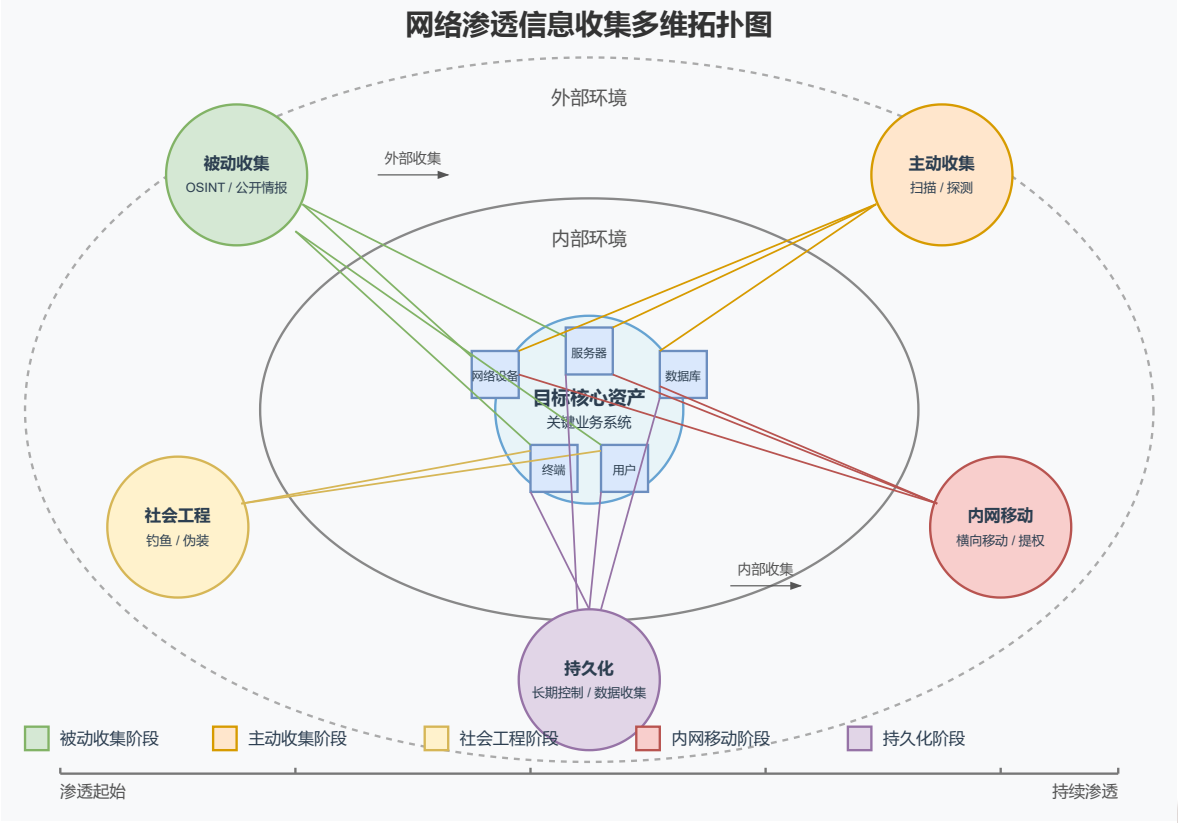
信息收集矩阵

网络渗透信息收集核心矩阵



一、外网信息收集阶段

A. 被动收集阶段

1. 企业资产识别

- **域名信息**
  - 主域名及子域名枚举（DNSdumpster, Sublist3r, Amass）
  -

- 历史DNS记录（SecurityTrails, 网页时光机）
- 域名注册信息（WHOIS查询）
- 相似域名及拼写变体（dnstwist, urlcrazy）

2. 公开情报收集 (OSINT)

- **企业架构信息**
  - 招股书、年报、财报分析
  - 组织架构图重建
  - 股权结构与投资关系图谱
  - 业务线与产品矩阵
- **人员情报**
  - 高管团队信息（LinkedIn, 脉脉）
  - 技术团队成员（GitHub, GitLab, Stack Overflow）
  - 人事变动与招聘信息（招聘网站, 猎头平台）
  - 员工社交媒体分析（Facebook, Twitter, 微博）
- **技术栈识别**
  - 公开演讲与技术分享（技术大会, YouTube）
  - 招聘需求分析（职位描述中的技术要求）
  - 技术博客与知识库文章
  - 开源贡献记录（GitHub, NPM）

3. 数字足迹分析

- **公开代码分析**
  - 代码仓库检索（GitHub, GitLab）
  - API文档分析
  - 移动应用逆向分析
  - 前端代码审计
- **文件元数据分析**
  - 公开文档元数据提取（ExifTool）
  - PDF创建者信息
  - 图片地理位置数据
  - 文档编辑历史
- **云服务资产**
  - AWS S3 Bucket发现
  - Azure Blob存储扫描
  - GitHub Action配置泄露
  - Docker Hub镜像分析

B. 主动收集阶段

1. 网络资产探测

- **IP范围识别**

- ASN查询（ASNmap, Shodan ASN视图）
- BGP路由信息分析
- CDN绕过技术（寻找源IP）
- 反向DNS查询

- **服务枚举**
  - 端口扫描（Nmap, Masscan）
  - 服务版本识别（Nmap, Wappalyzer）
  - TLS证书分析（证书透明度日志）
  - Banner抓取与指纹识别

- **Web应用分析**
  - CMS识别（Wappalyzer, WhatWeb）
  - Web技术栈分析
  - JavaScript依赖识别
  - API端点发现（Burp, FFUF）

2. 漏洞发现

- **自动化扫描**
  - 漏洞扫描器（Nessus, OpenVAS）
  - Web应用扫描（Burp Suite, OWASP ZAP）
  - API安全测试（Postman, SoapUI）
  - 移动应用安全测试（MobSF）

- **手动测试**
  - 登录页面测试
  - 密码策略分析
  - 跨站请求伪造测试
  - 业务逻辑漏洞探索

3. 邮件系统分析

- **邮件服务器配置**
  - SPF记录分析
  - DKIM配置检查
  - DMARC策略评估
  - MX记录枚举
- **邮件地址收集**
  - 公开邮件地址获取（theHarvester）
  - 邮件命名规则推断
  - 邮件格式验证
  - 自动回复信息分析

二、内网信息收集阶段

A. 初始访问后被动收集

1. 系统信息获取

- **操作系统信息**

    - 系统版本与补丁级别
    - 已安装软件清单
    - 系统服务状态
    - 杀毒与EDR解决方案识别
- **用户与权限**
    - 本地用户账户枚举
    - 组权限分析
    - 登录会话识别
    - 密码策略评估
- **配置文件分析**
    - 应用配置文件审计
    - 计划任务检查
    - 自启动项分析
    - 环境变量检查

2. 网络结构分析

- **网络接口**
    - 网卡配置信息
    - 路由表分析
    - ARP缓存检查
    - DNS配置评估

- **网络连接**
  - 建立的TCP/UDP连接
  - 监听端口查看
  - 出站连接分析
  - 进程与端口关联
- **主机通信**
  - 内网流量监听
  - SMB共享发现
  - 内网DNS请求分析
  - 定时通信模式识别

B. 内网主动收集

1. 内网探测

- **网络拓扑**
  - 内网存活主机扫描
  - 网段划分识别
  - 网络设备发现（路由器、交换机）
  - 网络拓扑图绘制
- **服务发现**

    - 内网服务枚举
    - 内部Web应用发现
    - 数据库服务识别
    - 文件共享服务检索
- **域环境分析**
    - 域控制器识别
    - 域用户与组枚举
    - 域信任关系分析
    - Active Directory结构图

2. 凭证收集

- **本地凭证**
    - 凭证转储（Mimikatz）
    - 配置文件中的密码
    - 浏览器保存的凭证
    - 本地密码哈希提取
- **域凭证**
    - Kerberos票据提取
    - NTDS.dit分析
    - 组策略偏好密码
    - 服务账户凭证

- **应用凭证**
  - 数据库连接字符串
  - API密钥与令牌
  - SSH密钥文件
  - 配置文件中的加密凭证

3. 数据价值评估

- **敏感数据定位**
  - 文件共享内容分析
  - 数据库架构与内容审查
  - 业务关键系统识别
  - 知识产权资产定位
- **数据流分析**
  - 信息流向追踪
  - 数据处理流程图
  - 关键业务流程识别
  - 数据备份策略分析

三、社会工程与高级战术

A. 社会工程准备

1. 目标人员分析

- **心理画像**

    - 个人兴趣与爱好收集
    - 社交媒体行为分析
    - 工作习惯推断
    - 性格特征评估
- **社交关系图谱**
    - 同事关系网络
    - 上下级链接关系
    - 外部合作伙伴关系
    - 私人社交圈分析
- **行为模式识别**
    - 工作时间规律
    - 常用设备偏好
    - 通讯工具使用习惯
    - 决策模式分析

2. 攻击载体准备

- **钓鱼素材设计**
    - 目标企业邮件模板克隆
    - 定制化文档创建
    - 诱饵内容设计（基于目标兴趣）
    - 虚假登录页面构建

- **伪装身份构建**
  - 虚假社交媒体账号
  - 伪造联系人网络
  - 可信度建设策略
  - 角色扮演准备

B. 高级持续收集

1. 长期监控

- **行为基线建立**
  - 正常活动模式记录
  - 网络流量基线
  - 用户行为基线
  - 系统活动基线
- **异常检测规避**
  - 低频率操作策略
  - 噪音基线内活动
  - 合法工具使用
  - 活动时间与目标时区同步

2. 横向移动准备

- **权限边界图**

- 不同权限域识别
- 信任关系图谱
- 跨域访问路径
- 访问控制列表分析

- **弱链接识别**
  - 过度授权账户发现
  - 不安全的信任关系
  - 遗留系统接口
  - 管理便利性配置

3. 持久化机制准备

- **长期访问机制**
  - 恶意植入物规划
  - 启动项检查
  - 定时任务设计
  - 触发式后门规划

- **隐蔽通信通道**
  - 合法协议隧道
  - 外部控制基础设施
  - 数据渗出路径
  - 检测规避技术