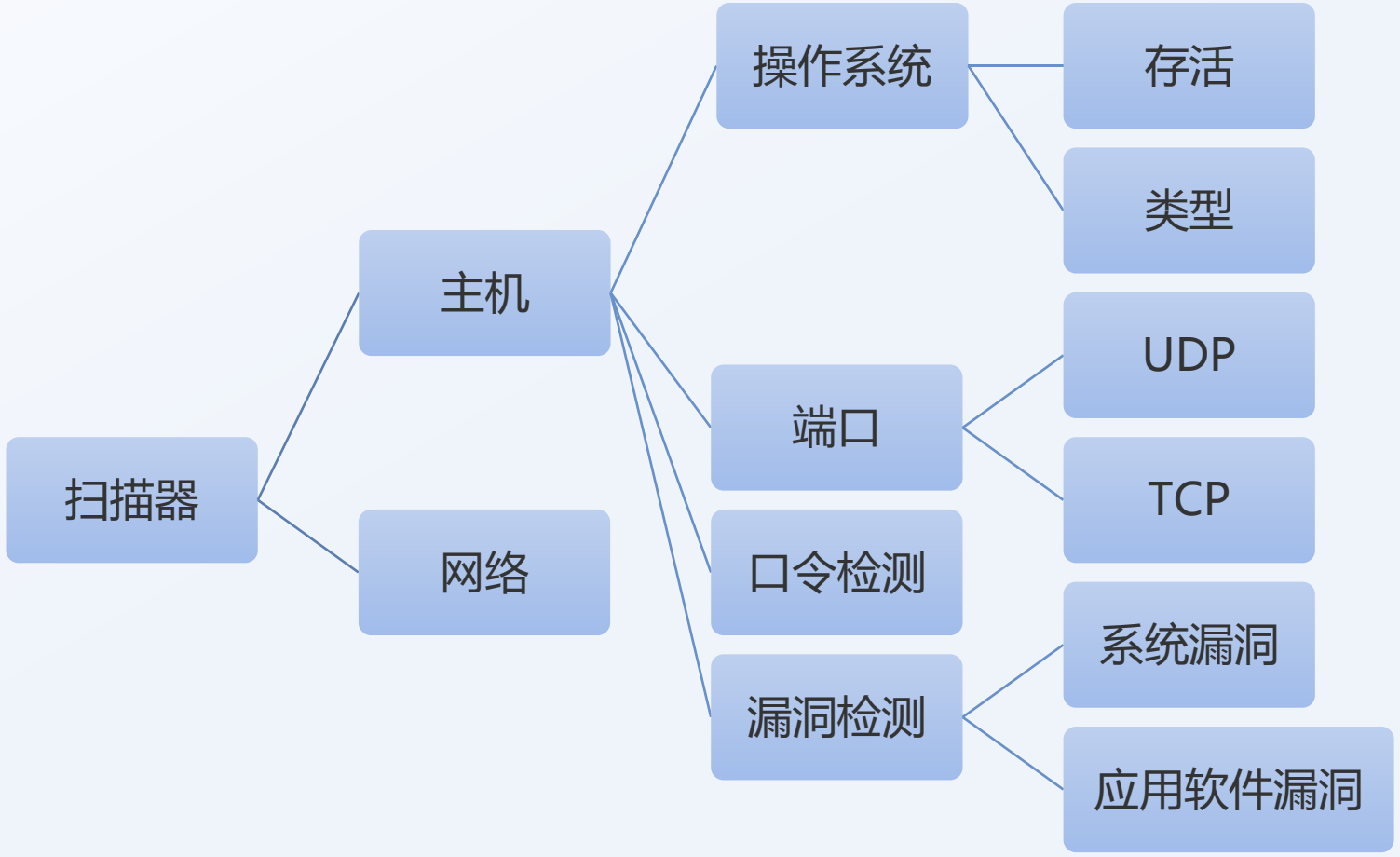
原因

- 软件编写存在bug
- 系统配置不当
- 口令被破解
- （协议）设计存在缺陷

2.2 信息收集

扫描器分类

- 漏洞扫描：是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用的漏洞的一种安全检测（渗透攻击）行为。

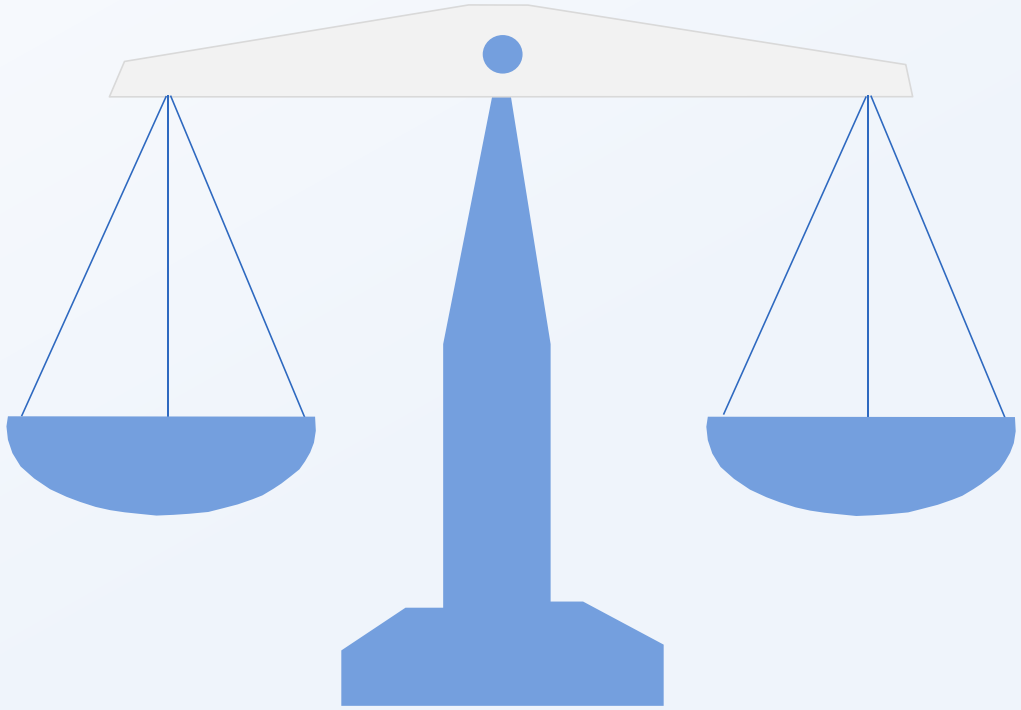


2.2 信息收集

端口扫描

目的

对目标计算机进行端口扫描，可以使用户了解目标系统目前向外界提供了哪些服务。进一步探索该服务是否存在漏洞或者能得到一些有用的信息，从而发现系统的安全漏洞。



原理

从技术原理上来说，端口扫描向目标主机的TCP/UDP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。

2.2 信息收集

TCP数据包

TCP SYN扫描的原理

2.2 信息收集

UDP扫描

ICMP扫描

TCP SYN扫描

UDP主机扫描

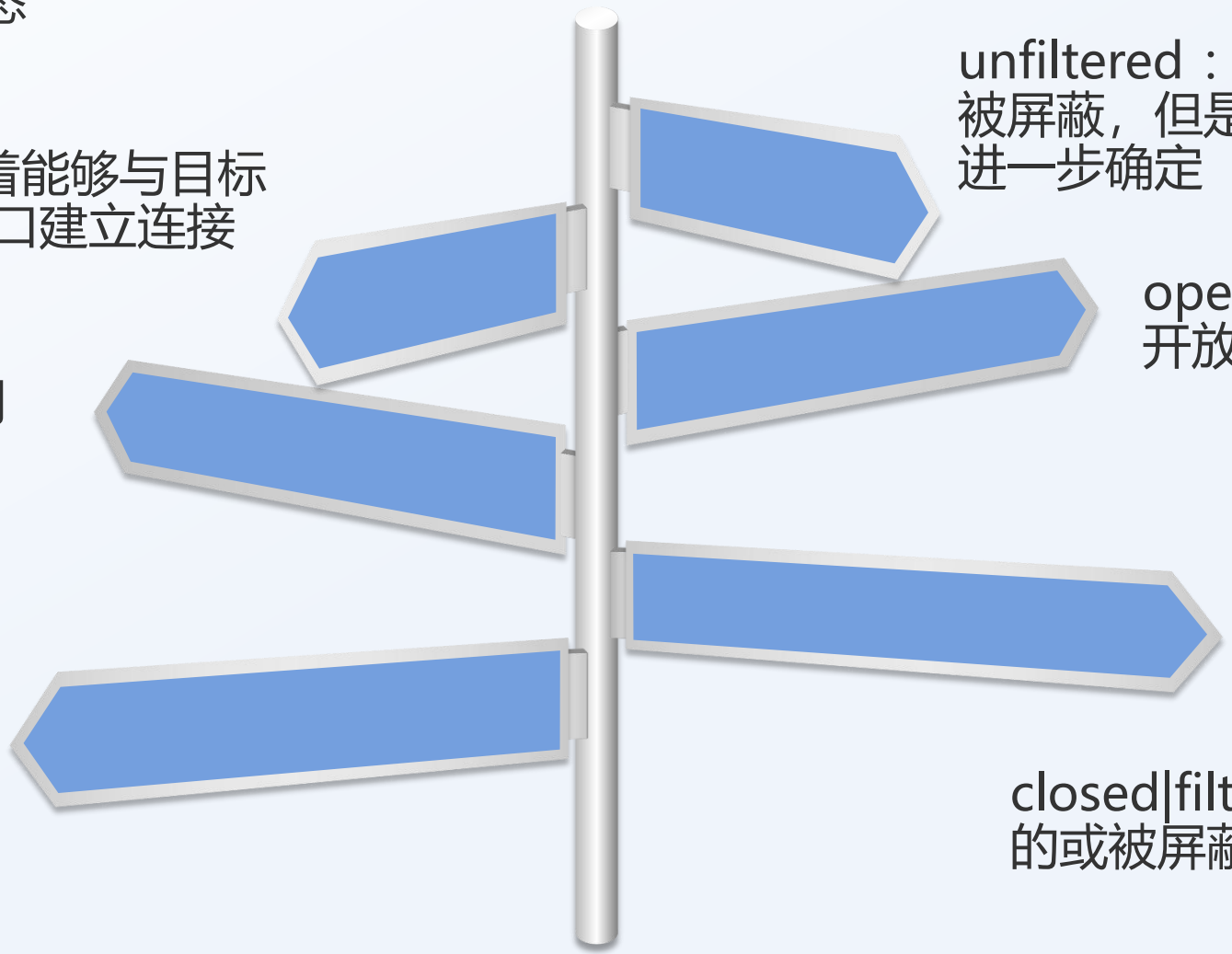
2.2 信息收集

端口的状态

Open：意味着能够与目标主机在这个端口建立连接

closed： 关闭

Filtered：表示防火墙或者其它的网络安全软件掩盖了这个端口，无法确定其状态



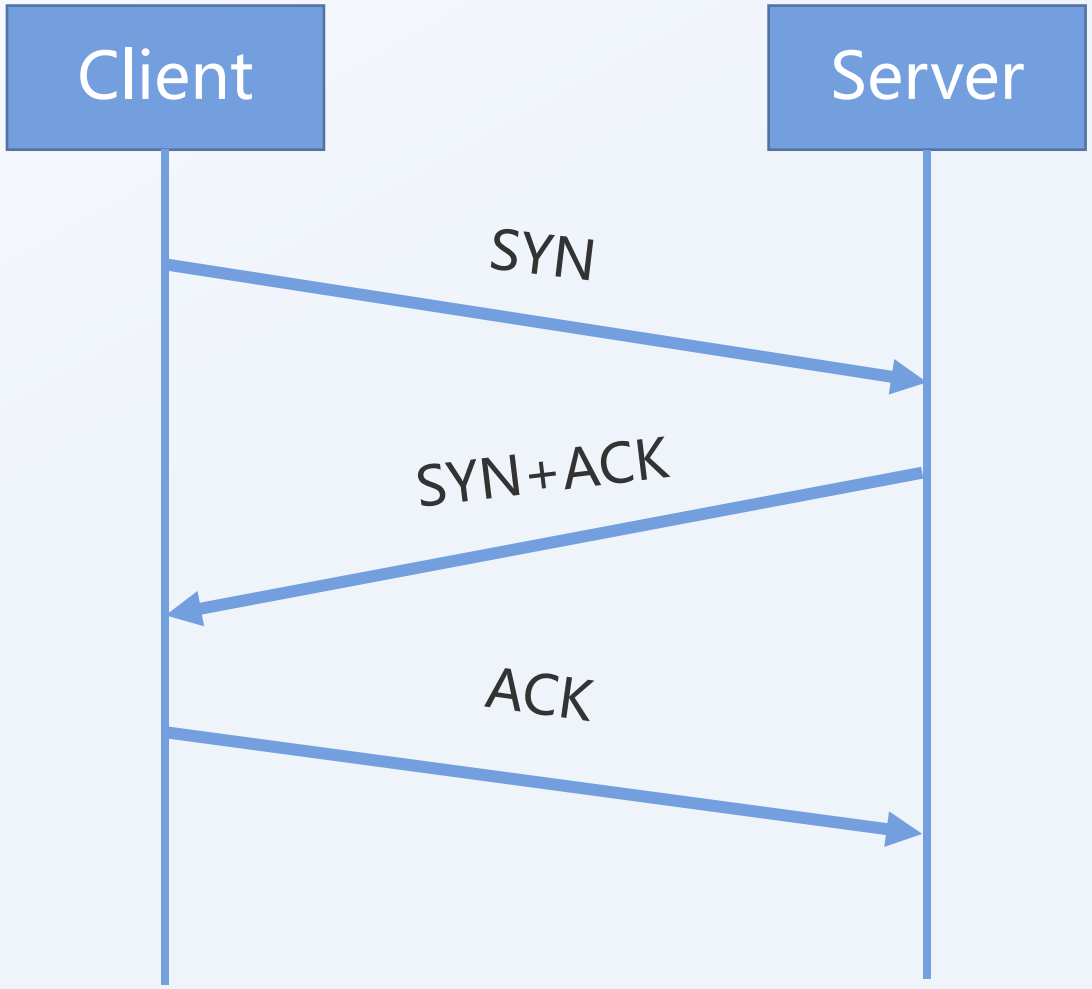
unfiltered： 端口没有被屏蔽，但是否开放需要进一步确定

open|filtered： 端口是开放的或被屏蔽

closed|filtered： 端口是关闭的或被屏蔽

2.2.1 TCP 端口扫描

原理：TCP三次握手



2.2.2 全连接端口扫描

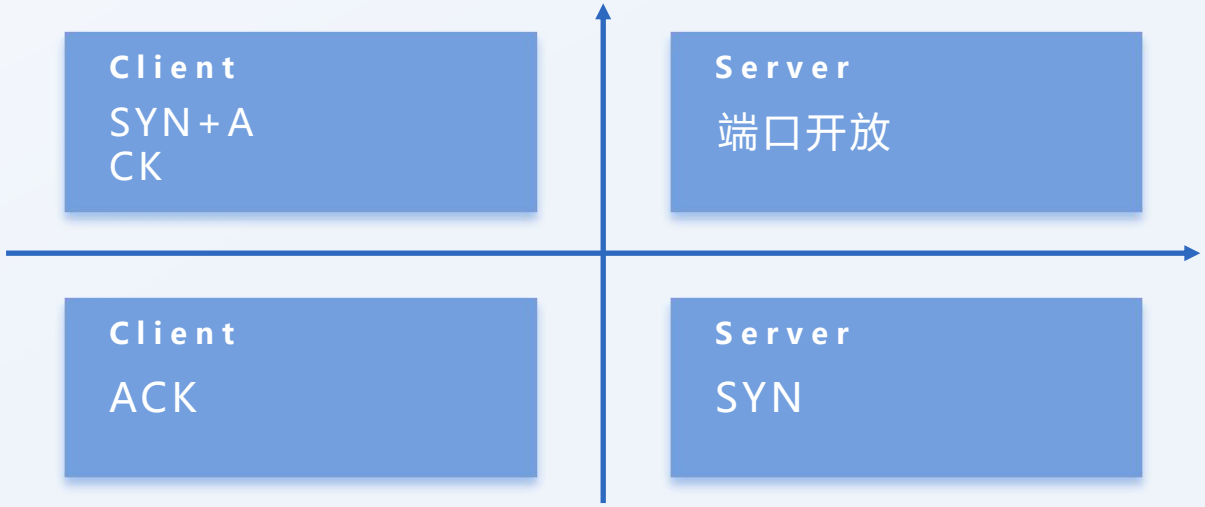
SYN

RST

有的系统回复：
RST+ACK

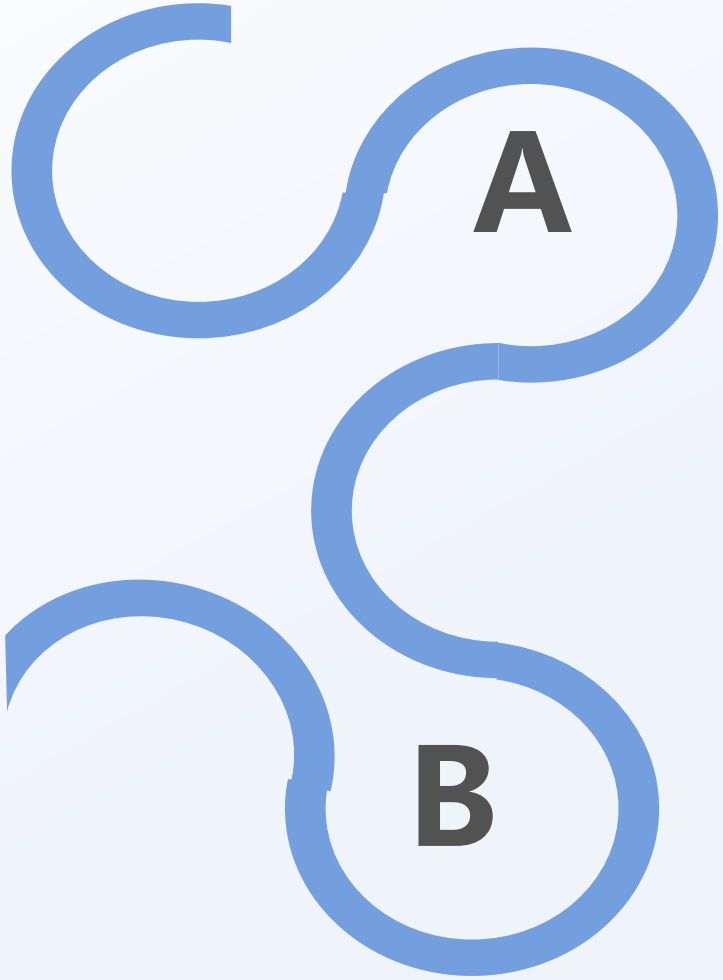
端口关闭

原理



2.2.2 全连接端口扫描

全连接扫描的优缺点



优点

- 不需要管理员权限

缺点

- 效率较低
- 被操作系统记录日志

2.2.3 半开连接端口扫描

原理：三次握手的过程

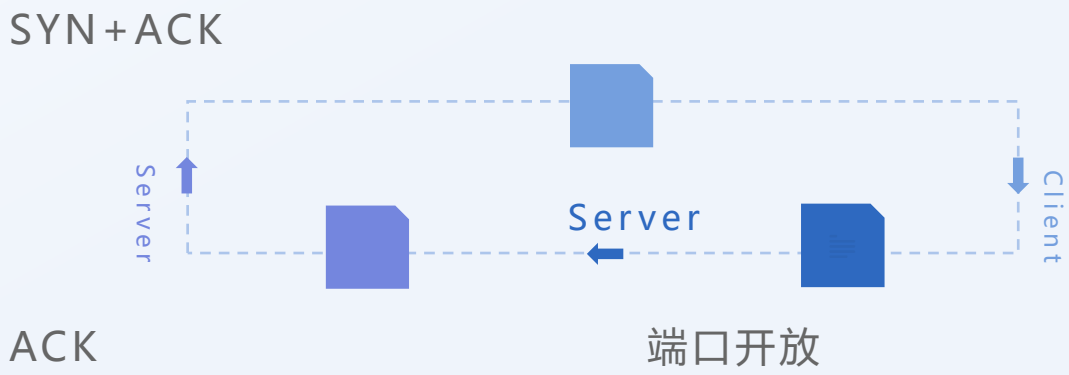
SYN

Client

SYN

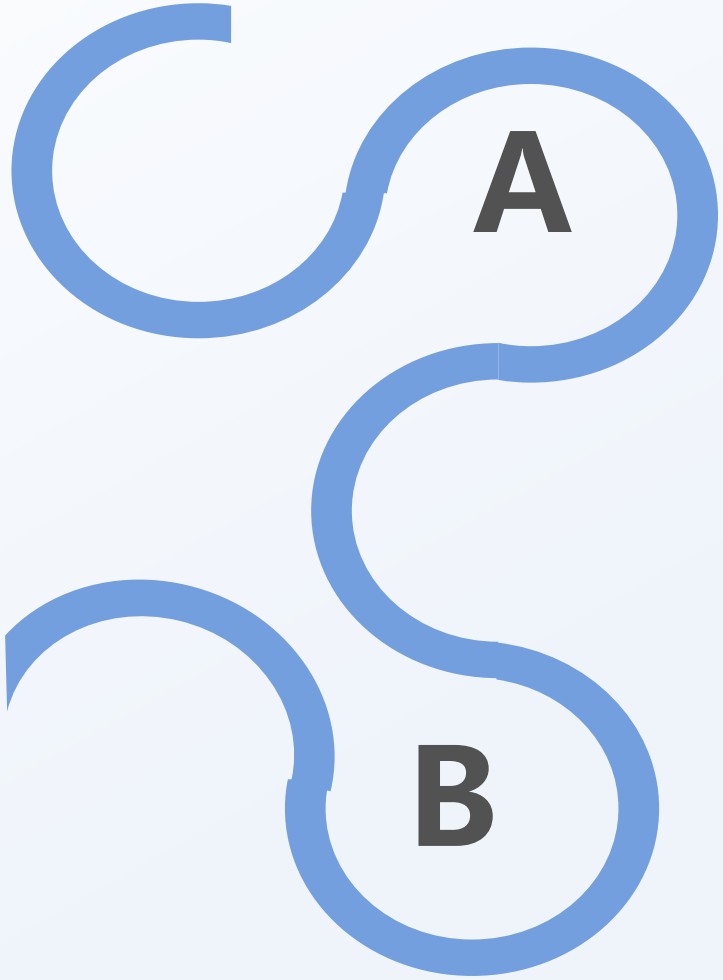
RST

端口关闭



2.2.3 半开连接端口扫描

SYN扫描的优缺点



优点

- 扫描效率高
- 操作系统不记录日志

缺点

- 扫描主机需要管理员权限
- 会被防火墙或IDS记录日志

2.2.4 Nmap扫描主机

TCP同步（SYN）

端口扫描（-sS参数）

TCP connect()

端口扫描（-sT参数）

Ping扫描（-sP参数）

UDP端口扫描

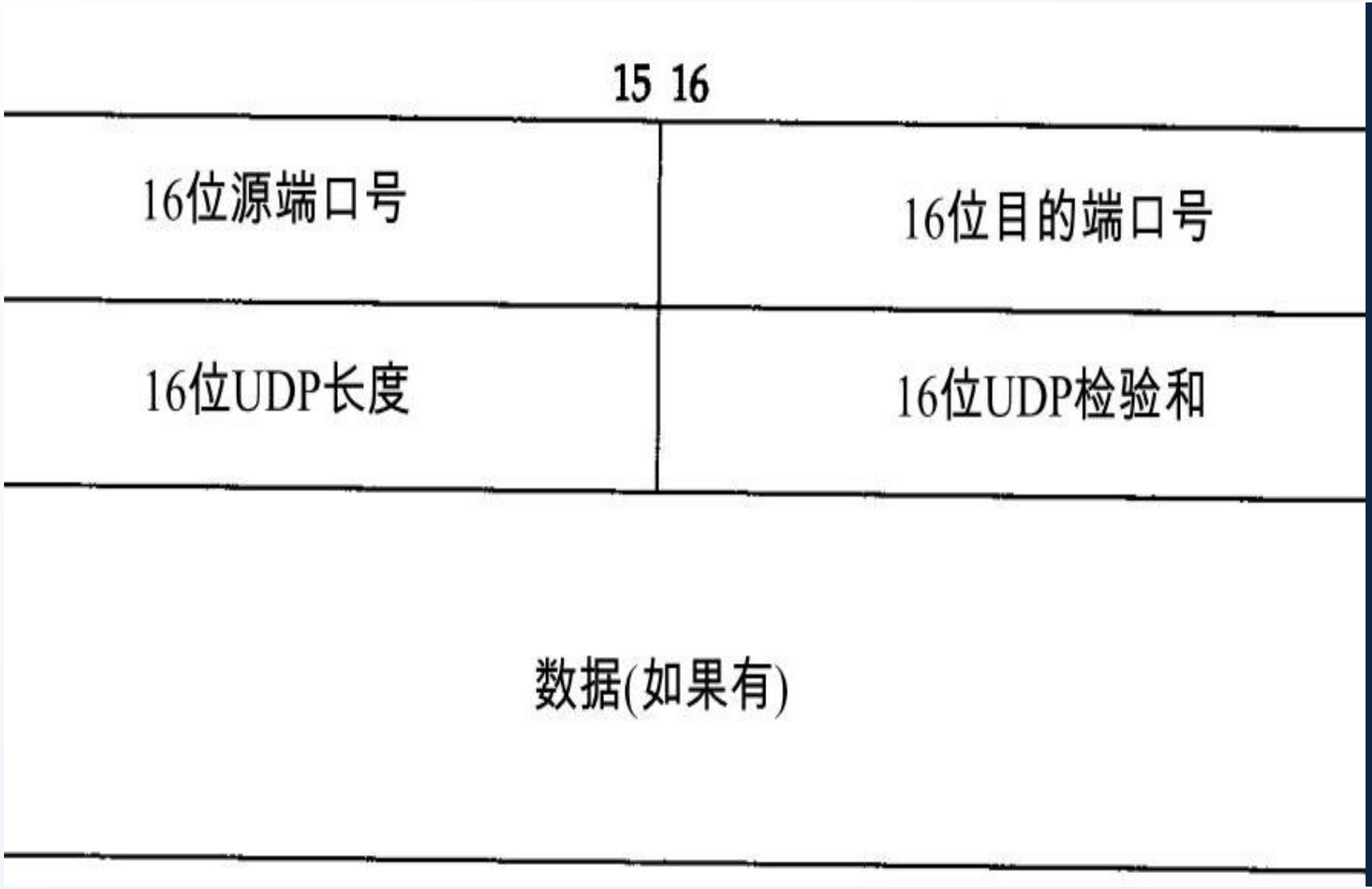
（-sU参数）

2.2.4 Nmap扫描主机

- FIN扫描（-sF）
- 圣诞树扫描（-sX）

其他扫描方式

2.2.4 Nmap扫描主机



UDP主机扫描的原理

2.2.4 Nmap扫描主机

ICMP常用类型

类型	代码	描述
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
5	0	Redirect
8	0	Echo Request

2.2.4 Nmap扫描主机

UDP主机扫描

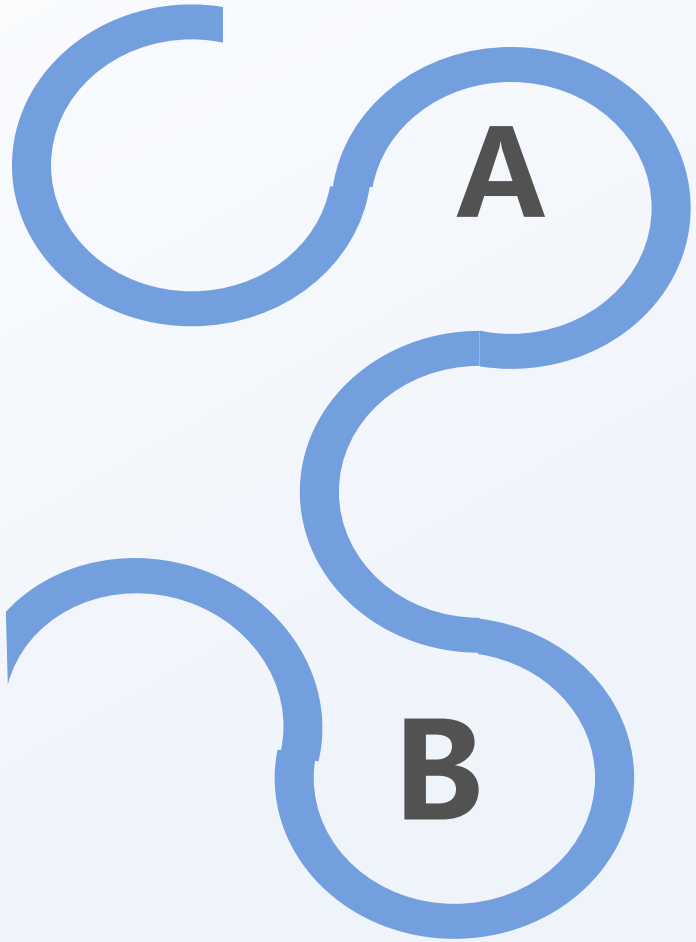
UDP（数据随机）

（端口开放，无响应）

端口关闭ICMP端口不可达

2.2.4 Nmap扫描主机

UDP扫描的优缺点



优点

- 可同时进行主机扫描和端口扫描

缺点

- 需要扫描目标主机关闭的UDP端口
- 返回的ICMP包会被防火墙阻断
- 扫描方需要管理员权限
- 扫描结果不够准确

2.2.4 Nmap扫描主机

应用举例

Nmap工具UDP ping探测主机