# 探测行为识别与防御方案设计

## 背景及意义

## 相关技术和工具

1. 数据采集

tcpdump

1. IDS/IPS

Suricata

Zeek

1. 深度学习
2. 移动目标防御技术
3. 混淆工具

Obfsproxy：流量混淆

Portforge：端口混淆

Phantun：udp混淆

OSfuscate：操作系统混淆

## 方案总体框架

1. Moloch实现流量的收集存储
2. Suricata/Zeek+深度学习 实现探测行为识别和边界防护
3. 基于移动目标防御技术实现资产的混淆

## 方案详细设计

### 3.1、数据采集

Moloch

### 3.2、探测行为识别

#### 字段匹配

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”。

#### 行为建模

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。

#### 神经网络

### 3.2、探测行为防护

#### 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。

#### 基于边界的防护技术

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。

##### 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。

##### 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。

##### 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。

#### 基于移动目标防御的防护技术

##### 基于通信网络变换的防护

1. 基于

### 3.3、测绘行为欺骗







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。

## 风险

## 总结