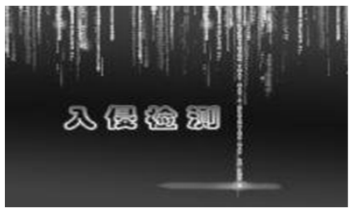
第 十四 章　入侵检测与网络欺骗



内容提纲

1. **Why: 为什么需要入侵检测？**
2. **What: 什么是入侵检测？**
3. **How: 如何进行入侵检测？**
4. **State: 研究现状？**
5. **网络欺骗**

（一）Why?

- 防火墙：根据规则对进出网络的信息进行过滤
  - 本身问题：可能存在安全漏洞成为被攻击的对象
  - 配置不当：起不到作用
  - 网络边界：有缺口（如 Modem，无线）
  - 不是万能：入侵教程、工具随处可见，攻击模式的多样性，并不能阻止所有攻击
- 内部攻击(Abuse)：
  - 并不是所有攻击均来自外部
- 误用(Misuse)

（一）Why?

- 突破边界不可避免，且难以发现
  - FireEye 的M-Trends 2020 Reports中，发现攻击者隐藏或者驻留时间的中位数为56天。近几年的威胁检测时间都在不断缩短，主要是由于对于内部威胁发现较早，极大减少了中位数，但外部威胁的驻留时间还有141天，近5个月之久

GLOBAL MEDIAN DWELL TIME BY YEAR

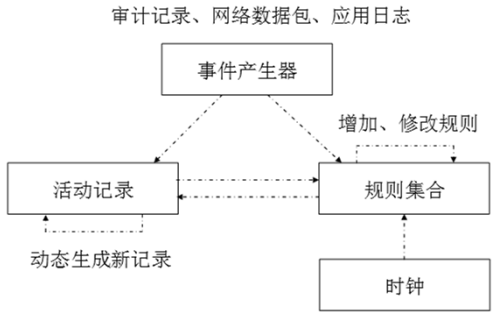
Compromise Notifications	2011	2012	2013	2014	2015	2016	2017	2018	2019
All	416	243	229	205	146	99	101	78	56
Internal Detection	–	–	–	–	56	80	57.5	50.5	30
External Notification	–	–	–	–	320	107	186	184	141

- 1980年4月，James P. Anderson:《Computer Security Threat Monitoring and Surveillance》: 入侵检测开山之作
  - 第一次详细阐述了入侵检测的概念
  - 对计算机系统威胁进行分类：外部渗透、内部渗透和不法行为
  - 提出了利用审计跟踪数据监视入侵活动的思想
- 从1984年到1986年：乔治敦大学的Dorothy Denning和SRI/CSL的Peter Neumann：研究出了一个实时入侵检测系统模型—IDES（入侵检测专家系统）
- 1990，加州大学戴维斯分校的L. T. Heberlein等人开发出了NSM（Network Security Monitor）：第一次直接将网络流作为审计数据来源：新的一页(HIDS, NIDS)

内容提纲

1. **Why: 为什么需要入侵检测？**
2. **What: 什么是入侵检测？**
3. **How: 如何进行入侵检测？**
4. **State: 研究现状？**
5. **网络欺骗**

- 1987, Denning：
  - Intrusion Detection (ID) is to detect a wide range of security violations from attempted break-ins by outsiders to systen



- 2000, Allen
  - Intrusion Detection (ID) is to monitor and collect system and network information and analyzes it to determine if an attack or an intrusion has occurred.
- 入侵检测：通过从计算机系统或网络的关键点收集信息并进行分析，从中发现系统或网络中是否有违反安全策略的行为和被攻击的迹象

- 被入侵的对象：
  - 网络
  - 计算机
  - 应用（控制了计算机不一定能控制应用）
- 几个英文词汇：
  - Attack vs. Intrusion
  - Attack vs. Intrude
  - Attacker vs. Intruder (successful attacker)
  - Victim (the target of an attack) vs. Compromised Host
  - Vulnerability

- IDS：Intrusion Detection System
  - A combination of hardware and software that monitors and collects system and network information and analyzes it to determine if an attack or an intrusion has occurred. Some ID systems can automatically respond to an intrusion.
- 入侵检测系统：是指实施入侵检测的软件与硬件的组合。

- IPS: Intrusion Protection System
  - 入侵检测 + 主动防御
- 主动防御：
  - 预先对入侵活动和攻击性网络流量进行拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报
  - 发现攻击作出响应
- 存在问题：
  - 由于增加了主动阻断能力，检测准确程度的高低对于IPS来说十分关键存在问题：多种技术融合
  - 误报导致合法数据被阻塞

分类

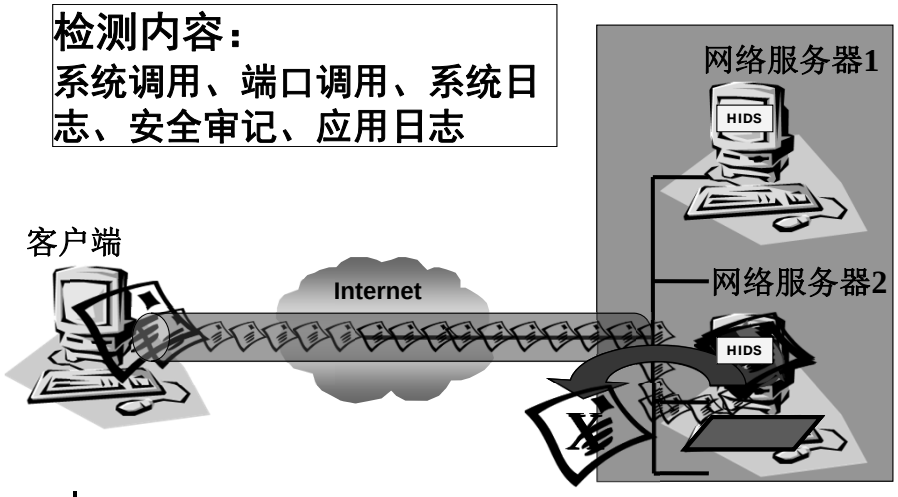
- 根据检测方法来分：
  - 基于特征的入侵检测
  - 基于异常的入侵检测
  - 混合的入侵检测
- 根据数据源来分：
  - 基于应用的入侵检测系统(Application-based IDS)
  - 基于主机的入侵检测系统(Host-based IDS)
  - 基于网络的入侵检测系统(Network-based IDS)
  - 混合的入侵检测系统(Hybrid IDS)

分类（续）

- 按系统各模块的运行方式来分：
  - 集中式：系统各个模块包括数据的收集分析集中在一台主机上运行
  - 分布式：系统的各个模块分布在不同的计算机和设备上
- 根据时效性来分：
  - 脱机分析：行为发生后，对产生的数据进行分析
  - 联机分析：在数据产生的同时或者发生变化时进行分析

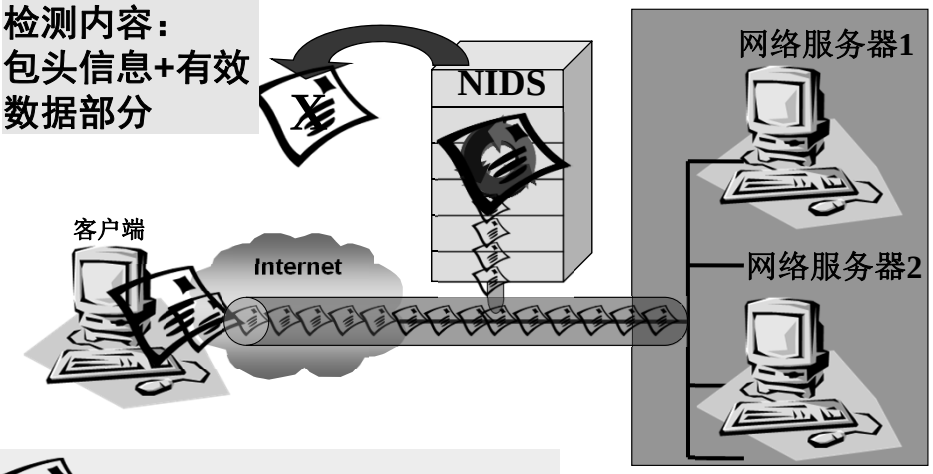
基于主机的IDS

检测内容：
系统调用、端口调用、系统日志、安全审记、应用日志



基于网络入侵检测系统工作原理

检测内容：
包头信息+有效数据部分



数据包=包头信息+有效数据部分

内容提纲

1. Why: 为什么需要入侵检测？
2. What: 什么是入侵检测？
3. How: 如何进行入侵检测？
4. State: 研究现状？
5. 网络欺骗

（一）检测方法

- 两种主要的检测方法：
  - 特征检测（signature detection or misuse detection or signature-based detection or misuse-based detection）
  - 异常检测（anomaly detection or anomaly-based detection）

方法一：特征检测方法

- 特征检测
  - 定义：收集非正常操作的行为特征（signature），建立相关的特征库，当监测的用户或系统行为与库中的记录相匹配时，系统就认为这种行为是入侵。特征：
    - 静态特征：如 signature analysis which is the interpretation of a series of packets (or a piece of data contained in those packets) that are determined, in advance, to represent a known pattern of attack
    - 动态特征：如网络统计数据、计算机或应用系统中的审计记录、日志、文件的异常变化、硬盘、内存大小的变化
    - 特征描述：描述语言
  - 针对的是已知攻击！
  - 检测率取决于：攻击特征库的正确性与完备性

特征检测法实现方式

- 1. 模式匹配法
  - 将收集到的入侵特征转换成模式，存放在模式数据库中。检测过程中将收集到的数据信息与模式数据库进行匹配，从而发现攻击行为。
  - 模式匹配的具体实现手段多种多样，可以是通过字符串匹配寻找特定的指令数据，也可以是采用正规的数学表达式描述数据负载内容。技术成熟，检测的准确率和效率都很高

特征检测法实现方式

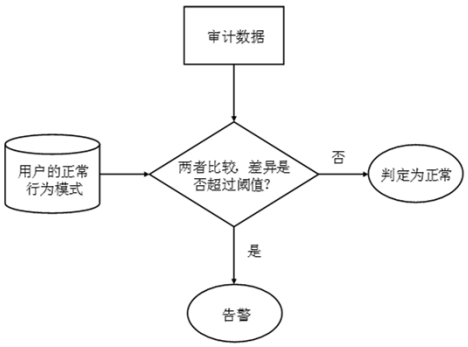
- 2. 专家系统法
  - 入侵活动被编码成专家系统的规则：“If 条件 Then 动作”的形式。入侵检测系统根据收集到的数据，通过条件匹配判断是否出现了入侵并采取相应动作
  - 实现上较为简单，其缺点主要是处理速度比较慢，原因在于专家系统采用的是说明性的表达方式，要求用解释系统来实现，而解释器比编译器的处理速度慢。另外，维护规则库也需要大量的人力精力，由于规则之间具有联系性，更改任何一个规则都要考虑对其他规则的影响。

特征检测法实现方式

- 3. 状态迁移法
  - 利用状态转换图描述并检测已知的入侵模式。入侵检测系统保存入侵相关的状态转换图表，并对系统的状态信息进行监控，当用户动作驱动系统状态向入侵状态迁移时触发入侵警告。
  - 状态迁移法能够检测出多方协同的慢速攻击，但是如果攻击场景复杂的话，要精确描述系统状态非常困难。因此，状态迁移法通常与其他的入侵检测法结合使用。

方法二：异常检测方法

- 异常检测（误用检测）
  - 首先总结正常操作应该具有的特征（用户轮廓），当用户活动与正常行为有重大偏离时即被认为是入侵。



如何定义正常行为?

- 行为：需要一组能够标识用户特征、网络特征或者系统特征的测量参数，如CPU利用率、内存利用率、网络流量等等。基于这组测量参数建立被监控对象的行为模式并检测对象的行为变化。
- 两个关键问题：
  - 选择的各项测量参数能否反映被监控对象的行为模式。
  - 如何界定正常和异常。

数据源评价

- 正常行为的学习依赖于学习数据的质量，但如何评估数据的质量呢？
- 可以利用信息论的熵、条件熵、相对熵和信息增益等概念来定量地描述一个数据集的特征，分析数据源的质量。

数据源评价

- 定义 14-1. 给定数据集合X, 对任意$x \in C_x$, 定义熵$H(X)$为：

$$H(X) = \sum_{x \in Cx} P(x) \log \frac{1}{P(x)}$$

- 在数据集中，每个唯一的记录代表一个类，熵越小，数据也就越规则，根据这样的数据集合建立的模型的准确性越好。

数据源评价

- 定义14-2. 定义条件熵$H(X \mid Y)$为：

$$H(X \mid Y) = \sum_{x,y \in C_x, C_y} P(x,y) \log \frac{1}{P(x \mid y)}$$

- 其中，$P(x, y)$为x 和y 的联合概率，$P(x \mid y)$为给定y 时x 的条件概率。安全审计数据通常都具有时间上的序列特征，条件熵可以用来衡量这种特征，按照上面的定义，令$X=(e_1, e_2, \ldots, e_n)$，令$Y=(e_1, e_2, \ldots, e_k)$，其中$k<n$，条件熵$H(X \mid Y)$可以衡量在给定$Y$ 以后，剩下的X 的不确定性还有多少。条件熵越小，表示不确定性越小，从而通过已知预测未知的可靠性越大。

数据源评价

- 案例：系统调用系列与LSM监控点系列

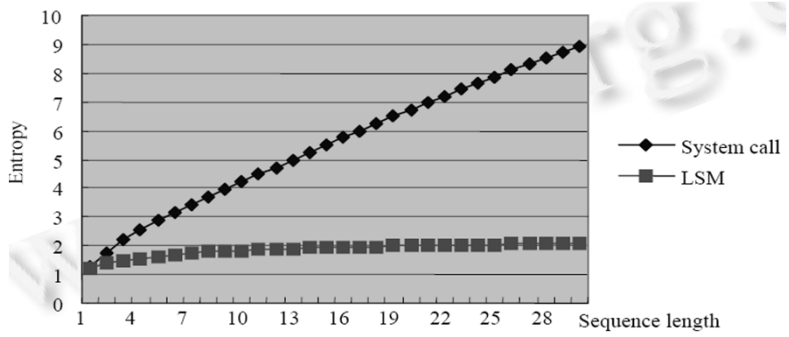


Fig.1 Entropy of system call and LSM

图 1 熵对比图

数据源评价

- 案例：系统调用系列与LSM监控点系列

根据实验数据,假设滑动窗口的大小为 n,窗口中从 1~n 有 n 个系统调用,用 X 表示,其中以从 1~n−1 个系统调用作为属性,用 Y 表示,第 n 个系统调用作为分类.计算条件熵 $H(X|Y)$.同样,对 LSM 数据计算其条件熵.计算的结果如图 2 所示.

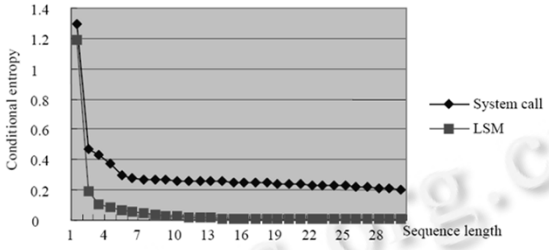


Fig.2 Conditional entropy of system call and LSM

图 2 条件熵对比图

从图 1、图 2 可以看出,LSM 数据的熵与条件熵明显小于系统调用的熵与条件熵, LSM 数据是有一定优势的.同时,从图 2 也可以看出,对系统调用,当滑动窗口大于 6 后,条件熵变化不大,因此 K 取 6 是合适的;而对于 LSM 数据源,K 取 10 较为合适,因此,LSM 数据不足之处是实际使用时,所需的窗口较大,计算复杂度有所增加.

异常检测实现方法

- 1. 统计分析法
  - 以统计理论为基础建立用户或者系统的正常行为模式。主体的行为模式常常由测量参数的频度、概率分布、均值、方差等统计量来描述。抽样周期可以短到几秒钟长至几个月。
  - 异常：将用户的短期特征轮廓与长期特征轮廓进行比较，如果偏差超过设定的阈值，则认为用户的近期活动存在异常。
  - 入侵判定思路较为简单，但是在具体实现时误报率和漏报率都较高，此外，对于存在时间顺序的复杂攻击活动，统计分析法难以准确描述

异常检测实现方法

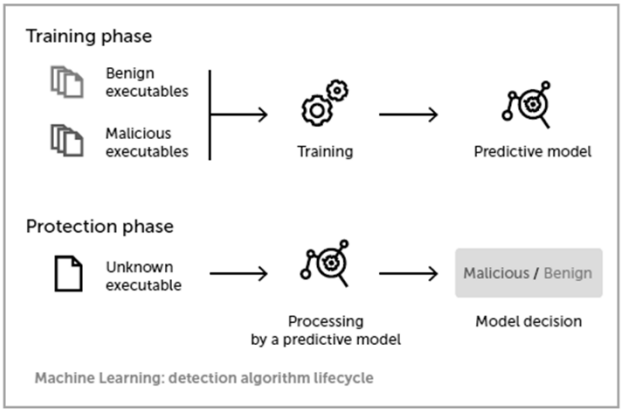
- 2. 神经网络法
  - 向神经网络提交标识用户正常行为的训练数据，神经网络可以通过自学习建立用户或者系统活动的正常特征模式。
  - 异常：采用神经网络对用户或者系统活动进行监控，神经网络将把接收到的事件数据与事先建立的正常特征模式进行比较，判断活动是否出现了异常。
  - 突出优点是不需要指定测量参数来构造标识用户或系统行为的特征集，解决了统计分析法在特征选择方面的困难。存在一个严重的缺陷：发现异常时，神经网络不会提供关于异常的任何分析和解释。

异常检测实现方法

- 3. 聚类分析法
  - 聚类分析以对象之间的相似度为依据，将物理或抽象对象组成的集合进行划分，把相类似的对象集中在一起，归属到一个类中。采用聚类分析法进行异常检测，是希望在描述用户行为或者系统行为的数据中发现不同类别（正常、攻击）的数据集合。 K-means是经典的聚类算法。
  - 异常：需要采用用户行为或者系统行为的一些属性描述被监控主体的行为特征。这些属性必须具有很好的区分度，能够区分出正常活动和异常活动，从而确保数据在经过聚类算法处理以后，标识用户正常活动的数据聚集在一起，而标识攻击等异常活动的数据聚集在一起。

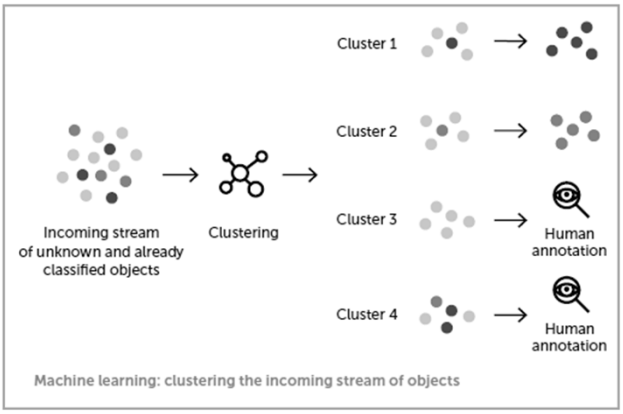
Kaspersky

- Machine learning



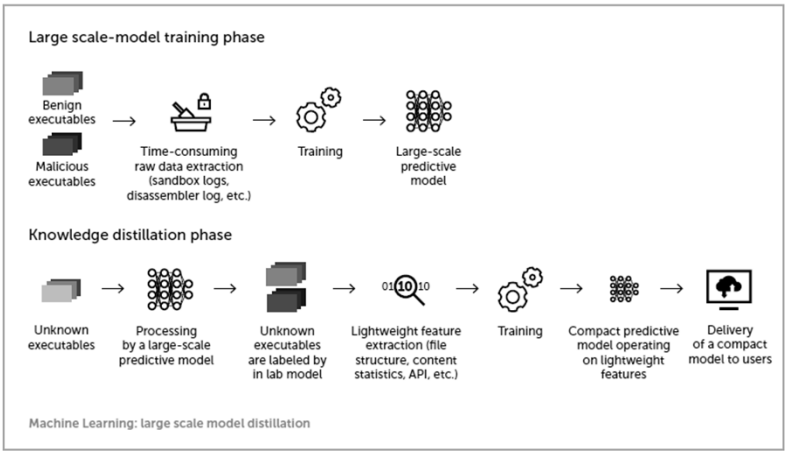
Kaspersky

- Machine learning



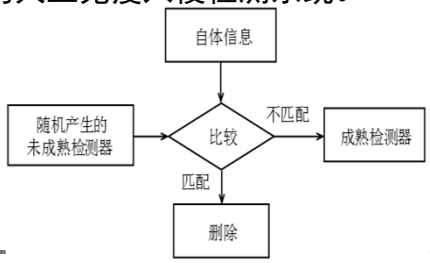
Kaspersky

- Machine learning



异常检测实现方法

- 4. 人工免疫
  - 将非法程序及非法应用与合法程序、合法数据区分开来，与人工免疫系统对自体和非自体进行类别划分相类似。 Forrest采用监控系统进程的方法实现了Unix平台的人工免疫入侵检测系统。



方法二：异常检测方法

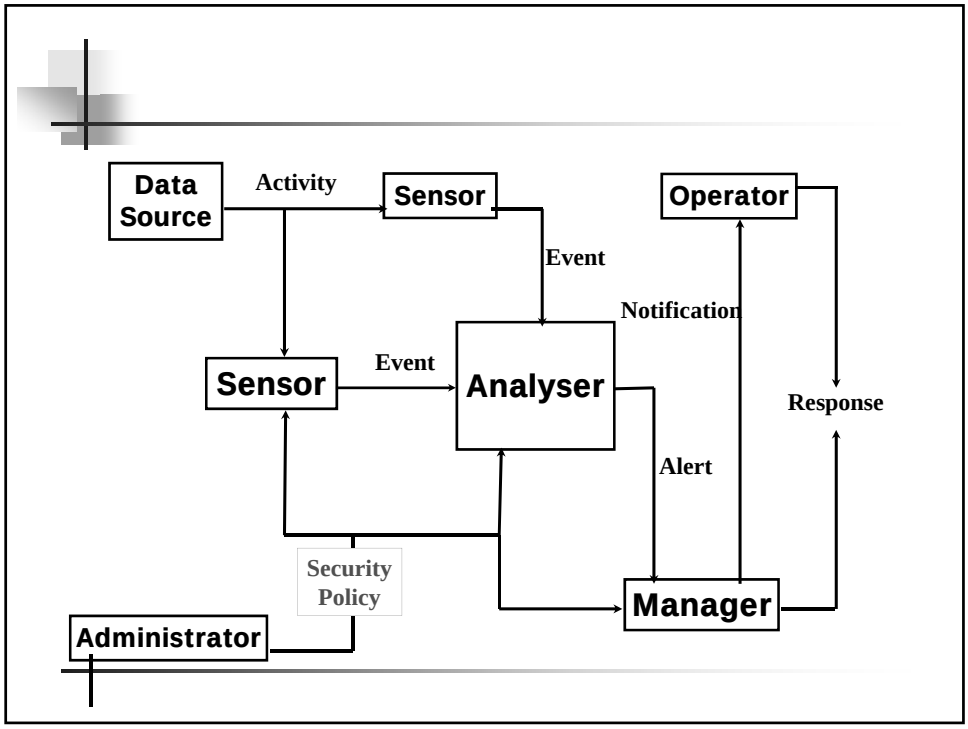
- 异常检测（误用检测）
  - 可以检测未知攻击！？
  - 不在预定义的合法行为集中，就一定是攻击吗？
  - 检测率取决于：正常行为模式的正确性与完备性以及监控的频率
  - 系统能针对用户行为的改变进行自我调整和优化，但随着检测模型的逐步精确，检测过程会消耗更多的系统资源

两种方法比较

- 检测的攻击类型：已知与未知
- 特　征：已知攻击特征与已知正常行为特征
- 性　能：误报率(rate of false positive)与漏报率(rate of false negative)
  - 对每种方法，各在何种情况下发生误报、漏报？

（二）数据源

- 什么样的数据可作为判断入侵的依据？
- 应用数据
  - 应用程序的运行数据（日志、配置文件、状态）
- 主机数据
  - 系统日志文件
  - 目录和文件的异常变化
  - 程序执行中的异常行为
- 网络数据
  - 网络统计数据
  - 网络协议分组的控制字段内容：IP地址、端口号
  - 网络协议分组的数据字段中的特殊内容
- 用户行为？



（四）评价指标

	intrusion	no intrusion
alarm raised	True Positive (TP) intrusion detected	False Positive (FP) false alarm
no alarm raised	False Negative (FN) intrusion missed	True Negative (TN) normal operation

False positive rate	$FPR = \frac{FP}{(FP+TN)}$
True negative rate	$TNR = 1 - FPR$
False negative rate	$FNR = 1 - TPR$
True positive rate	$TPR = \frac{TP}{(TP+FN)}$
Alarm precision	$AP = \frac{TP}{(TP+FP)}$

Figure 11.1: IDS event outcomes (left) and metrics (right). FP and FN (yellow) are the classification errors. TPR is also called the *detection rate*.

内容提纲

1. Why: 为什么需要入侵检测？
2. What: 什么是入侵检测？
3. How: 如何进行入侵检测？
4. State: 研究现状 ？
5. 网络欺骗

研究领域

- 高速网络中的数据获取及处理问题
  - 光分流器，并行、分布式处理：有什么问题？
- 寻找更好的数据来描述用户、程序行为的模式
  - 如何评价数据源？（信息率中的熵）
- 降低误报率和漏报率：最难！
  - 事件关联
- 综合集成：与其它安全产品联动，UIM，安全态势感知
- APT攻击检测

APT检测

- 检测难点：
  - ① 攻击行为特征提取难（滞后性）：0 day漏洞，未知特征木马
  - ② 攻击单点隐蔽性强：动态行为和静态文件的隐蔽性
  - ③ 攻击渠道多样化：多种攻击方法
  - ④ 攻击空间不确定：任何一个网络暴露点都有可能是攻击目标，攻防双方信息不对称

APT检测

- 检测难点：
  - ⑤ 攻击持续和隐蔽时间长：传统的检测方式是基于单个时间点的实时检测，难以对跨度如此长的攻击进行有效跟踪。慢速、分阶段实施的APT 攻击淹没在大数据中。大数据的价值低密度性，使得安全分析工具很难聚焦在价值点上。

基于大数据分析的APT检测

- 由于网络中的安全数据具有体量巨大、来源多样、增涨速度快和价值密度低等大数据特征，兴起了基于网络大数据的安全检测：实现海量网络安全数据的深度关联分析，并对宽时间窗口内的多类型安全事件进行智能关联，在检测APT方面有优势

研究领域

- 机器学习用于异常检测
  - 解决未知威胁的检测问题
  - Darktrace公司的免疫防御

Darktrace

The Enterprise Immune System

Detects and fights cyber-threats in real time

Real-time threat detection and autonomous response

Cyber AI across the cloud, enterprise, and industrial

No rules, signatures, or prior assumptions

Darktarce

Core principles of Darktrace's machine learning

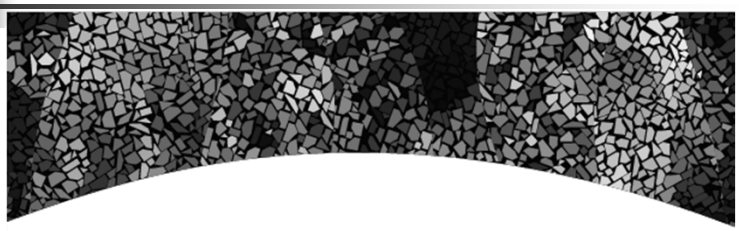
- It learns what is normal within a network 'on the job' – it does not depend upon knowledge of previous attacks.
- It thrives on the scale, complexity and diversity of modern businesses, where every device and person is unique.
- It turns the innovation of attackers against them – any unusual activity is visible.
- It constantly revises assumptions about behavior, using probabilistic mathematics.
- It is always up to date and not reliant on human input.

Darktrace

The impact of Darktrace's unsupervised machine learning on cyber security is transformative. Its cyber AI technology has quickly proved itself capable of seeing hitherto undiscovered cyber events, from a variety of threat sources, which would otherwise have gone unnoticed. These include:

- Insider threat – malicious or accidental.
- Zero-day attacks – previously unseen, novel exploits.
- Latent vulnerabilities – dormant vulnerabilities that are undiscovered, often due to the lack of network visibility.
- Machine-speed attacks – ransomware and other automated attackers that propagate and/or mutate very quickly and are virtually impossible to stop and neutralize using human-dependent response mechanisms.
- Silent and stealthy attacks that lurk in networks undetected.

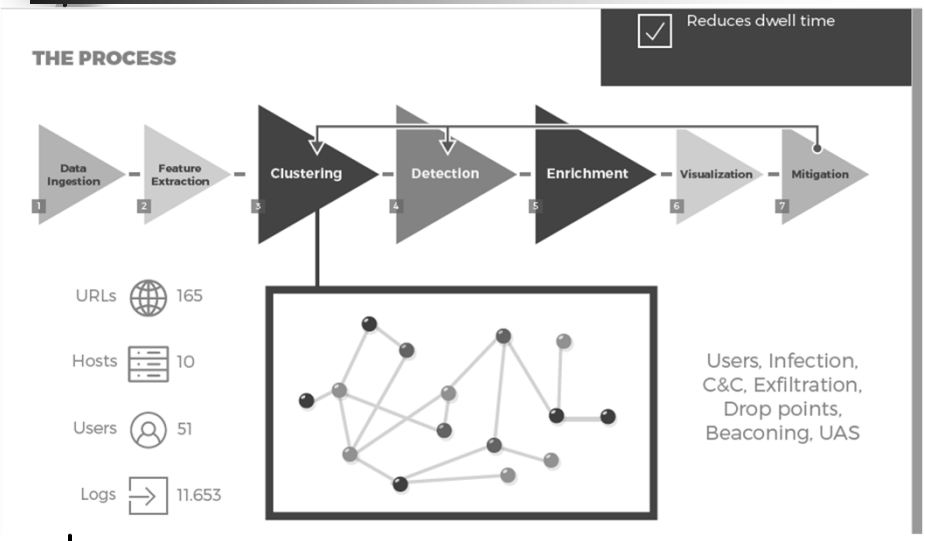
SecBI



SECBI
AUTONOMOUS INVESTIGATION™

STOP CHASING ANOMALIES AND ALERTS:
DETECT THE FULL SCOPE OF AN ATTACK

SecBI



研究领域

- 网络欺骗

内容提纲

1. Why: 为什么需要入侵检测？
2. What: 什么是入侵检测？
3. How: 如何进行入侵检测？
4. State: 研究现状？
5. 网络欺骗

网络欺骗

- 网络欺骗（Cyber Deception）
  - 最早由美国普渡大学的 Gene Spafford 于1989年提出，它的核心思想是：采用引诱或欺骗战略，诱使入侵者相信网络与信息系统中存在有价值的、可利用的安全弱点，并具有一些可攻击窃取的资源（当然这些资源是伪造的或不重要的），进而将入侵者引向这些错误的资源，同时安全可靠地记录入侵者的所有行为，以便全面地了解攻击者的攻击过程和使用的攻击技术。

网络欺骗

- 网络欺骗用途
  - 吸引攻击流量，影响入侵者使之按照防护方的意志进行行动
  - 检测入侵者的攻击并获知其攻击技术和意图，对入侵行为进行告警和取证，收集攻击样本
  - 增加入侵拖延攻击者攻击真实目标者的工作量、入侵复杂度以及不确定性，
  - 为网络防护提供足够的信息来了解入侵者，这些信息可以用来强化现有的安全措施

蜜罐

- 蜜罐（Honeypot）是最早采用欺骗技术的网络安全系统。
  - 定义：蜜罐是一种安全资源，其价值在于被探测、攻击或突破
  - 目标：就是使它被扫描探测、攻击或被突破，同时能够很好地进行安全控制

蜜罐分类

- 根据部署方式可以分为生产型蜜罐和研究型蜜罐

蜜罐分类

- 根据交互程度或逼真程度的高低可以分为低交互蜜罐、中交互蜜罐和高交互蜜罐

蜜罐分类

- 按照实现方式可将蜜罐分为物理蜜罐和虚拟蜜罐

蜜罐功能与关键技术

- 低交互蜜罐的功能相对简单，一般包括：
  - ①攻击数据捕获与处理，在一个或多个协议服务端口上监听，当有攻击数据到来时捕获并处理这些攻击数据，必要的时候还需给出响应，将处理后的攻击数据记录到本地日志，同时向平台服务端（如果有的话）实时推送；
  - ②攻击行为分析，对攻击日志进行多个维度（协议维，时间维，地址维等）的统计分析，发现攻击行为规律，并用可视化方法展示分析结果

蜜罐功能与关键技术

- 高交互蜜罐的功能相对复杂，一般包括：
  - 网络欺骗：对蜜罐进行伪装，使它在被攻击者扫描时表现为网络上的真实主机
    - 空间欺骗技术
    - 网络流量仿真
    - 网络动态配置
    - 多重地址转换
    - 创建组织信息欺骗

蜜罐功能与关键技术

- 高交互蜜罐的功能相对复杂，一般包括：
  - 攻击捕获：采集攻击者对网络实施攻击的相关信息，通过分析捕获的信息，可以研究攻击者所利用的系统漏洞，获取新的攻击方式，甚至是零日攻击。难点是要在防止被攻击者识破的情况下尽可能多地记录下系统状态信息，还有通信加密问题

蜜罐功能与关键技术

- 高交互蜜罐的功能相对复杂，一般包括：
  - 数据控制：限制蜜罐向外发起的连接，确保蜜罐不会成为攻击者的跳板
  - 数据分析：对蜜罐采集到的信息进行多个维度（协议维，时间维，地址维，代码维等）的统计分析，发现攻击行为规律，并用可视化方法展示分析结果

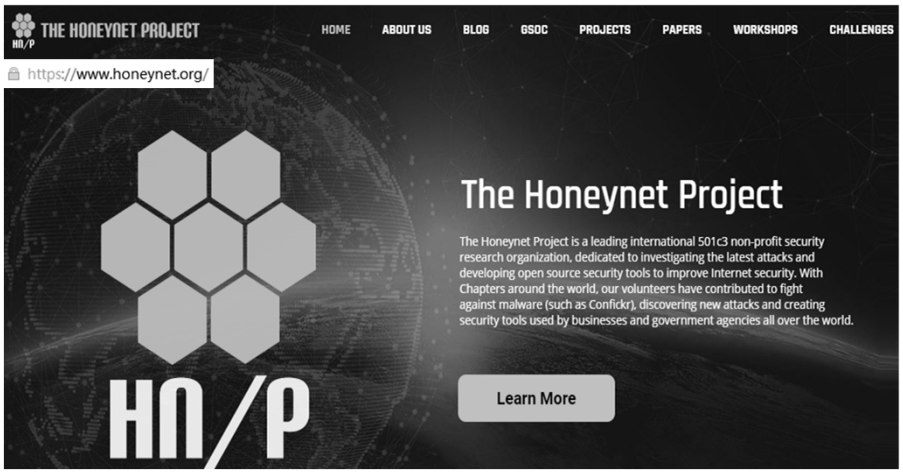
蜜罐相关项目

- 经过多年的发展，有很多商用或开源的蜜罐项目，如honeyd, The Honeynet Project, 狩猎女神，Specter, Mantrap等。开源软件平台gitbub上可以找到大量各种类型的蜜罐(https://github.com/paralax/awesome-honeypots/blob /master/README_CN.md给出了一个比较完整的蜜罐资源列表及网络链接)，如数据库类蜜罐（如HoneyMysql，MongoDB等）、Web类蜜罐（如Shadow Daemon，StrutsHoneypot, WebTrap等）、服务类蜜罐（如Honeyprint, SMB Honeypot, honeyntp, honeyprint等）、工业控制类蜜罐（如Conpot, Gaspot, SCADA Honeynet, gridpot）

蜜网

- 蜜网（Honeynet）是由多个蜜罐组成的欺骗网络，蜜网中通常包含不同类型的蜜罐，可以在多个层面捕获攻击信息，以满足不同的安全需求
  - 蜜网既可以用多个物理蜜罐来构建，也可以由多个虚拟蜜罐组成。目前，通过虚拟化技术（如VMware）可以方便地把多个虚拟蜜罐部署在单个服务器主机上

蜜网



网络欺骗防御

- 有关“网络欺骗防御”这一名词的内涵和外延目前还没有一个统一的、权威的定义
- 本书的观点：网络欺骗防御是一种体系化的防御方法，它将蜜罐、蜜网、混淆等欺骗技术同防火墙、入侵检测系统等传统防护机制有机结合起来，构建以欺骗为核心的网络安全防御体系

网络欺骗防御

- Garter对网络欺骗防御（Cyber Deception Defense）的定义为：使用骗局或者假动作来阻挠或者推翻攻击者的认知过程，扰乱攻击者的自动化工具，延迟或阻断攻击者的活动，通过使用虚假的响应、有意的混淆、假动作、误导等伪造信息达到“欺骗”的目的

网络欺骗防御技术

- 根据网络空间欺骗防御的作用位置不同，可以将其分为不同的层次，包括：
  - 网络层欺骗
  - 终端层欺骗
  - 应用层欺骗
  - 数据层欺骗

网络欺骗防御系统

- 国内外已有一些网络欺骗防御产品：
  - TrapX Security的DeceptionGrid
  - DARPA的Prattle
  - 美国Sandia国家实验室的Hades
  - 长亭科技2016年推出基于欺骗伪装技术的内网威胁感知系统谛听（D-Sensor）
  - 幻阵是我国默安科技研发的一款基于攻击混淆与欺骗防御技术的威胁检测防御系统

DeepDig

- 把黑客变成免费渗透测试服务人员
  - 德克萨斯大学达拉斯分校的研究人员应用机器学习开发更有效的蜜罐式网络防御——智能DeepDig

换而言之就是将网络攻击作为基于机器学习的入侵检测系统的实时培训数据的免费来源。说直白点就是把攻击者当成免费的渗透测试人员。

UT达拉斯大学的计算机科学教授Kevin Hamlen博士解释说：

> 像Illusive Networks、Attivo这样的公司创建了旨在便对手感到困惑的网络拓扑，这使他们更难找到真正的资产来进行攻击。尽管防御仍然相对静止，但随着时间的流逝，攻击者学会了如何将蜜罐与真实资产区分开，从而导致了不对称博弈，最终获胜的往往是攻击者。但现有方法的缺点是这种欺骗手段不能从攻击中汲取教训。相比之下，DeepDig将真实资产变成陷阱，可以利用人工智能和数据挖掘从攻击中吸取教训（高价值数据）。

用蜜罐检测 **Kerberoasting** 攻击

BLOG: HOW TOS

Honeyroasting. How to detect Kerberoast breaches with honeypots

用蜜罐检测 **Kerberoasting** 攻击

BLOG: HOW TOS

Honeyroasting. How to detect Kerberoast breaches with honeypots

As we know one of the main issues facing defenders, especially in large environments, is protecting against threat actors after they gain a foothold in the environment. If an attacker lands on a domain-joined PC, the attack surface is massive, and it is vital to detect them as quickly as possible. Antivirus and more common EDR solutions have come on a long way in detecting and preventing attackers, but a sophisticated threat actor will likely be able to circumvent these controls by using custom implants and advanced techniques.

One method, which is often overlooked by defenders, is the use of honeypot accounts. A honeypot account is an account strategically positioned in a network to look interesting for an attacker. If any contact is made with the honeypot account than an alert is sent to the defenders to investigate.

The primary aim of using the honeypot account in this context is to detect Kerberoasting (covered in @myexploit2600's post How to: Kerberoast like a boss) which based on our experience in the industry is one of the most common attack vectors used after a foothold is obtained within a network.

One of the advantages of using a honeypot account is that there are no additional software costs. A lot of blue team solutions cost big money and require a significant amount of resource to implement and administer.

蜜罐资源链接

- https://github.com/paralax/awesome-honeypots

Awesome Honeypots awesome

A curated list of awesome honeypots, plus related components and much more, divided into categories such as Web, services, and others, with a focus on free and open source projects.

There is no pre-established order of items in each category, the order is for contribution. If you want to contribute, please read the guide.

Discover more awesome lists at sindresorhus/awesome.

Contents

- Related Lists
- Honeypots
- Honeyd Tools
- Network and Artifact Analysis
- Data Tools
- Guides

谢谢大家，一起交流学习！

QQ：10068 0 2383