## 探测行为检测与防护方案调研

## 探测行为识别技术

### 设备实体探测行为识别

目前,最为主流的设备探测技术依然是基于指纹实现的,如Shodan、Zoomeye、Censys以及各类漏洞扫描产品,基本原理是对目标设备进行网络扫描,根据响应包中的多个字段信息构造设备指纹,如开放端口号、会话方式及协议等,同指纹库进行匹配,确定探测的设备类别。因此,通过识别指纹探测行为,可以有效识别相应设备的探测行为。

为了细粒度地识别设备探测行为,可根据设备指纹库将设备分类,基于不同类别设备的探测方法的差异性,识别探测数据包。根据网络空间大多数设备已有相应的分类命名规则,确定每类设备的网络扫描方法,识别网络扫描数据包的格式,提取特征,归纳聚合,建立设备探测行为指纹库。

扫描程序发出的请求数据包和常规请求数据包之间往往存在内容上的差异,这些差异可以被用作识别探测行为的指纹。例如,Nmap在进行操作系统扫描时,发送的UDP数据包中默认使用字符“C”填充数据部分,而在ICMP数据包中使用“0”填充,同时,扫描时默认的TCP窗口大小字段固定为“1024”;Zmap在扫描时使用固定的IPID“54321”以及固定的窗口大小“65535”。针对部分未知类别的设备,通过深入分析设备探测行为的模式,将其与已知类别设备的探测行为模式相比较,采用相似性度量方法,将其归类为最相似的类别,从而识别针对该设备的探测行为。

### 应用服务探测行为识别

针对应用服务的探测主要有端口扫描和漏洞扫描。端口扫描是向目标系统发送探测数据包,旨在探测网络主机是否存在开放端口和其他可用服务;漏洞扫描是在端口扫描的基础上,将扫描结果同漏洞库数据进行匹配,进一步识别应用服务类型、版本等信息。

为了识别应用服务探测行为,首先应分析系统端口的开放状态,并且记录探测方访问应用服务时留下的信息,进而通过分析探测数据包、提取报文特征、建立数学模型、数据可视化等方式,并结合统计学方法、人工智能算法或其他启发式方法识别探测行为。

为了识别应用层的探测行为,我们可以通过HTTP的状态码、URL长度、User-Agent字段等特征来区分探测程序发出的请求和正常请求。例如,Web漏洞扫描器Awvs(AcunetixWebVulnerabilityScanner)在请求的URL、Headers、Body等字段包含了“by\_wvs”、“acunetix\_wvs\_security\_test”等能代表自己的特征字符串;Sqlmap在User-Agent中包含了“sqlmap”这个特征字符串。

### 局限性

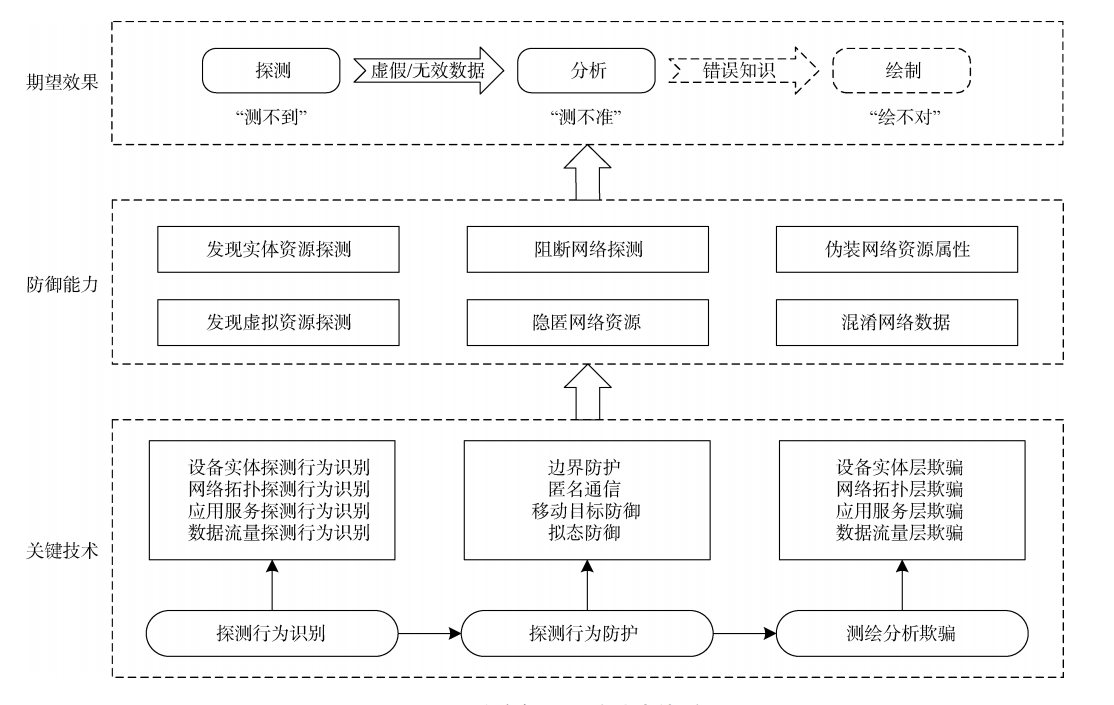
设备实体探测和应用服务探测行为识别依赖于对扫描工具的指纹构建,但通常有经验的攻击方会基于开源的扫描工具进行二次开发,刻意改变默认字段、请求负载等指纹特征,从而使得原有的指纹信息失效。扫描工具的行为模式、流量统计信息等特征也在时刻变化,加大了统计学方法、人工智能算法或其他启发式方法的识别难度。

### 流量行为分析

针对以上局限性，我们可以分析流量行为，总结出不同扫描器或者搜索引擎的扫描行为规律，进而确定其扫描行为。

## 探测行为防护和欺骗技术

### 框架



### 描述

探测行为的防护技术需要同时具备：阻断测绘方的探测行为和隐匿己方网络空间资源的能力。一方面, 使测绘方的探测受阻, 难以获取到分析建模阶段所需的数据, 另一方面, 使测绘方仅能够获取到动态、随机、多样的无效数据, 进而, 使得测绘方陷入数据不足或数据无效的困境, 使其无法实现网络路径重构、拓扑分析、资源映射等目标。

探测行为防护的主要技术概括为四个方面: 基于边界的防护、基于匿名通信技术的防护、基于移动目标防御技术的防护以及基于拟态防御技术的防护。

### 基于边界的防护

借鉴防火墙、入侵检测与防御等基于边界的防护技术, 有效发现并阻断探测行为。

1. 访问控制

配置防火墙的访问控制列表（ACL）控制数据的流入流出；同时结合NAT/PAT技术隐藏内网设备的IP地址。

1. 入侵检测与防御

入侵检测系统(Intrusion Detection System,IDS)旨在识别传统防火墙无法识别的恶意流量和非授权的访问, 对于充分保证网络的机密性、完整性和可用性至关重要。分为基于签名的入侵检测系统(Signature-based Intrusion Detection Systems,SIDS)和基于异常的入侵检测系统(Anomaly-based Intrusion Detection Systems,AIDS)。前者如：Snort和NetSTAT；后者又进一步可以分为三大类: 基于统计的、基于知识的以及基于机器学习/深度学习的。

入侵防御系统(Intrusion Protection System,IPS)是一种主动保护系统,是IDS 的进一步发展。IPS能够监视网络或网络设备间的数据传输, 即时中断、调整或隔离一些不正常或是具有伤害性的行为。

1. 不足

基于边界的防护在阻断探测行为方面虽然有着不错的效果, 但是仍有不足之处。在制定访问控制策略、确定网络隔离的力度等方面仍然需要较多的人为干预,通常依赖于已有的经验, 自动化、智能化不足;IDS和IPS则难以适用于所有的网络环境,其鲁棒性不断受到变化多端的逃避技术的挑战,且在面对数据加密的情况时也难以保证可靠性。

### 欺骗技术







操作系统混淆：

混淆工具：OSfuscate是一种能够在Windows操作系统上运行的操作系统混淆工具, 该工具对操作系统的注册表值进行修改, 使得指纹识别工具不能正确地收集到操作系统指纹信息。虚假蜜罐欺骗：通过修改计算机系统中一些比较常见的指标, 令攻击方认为计算机系统是一个蜜罐, 从而使其放弃对计算 机系统的攻击。Rowe等人在实验中采取了将计算机系统的VMWare暴露出来以及在文件系统中加入Honeynet项目中的蜜罐工具目录等方式实现了虚假蜜罐欺骗。

虚拟指纹构建：

Honeyd 蜜罐:可以欺骗Nmap 等探测工具, 使用此蜜罐能够对网络主机不同操作系统的网络协议栈进行仿真,构建出虚拟主机的操作系统指纹、TCP开放端口、UDP开放端口, 同时, Honeyd还能够虚拟出路由器,构建出一个虚拟网络拓扑结构。

流量混淆：

Obfsproxy：可以将流量伪装成 HTTP 流量或者即时通讯软件流量

机器/深度学习：对抗样本生成，过在正常的网络流量中增加扰动,形成欺骗流量的对抗样本, 导致以深度学习模型为基础的流量分类方法出现错误。