# 识别保护机制

## 网络保护

* + 1. “简单”的数据包过滤器（js、输入验证等）
    2. 流量整形设备（是一种主动调整流量输出速率的措施，下游设备入接口处可能出现流量拥塞的情况将上游不规整的流量进行削峰填谷，输出一条比较平整的流量）
    3. DLP systems（<https://searchinform.com/infosec-blog/dlp-systems/> protect companies from leaks of sensitive data ，analyze all outgoing and sometimes incoming information）
    4. 加密/隧道：第2层隧道协议对应于OSI模型的数据链路层，使用帧作为数据交换单位。PPTP（点对点隧道协议）、L2TP（第二层隧道协议）和L2F（第2层转发协议）都属于第2层隧道协议，是将用户数据封装在点对点协议（PPP）帧中通过互联网发送。第3层隧道协议对应于OSI模型的网络层，使用包作为数据交换单位。IPIP（IP over IP）以及IPSec隧道模式属于第3层隧道协议，是将IP包封装在附加的IP包头中，通过IP网络传送。无论哪种隧道协议都是由传输的载体、不同的封装格式以及用户数据包组成的。它们的本质区别在于，用户的数据包是被封装在哪种数据包中在隧道中传输

## 基于主机的保护

* + 1. 堆/栈保护（空间分配：栈【操作系统自动分配，一级缓存用完即消除，先进后出的数据结构】 堆【一般程序员分配，二级缓存由回收算法实现】）
    2. 白名单
    3. 杀毒软件、过滤、行为分析

## 应用级保护

* + 1. 确定应用程序的保护
    2. ？编码选项
    3. 潜在旁路途径
    4. 白名单的网页

## 储存保护

* + 1. LUN Masking HBA-主机级别

(HBA: <https://www.cnblogs.com/airoot/p/10673090.html> HBA就是指Host和I/O BUS直接的一个适配器)

* + 1. ISCSI CHAP Secret 储存控制器（质询握手身份验证协议）

# 足迹

## 外网足迹

### 确定客户范围

* + 1. Whois查询
    2. Bgp looking glasses（bgp数据库 <http://www.bgplookingglass.com/> 1. 确认某个区域/ISP的用户访问自己的服务时走的路线。2. 在使用自己的BGP网络对外宣告地址时，需要看看自己的ISP是否真的接受了对应的路由。）
    3. 附属公司
    4. 第三方鉴定权和审核
    5. 核实的顾客
    6. 新闻组领导
    7. Mailing list领导
    8. Robtex（作用：查询rbl 网址：<https://www.robtex.com/> RBL是郵件過濾設備的基本功能之一，在郵件進入設備檢查之前，就可以從來源IP判斷該封郵件的真實性。）

### 被动式侦察

1. 搜索引擎黑客
   1. Google
   2. Yahoo
   3. Bing
2. 手动浏览
3. Shodan、zoomeye

### 活动足迹

1. 端口扫描
2. Banner Grabbing（获取banner信息 五种方式 <https://www.hackingarticles.in/5-ways-banner-grabbing/>）
3. Dns区域传输（讲解以及漏洞验证<https://www.jianshu.com/p/df9acb344026> ）
4. ？SMTP Bounce Back
5. PHP，ASP，easy targets Web应用程序语言映射
6. SNMP Sweeps(SNMP sweeps are often good at finding a ton of information about a specific system or actually compromising the remote device)
7. 正向/反向DNS
8. DNS穷举
9. 网站镜像 网站版本大全

（<http://webcache.googleusercontent.com/search?q=cache:https://archive.org/web/&strip=0&vwsrc=0>）

1. Robots.txt

### 建立目标列表

1. 测绘版本
2. 确认补丁升级
3. 寻找弱的web应用程序
4. Identify lockout threshold（认证限制次数，防止爆破）
5. 基于错误（网站的回显的报告错误）
6. 确定比较弱的端口（端口扫描工具）
7. 过时的系统
8. 虚拟话平台与虚拟机
9. 储存基础架构

## 内部足迹

#### 活动足迹

1. 端口扫描
2. SNMP Sweeps
3. Dns区域传输
4. SMTP Bounce Back
5. 正向、反向DNS
6. Banner Grabbing
7. Voip的映射
   1. 扩展
   2. 特殊的邮箱
   3. 认证
8. Arp发现/Arp Discovery
9. DNS发现/DNS discovery

#### 被动式探测

1. 被动式探测、数据包嗅探、广播流量曲线变化分析
   1. ARP
   2. NetBios
   3. Other UDP
2. 建立目标列表
   1. 测绘版本
   2. 确认补丁升级
   3. 寻找弱的web应用程序
   4. Identify lockout threshold（认证限制次数，防止爆破）
   5. 基于错误（网站的回显的报告错误）
   6. 确定比较弱的端口（端口扫描工具）
   7. 过时的系统
   8. 虚拟话平台与虚拟机
   9. 储存基础架构

# HUMINT（人工情报）

1. 关键员工
2. 合作伙伴/供应商
3. 社会工程

# 隐蔽收集

## 现场收集（on-location gathering）

1. 物理安全检测
2. 无线扫描/RF频率扫描
3. 员工行为培训考察
4. 访问/临近设施（共享空间）
5. 垃圾箱
6. 使用的设备类型

## 非现场搜集

1. 数据中心位置
2. 网络供应商

# 目标选取

1. 管理员
2. 高水平雇员
3. 随机雇员（临时工？）
4. 员工w/特别访问权限
   1. 开发
   2. 工程师
   3. 会记
   4. 销售

# OSINT

## 企业

### 物理

1. 地点
   1. 业主
   2. 土地/税务记录
   3. 公用/单独
   4. 时区
2. 普遍性
3. 人际关系

### 逻辑

1. 业务合作伙伴
2. 竞争对手
3. Touchgraph？
4. Hoovers profile？（美国的公司信息收集）
5. 产品线
6. 立体市场Market Verticle

### 组织结构图

1. 位置识别
2. 交易
3. 关联公司

### 电子

1. 文档/数据源泄露
2. 营销传播
3. 资产
   1. Network blocks owned
   2. 电子邮件地址
   3. 外部基础设置
   4. 使用过的技术
   5. 采购协议
   6. 远程访问
   7. 应用程序使用情况
   8. 防御技术
   9. 人员能力
4. 金融
   1. 报告
   2. 市场分析
   3. 贸易投资
   4. 历史价值

## 个人雇员

### SOCNet Profile

* 1. 元数据泄露
  2. Tone
  3. 频率
  4. 位置感知
     1. Bing地图应用（<https://www.bing.com/maps>）
     2. 四方（<https://map.51240.com/zhongguo__map/>）
     3. 谷歌纵横（已关闭，代替：Trusted Contacts（可信联系人），qq好友位置共享、百度地图好友位置查找）
     4. Yelp（<https://www.yelp.com/> 地图，查询吃喝帮助等信息）

### 社交媒体

* + 1. Facebook/openbook
    2. Linkedin
    3. Xing（<https://www.xing.com/> 是一个以就业为导向的德国社交网站，可以输入姓名进行查询）
    4. Twitter
    5. Blogger/blogpot
    6. Myspace（<https://myspace.com/> Myspace是一个社交网络服务网站，可以进行搜索）
    7. Wordpress
    8. Livejournal（<https://www.livejournal.com/> 是一个在互联网上提供写作的虚拟社区服务）
    9. Foursquare（<https://play.google.com/store/apps/details?id=com.joelapenna.foursquared&hl=en_US> app 是一个提供用户定位的社交网络服务，它提供移动设备软件和游戏。）
    10. Yahoo
    11. Google profile
    12. Flickr（<https://www.flickr.com/> 为一家提供图片分享的虚拟网络相册）
    13. Picfog（[https://www.crunchbase.com](https://www.crunchbase.com/) ）
    14. DeviantArt（<https://www.deviantart.com/> 是一个为艺术家展示各自作品、并交流讨论而设计的社交网路服务网站）
    15. Aim
    16. Irc
    17. Icq
    18. Qq
    19. JUST USE NAMECHK or something likeit (<https://namechk.com/> )

### 互联网足迹

* 1. Email地址
  2. 用户名/Handles
  3. 个人域名
  4. 静态ip

1. Bloggosphere（<https://www.urbandictionary.com/define.php?term=bloggosphere> 也称网志空间或部落格空间，是博客、博客作者及其社群的统称）

### 移动足迹

1. 电话号码
2. 手机类型
3. 使用情况
4. 安装的应用程序
5. 所有者/管理员