6 审计设备【日志分析】

审计信息：180 天。

追溯、安全运营分析【大的数据分析平台，IDS】

0x01 实验环境

1)EventLog Analyzer

EventLog Analyzer 是一个基于 Web 的，实时的用于日志收集和合规性管理的信息安全和事件管理(SIEM)解决方案，可以提升你内部网络的安全，满足你最新的 IT 审计需求。通过无代理的架构，EventLog Analyzer 可以对日志进行收集、分析、查找、报表、归档。支持大量的日志类型：系统日志(Windows、Linux、UNIX 等等),网络设备(路由、交换机等等),应用程序(Oracle、Apache 等等)。提供了对网络中用户活动、策略违反、网络异常和内部威胁的深刻洞察。网络管理员和 IT 经理用 Evenglog Analyzer 进行网络系统审计，为各种法案(SOX、HIPAA、PCI DSS、GLBA 等)生成合规性报表。

集中采集主机、服务器、网络设备、安全设备、数据库以及各种应用服务系统产生的日志和事件；从海量日志数据中精确查找关键有用的事件数据，准确定位网络故障并提前识别安全威胁；预置丰富的报表，满足合规性审计需要。

0x02 原理介绍

流量收集与分析，统一的日志格式，安全级别的划分，难点在于：不同厂商日志的统一；安全基线的设置

0x30 实践操作