CAN304 W11

Intrusion detection

Classes of Intruders：

- Cyber criminals
  - 有组织犯罪集团的个人或成员；目标：经济奖励；活动：身份盗窃、财务凭证盗窃、数据盗窃或数据勒索
- Activists
  - 个人（通常是内部人员），或更大的外部攻击者群体的成员；受社会或政治原因驱动；活动：网站污损、Dos 攻击或导致负面宣传的数据盗窃和分发
- State-sponsored organizations
  - 政府资助的黑客团体
- Others
  - 具有上述动机以外的其他动机的黑客

Security Intrusion：安全事件，或多个安全事件的组合。其中入侵者在未经授权的情况下获得或试图获得对系统（或系统资源）的访问权。

Intrusion Detection：一种安全服务，用于监视和分析系统事件，以便查找和提供实时或近乎实时的警告以未经授权的方式访问系统资源的尝试。

Intrusion Detection System (IDS)

An IDS comprises three logical components：

- Sensors
  - 收集数据（网络数据包、日志文件和系统调用跟踪）
- Analyzers
  - 确定是否发生了入侵
- User interface
  - 查看输出或控制系统行为

IDS Requirements：

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on a system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large number of systems
- Provide graceful degradation of services
- Allow dynamic reconfiguration

Analysis Approaches

- Anomaly detection
  - 对正常行为进行建模
  - 涉及收集与合法用户在一段时间内的行为有关的数据；分析当前观察到的行为以确定该行为是合法用户的行为还是入侵者的行为
- Signature/Heuristic detection
  - 对恶意模式或行为进行建模，also known as misuse detection
  - 使用一组已知的恶意数据模式（签名）或攻击规则（启发式）；将当前行为与签名或规则进行比较，以确定是否属于入侵者
  - 只能识别具有模式或规则的已知攻击

Anomaly Detection

- Two steps:
  - 1. 开发合法用户行为模型，2. 将当前观察到的行为与模型进行比较，以便将其分类为合法或异常活动
- 使用多种分类方法：
  - Statistical：使用观察指标的单变量、多变量或时间序列模型分析观察到的行为
  - Knowledge based：方法使用专家系统，该系统根据一组对合法行为进行建模的规则对观察到的行为进行分类
  - Machine-learning：方法使用数据挖掘技术从训练数据中自动确定合适的分类模型

Signature or Heuristic Detection

通过观察系统中的事件并将一组签名模式应用于数据或一组表征数据的规则来检测入侵，从而决定观察到的数据是表示正常行为还是异常行为。

- Signature approaches
  - 将大量已知恶意数据模式与存储在系统上或通过网络传输的数据进行匹配；广泛用于防病毒产品、网络流量扫描代理和 NIDS (network intrusion detection systems)
- Rule-based heuristic identification
  - 涉及使用规则来识别已知渗透或将利用已知弱点的渗透

Intrusion Detection System (IDS)

根据所分析数据的来源和类型，IDS 分为：

- Host-based IDS (HIDS)
  - 监控单个主机的特征以发现可疑活动
- Network-based IDS (NIDS)
  - 监控网络流量并分析网络、传输和应用程序协议以识别可疑活动
- Distributed or hybrid IDS
  - 将来自多个传感器（通常基于主机和基于网络）的信息组合在一个中央分析器中，该分析器能够更好地识别和响应入侵活动

Host-Based Intrusion Detection (HIDS)

为易受攻击或敏感的系统添加专门的安全软件层。例如，数据库服务器和管理系统。

可以使用 anomaly 或 signature/heuristic approaches。

监控活动以检测可疑行为：主要目的是检测入侵，记录可疑事件并发送警报；可以检测外部和内部入侵。

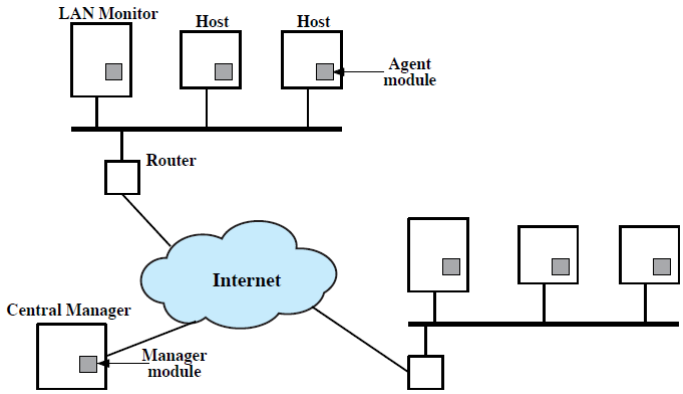
HIDS: Data Sources and Sensors

入侵检测的一个基本组成部分是收集数据的传感器。

常见的数据源包括：System call traces，Audit (log file) records，File integrity checksums，Registry access。

Distributed HIDS

HIDS 还可以使用 Distributed approach。



- Host agent module
  - 收集主机上与安全相关的事件的数据；将这些数据传输给中央管理器
- LAN monitor agent module
  - 一个 Host agent module + 分析 LAN 流量并将结果报告给中央管理器
- Central manager module
  - 接收来自 LAN monitor 和 Host agent 的报告；处理和关联这些报告以检测入侵

Network-Based IDS (NIDS)

监控网络上选定点的流量，实时（或接近实时）逐个数据包检查流量。可以检查网络、传输和/或应用程序级协议活动。

包括多个传感器、一个或多个用于 NIDS 管理的服务器，以及一个或多个用于人机界面的管理控制台。可以在传感器、管理服务器或两者的组合处分析通信量。

Types of Network Sensors

传感器可以以两种模式之一进行部署：inline and passive。

- Inline sensor
  - 插入到网段中，以便它所监视的通信量必须通过该传感器
- Passive sensor

- 监视网络流量的副本；实际流量不会通过设备

Intrusion Detection Techniques for NIDS

- Signature Detection
- Anomaly Detection Techniques：模型使用组织特定的流量配置文件进行训练
- Stateful Protocol analysis (SPA)：模型使用预先确定的通用供应商提供的良性协议流量配置文件进行训练。SPA NIDS 是 Anomaly NIDS 的子集

Logging of Alerts

NIDS 传感器记录的典型 log 信息包括：

• Timestamp
• Connection or session ID
• Event or alert type
• Rating (e.g., priority, severity, impact, confidence)
• Network, transport, and application layer protocols
• Source and destination IP addresses
• Source and destination TCP or UDP ports, or ICMP types and codes
• Number of bytes transmitted over the connection

Honeypots

Decoy systems designed to:

- 转移攻击者访问关键系统的注意力；收集有关攻击者活动的信息；鼓励攻击者在系统上停留足够长的时间，以便管理员做出响应
- 这些系统充满了系统的合法用户无法访问的捏造信息
- 这些是没有生产价值的资源；因此，传入通信最有可能是探测、扫描或攻击；已启动的出站通信表明系统可能已遭到入侵

Honeypot Classifications

- Low interaction honeypot
  - 由一个软件包组成，该软件包可以很好地模拟特定的 IT 服务或系统，以提供逼真的初始交互，但不执行这些服务或系统的完整版本
  - 提供不太真实的目标
  - 通常足以用作分布式 IDS 的组件，以警告即将发生的攻击
- High interaction honeypot
  - 一个真正的系统，具有完整的操作系统，服务和应用程序，它们被检测并部署在攻击者可以访问的地方
  - 是一个更真实的目标，可能会长时间占据攻击者的注意力
  - 但是，它需要更多的资源
  - 如果受到威胁，则可用于对其他系统发起攻击

Firewalls and intrusion prevention

Firewalls

防火墙是一种网络安全系统，它根据预先确定的安全规则监视和控制传入和传出的网络流量。防火墙通常在受信任的网络和不受信任的网络（如 Internet）之间建立屏障。

Firewall Design Goals

从内部到外部的所有流量，反之亦然，都必须通过防火墙。仅允许本地安全策略定义的授权流量通过。防火墙本身不受渗透。

Firewall Filter Characteristics

防火墙访问策略可用于筛选流量的特征包括：

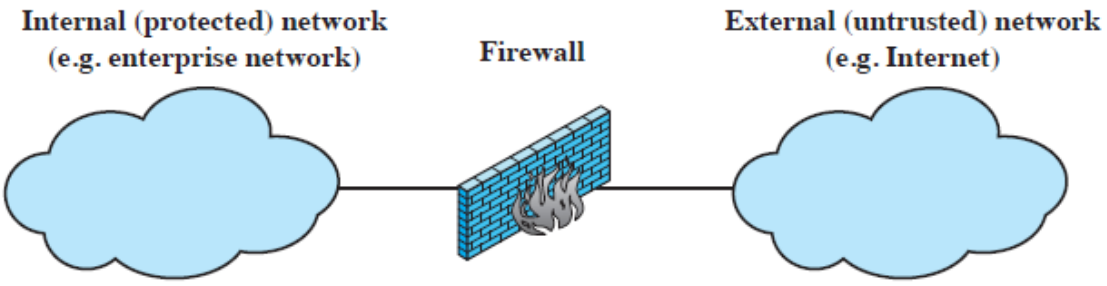
- IP address and protocol values
  - 基于源地址或目标地址和端口号、流向（入站或出站）以及其他网络和传输层特征
  - 由数据包过滤器和状态检查防火墙使用，通常用于限制对特定服务的访问
- Application protocol
  - 根据授权的应用程序协议数据控制访问；由应用程序级网关使用，用于中继和监视特定应用程序协议的信息交换
- User identity
  - 基于内部用户的身份
- Network activity
  - 根据时间或请求、请求速率或其他活动模式等注意事项控制访问

Firewall Capabilities and Limits

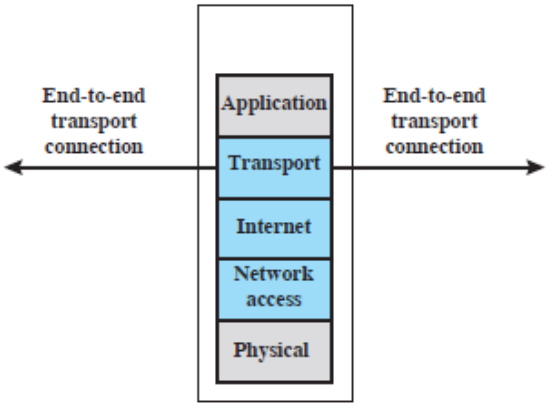
- Capabilities
  - 定义单个 choke point，提供用于监视安全事件（例如，审计、警报）的位置
  - 方便的平台，用于多个与安全无关的互联网功能，例如网络地址转换器
- Limitations
  - 无法抵御绕过防火墙的攻击
  - 可能无法完全抵御内部威胁
  - 笔记本电脑或便携式存储设备可能在企业网络外部被感染，然后在内部使用

Types of Firewalls

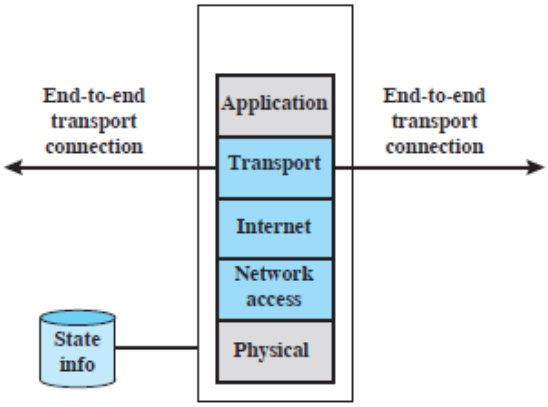
5 种 firewalls：



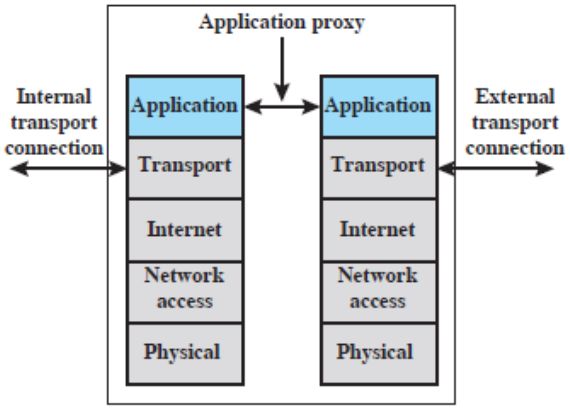
(a) General model



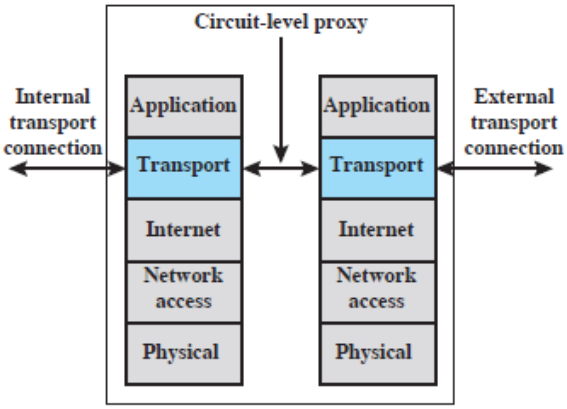
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Packet Filtering Firewall

- 将规则应用于每个传入和传出的 IP 数据包
  - 通常设置为基于 IP 或 TCP 标头中的匹配项的规则列表；根据规则匹配项转发或丢弃 (forwards or discards) 数据包
- Two default policies
  - Discard - 除非明确允许，否则禁止丢弃。更安全但会降低可用性
  - Forward - 除非明确禁止，否则允许。更易于管理和使用，但安全性较低

Stateful Inspection Firewall

通过创建出站 TCP 连接目录来收紧 TCP 流量的规则

- 每个当前建立的连接都有一个条目

- 数据包过滤器只允许那些符合此目录中条目之一的配置文件的数据包进入高编号端口

Application proxy Firewall

Also called Application-Level Gateway，充当应用程序级流量的中继。

使用 TCP/IP 应用程序的用户联系人网关 -> 用户已通过身份验证 -> 网关联系远程主机上的应用程序，并在服务器和用户之间中继 TCP 段

Circuit-Level proxy Firewall

Also called Circuit-Level Gateway。

设置两个 TCP 连接，一个在内部主机中的 Circuit-Level Gateway 与 TCP 用户之间，另一个在外部主机上。在不检查内容的情况下将 TCP 段从一个连接中继到另一个连接。

通常在内部用户受信任时使用：可以使用 application-level gateway 入站和 circuit-level gateway 出站。

Firewall Basing

- Bastion Hosts
  - 用作 application-level 或 circuit-level gateway 的平台
- Host-Based Firewalls
  - 用于保护单个主机的软件模块；此类防火墙的通用位置是服务器
- Personal Firewall
  - 个人计算机上的软件模块，例如，在家庭环境中

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- 是 IDS 的扩展，包括能够尝试阻止检测到的恶意活动；Can be host-based, network-based, or distributed/hybrid
- 可以使用 anomaly detection 来识别不是合法用户的行为，或使用signature/heuristic detection 来识别已知的恶意行为
- 可以像防火墙一样阻止流量，但要利用为 IDS 开发的算法类型来确定何时执行此操作