网络安全审计技术原理与应用

网络安全审计概述
网络安全审计系统组成与类型
网络安全审计机制与实现技术
网络安全审计主要产品与技术指标
网络安全审计应用

文老师软考教育

网络安全审计概述

文老师软考教育

◆网络安全审计概念：网络安全审计是指对网络信息系统的安全相关活动信息进行获取、记录、存储、分析和利用的工作。网络安全审计的作用在于建立“事后”安全保障措施，保存网络安全事件及行为信息，为网络安全事件分析提供线索及证据，以便于发现潜在的网络安全威胁行为，开展网络安全风险分析及管理。

◆目前，IT产品和安全设备都不同程度地提供安全审计功能。常见的安全审计功能是安全事件采集、存储和查询。对于重要的信息系统，则部署独立的网络安全审计系统。

◆网络安全审计相关标准：1985年美国国家标准局公布的《可信计算机系统评估标准》(Trusted Computer System Evaluation Criteria，TCSEC)中给出了计算机系统的安全审计要求。TCSEC从C2级开始提出了安全审计的要求，随着保护级别的增加而逐渐加强，B3级以及之后更高的级别则不再变化。

◆我国的国家标准GB 17859《计算机信息系统安全保护等级划分准则》（以下简称《准则》）从第二级开始要求提供审计安全机制。其中，第二级为系统审计保护级，该级要求计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。《准则》中明确了各级别对审计的要求，如表所示。

网络安全审计概述

级别类型	安全审计要求
用户自主保护级	无
系统审计保护级	计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间（例如：打开文件、程序初始化）；删除客体；由操作员、系统管理员或（和）系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源（例如：终端标识符）；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录区别于计算机信息系统可信计算基独立分辨的审计记录
安全标记保护级	在系统审计保护级的基础上，要求增强的审计功能是：审计记录包含客体名及客体的安全级别。此外，计算机信息系统可信计算基具有审计更改可读输出记号的能力
结构化保护级	在安全标记保护级的基础上，要求增强的审计功能是：计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件
访问验证保护级	在结构化保护级的基础上，要求增强的审计功能是：计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们

文老师软考教育

网络安全审计系统组成与类型

◆网络安全审计系统组成：网络安全审计系统一般包括审计信息获取、审计信息存储、审计信息分析、审计信息展示及利用、系统管理等组成部分。

◆针对不同的审计对象，安全审计系统的组成部分各不相同，审计细粒度也有所区分。例如，操作系统的安全审计可以做到对进程活动、文件操作的审计；网络通信安全审计既可对IP包的源地址、目的地址进行审计，又可以对IP包的内容进行深度分析，实现网络内容审计。

◆网络安全审计系统类型：按照审计对象类型分类，网络安全审计主要有操作系统安全审计、数据库安全审计、网络通信安全审计、应用系统安全审计、网络安全设备审计、工控安全审计、移动安全审计、互联网安全审计、代码安全审计等。操作系统审计一般是对操作系统用户和系统服务进行记录，主要包括用户登录和注销、系统服务启动和关闭、安全事件等。

◆ Windows、Linux等操作系统都自带审计功能，其审计信息简要叙述如下：

网络安全审计系统组成与类型

◆ Windows操作系统的基本审计信息有注册登录事件、目录服务访问、审计账户管理、对象访问、审计策略变更、特权使用、进程跟踪、系统事件等；

◆ Linux操作系统的基本审计信息有系统开机自检日志boot.log、用户命令操作日志acct/pacct、最近登录日志lastlog、使用su命令日志sulog、当前用户登录日志utmp、用户登录和退出日志wtmp、系统接收和发送邮件日志maillog、系统消息messages等。

◆数据库审计通常是监控并记录用户对数据库服务器的读、写、查询、添加、修改以及删除等操作，并可以对数据库操作命令进行回放。

◆网络通信安全审计一般采用专用的审计系统，通过专用设备获取网络流量，然后再进行存储和分析。
◆网络通信安全审计的常见内容为IP源地址、IP目的地址、源端口号、目的端口号、协议类型、传输内容等。

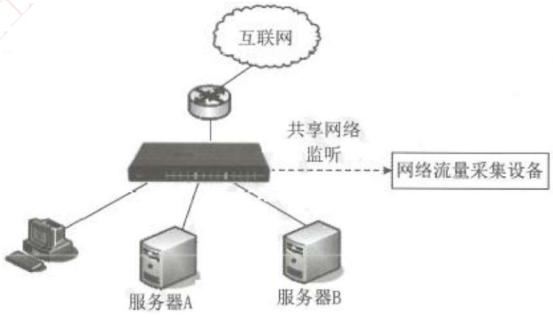
◆按照审计范围，安全审计可分为综合审计系统和单个审计系统。由于各IT产品自带的审计功能有限，审计能力不足，于是安全厂商研发了综合审计系统。单个审计系统主要针对独立的审计对象，审计数据来源单一，缺少多源审计对象的关联分析，常见的是IT系统或产品自带的审计功能。

文老师软考教育

网络安全审计机制与实现技术

◆网络安全审计机制主要有基于主机的审计机制、基于网络通信的审计机制、基于应用的审计机制等，下面主要介绍审计机制实现常用的技术。
◆系统日志数据采集技术：常见的系统日志数据采集技术是把操作系统、数据库、网络设备等系统中产生的事件信息汇聚到统一的服务器存储，以便于查询分析与管理。

◆网络流量数据获取技术：常见的技术方法有共享网络监听、交换机端口镜像(Port Mirroring)、网络分流器(Network Tap)等。其中，共享网络监听利用Hub集线器构建共享式网络，网络流量采集设备接入集线器上，获取与集线器相连接的设备的网络流量数据，如图所示。图中服务器A和服务器B的网络流量数据都可以被网络流量采集设备获取到。
◆对于不支持端口镜像功能的交换机，通常利用网络分流器(TAP)把网络流量导入网络流量采集设备。



网络安全审计机制与实现技术

◆网络流量采集设备安装网络数据捕获软件，从网络上获取原始数据，然后再进行后续处理。目前，常见的开源网络数据采集软件包是Libpcap（Library for Packet Capture）。Libpcap的工作流程如下：
(1)设置嗅探网络接口。在Linux操作系统中，大多数为eth0。
(2)初始化Libpcap。设定过滤规则，明确获取网络数据包的类型。
(3)运行Libpcap循环主体。Libpcap开始接收符合过滤规刚的数据包。

◆除了Libpcap外，还有Winpcap，它支持在Windows平台捕获网络数据包。Windump是基于Winpcap的网络协议分析工具，可以采集网络数据包。Tcpdump是基于Libpcap的网络流量数据采集工具，常常应用于Linux操作系统中。
◆ Wireshark是图形化的网络流量数据采集工具，可用于网络流量数据的采集和分析。

◆网络审计数据安全分析技术：网络审计数据蕴涵着网络安全威胁相关信息，需要通过数据分析技术方法来提取。常见的网络审计数据安全分析技术有字符串匹配、全文搜索、数据关联、统计报表、可视化分析等。

网络安全审计机制与实现技术

文老师软考教育

1．字符串匹配通过模式匹配来查找相关审计数据，以便发现安全问题。常见的字符串匹配工具是grep，其使用的格式：grep [options] [regexp] [filename]
regexp为正则表达式，用来表示要搜索匹配的模式。
2．全文搜索利用搜索引擎技术来分析审计数据。
3．数据关联是指将网络安全威胁情报信息，如系统日志、全网流量、安全设备日志等多个数据来源进行综合分析，以发现网络中的异常流量，识别未知攻击手段。
4. 统计报表是对安全审计数据的特定事件、阈值、安全基线等进行统计分析，以生成告警信息，形成发送日报、周报、月报。
5．可视化分析。将安全审计数据进行图表化处理，形成饼图、柱状图、折线图、地图等各种可视化效果，以支持各种用户场景。将不同维度的可视化效果汇聚成仪表盘，辅助用户实时查看当前事件变更。安全关键KPI状态高亮显示，突出异常行为的重要性。

◆网络审计数据存储技术：网络审计数据存储技术分为两种：一种是由审计数据产生的系统自己分散存储，审计数据保存在不同的系统中；目前，操作系统、数据库、应用系统、网络设备等都可以各自存储日志数据。另一种集中采集各种系统的审计数据，建立审计数据存储服务器，由专用的存储设备保存，便于事后查询分析和电子取证。

网络安全审计机制与实现技术

◆网络审计数据保护技术：网络审计数据涉及系统整体的安全性和用户的隐私性，为保护审计数据的安全，通常的安全技术措施有如下几种。

1．系统用户分权管理。操作系统、数据库等系统设置操作员、安全员和审计员三种类型的用户。操作员只负责对系统的操作维护工作，其操作过程被系统进行了详细记录；安全员负责系统安全策略配置和维护；审计员负责维护审计相关事宜，可以查看操作员、安全员工作过程日志；操作员不能够修改自己的操作记录，审计员也不能对系统进行操作。

2．审计数据强制访问。系统采取强制访问控制措施，对审计数据设置安全标记，防止非授权用户查询及修改审计数据。

3．审计数据加密。使用加密技术对敏感的审计数据进行加密处理，以防止非授权查看审计数据或泄露。

4．审计数据隐私保护。采取隐私保护技术，防止审计数据泄露隐私信息。

5．审计数据完整性保护。使用Hash算法和数字签名，对审计数据进行数字签名和来源认证、完整性保护，防止非授权修改审计数据。

网络安全审计主要产品与技术指标

◆日志安全审计产品：日志安全审计产品是有关日志信息采集、分析与管理的系统。产品的基本原理是利用Syslog、Snmptrap、NetFlow、Telnet、SSH、WMI、FTP、SFTP、SCP、JDBC、文件等技术，对分散设备的异构系统日志进行分布采集、集中存储、统计分析、集中管理，便于有关单位／机构进行安全合规管理，保护日志信息安全。日志安全审计产品的主要功能有日志采集、日志存储、日志分析、日志查询、事件告警、统计报表、系统管理等。

◆主机监控与审计产品：是有关主机行为信息的安全审查及管理的系统。产品的基本原理是通主机监控与审计产品过代理程序对主机的行为信息进行采集，然后基于采集到的信息进行分析，以记录系统行为，帮助管理员评估操作系统的风险状况，并为相应的安全策略调整提供依据。该产品的主要功能有系统用户监控、系统配置管理、补丁管理、准入控制、存储介质（U盘）管理、非法外联管理等。

◆数据库审计产品：是对数据库系统活动进行审计的系统。产品的基本原理是通过网络流量监听、系统调用监控、数据库代理等技术手段对所有访问数据库系统的行为信息进行采集，然后对采集的信息进行分析，形成数据库操作记录，保存和发现数据库各种违规的或敏感的操作信息，为相应的数据库安全策略调整提供依据。在数据库审计产品中，实现数据库审计主要有如下三种方式。

网络安全审计主要产品与技术指标

1．网络监听审计。对获取到的数据库流量进行分析，从而实现对数据库访问的审计和控制。其优点是数据库网络审计不影响数据库服务器，其不足是网络监听审计对加密的数据库网络流量难以审计，同时无法对数据库服务器的本地操作进行审计。

2．自带审计。通过启用数据库系统自带的审计功能，实现数据库的审计。其优点是能够实现数据库网络操作和本地操作的审计，缺点是对数据库系统的性能有一些影响，在审计策略配置、记录的粒度、日志统一分析方面不够完善，日志本地存储容易被删除。

3．数据库Agent。在数据库服务器上安装采集代理(Agent)，通过Agent对数据库的各种访问行为进行分析，从而实现数据库审计。其优点是能够实现数据库网络操作和本地操作的审计，缺点是数据库Agent需要安装数据库服务器，对数据库服务系统的性能、稳定性、可靠性有影响。

◆网络安全审计产品：网络安全审计产品是有关网络通信活动的审计系统。产品的基本原理是通过网络流量信息采集及数据包深度内容分析，提供网络通信及网络应用的活动信息记录。网络安全审计常见的功能主要包括如下几个方面。

网络安全审计主要产品与技术指标

文老师软考教育

1．网络流量采集。获取网上通信流量信息，按照协议类型及采集规则保存流量数据。
2．网络流量数据挖掘分析。对采集到的网络流量数据进行挖掘，提取网络流量信息，形成网络审计记录，主要包括如下内容。
(1)邮件收发协议（SMTP、POP3协议）审计。从邮件网络流量数据提取信息，记录收发邮件的时间、地址、主题、附件名、收发人等信息，并能够回放所收发的邮件内容。
(2)网页浏览(HTTP协议)审计。从Web网络流量数据提取信息，记录用户访问网页的时间、地址、域名等信息，并能够回放所浏览的网页内容。
(3)文件共享（NetBios协议）审计。从文件共享网络流量数据提取信息，记录网络用户对网络资源中的文件共享操作。
(4)文件传输（FTP协议）审计。从FTP网络流量数据提取信息，记录用户对FTP服务器的远程登录时间、读、写、添加、修改以及删除等操作，并可以对操作过程进行完整回放。
(5)远程访问（Telnet协议）审计。从FTP网络流量数据提取信息，记录用户对Telnet服务器的远程登录时间、各种操作命令，并可以对操作过程进行完整回放。
(6) DNS审计。从DNS网络流量数据提取信息，记录用户DNS服务请求信息，并可以对操作过程进行完整回放。

◆网络安全审计产品的性能指标主要有支持网络带宽大小、协议识别种类、原始数据包查询响应时间等。

网络安全审计主要产品与技术指标

◆工业控制系统网络审计产品：工业控制系统网络审计产品是对工业控制网络中的协议、数据和行为等进行记录、分析，并做出一定的响应措施的信息安全专用系统。产品的基本原理是利用网络流量采集及协议识别技术，对工业控制协议进行还原，形成工业控制系统的操作信息记录，然后进行保存和分析。
◆工业控制系统网络审计产品的实现方式通常分两种情况：一种是一体化集中产品，即将数据采集和分析功能集中在一台硬件中，统一完成审计分析功能；另一种是由采集端和分析端两部分组成，采集端主要提供数据采集的功能，将采集到的网络数据发送给分析端，由分析端进一步处理和分析，并采取相应的响应措施。

◆运维安全审计产品：运维安全审计产品是有关网络设备及服务器操作的审计系统。运维安全审计产品主要采集和记录IT系统维护过程中相关人员“在什么终端、什么时间、登录什么设备（或系统）、做了什么操作、返回什么结果、什么时间登出”等行为信息，为管理人员及时发现权限滥用、违规操作等情况，准确定位身份，以便追查取证。
◆运维安全审计产品的基本原理是通过网络流量信息采集或服务代理等技术方式，记录Telnet、FTP、SSH、tftp、HTTP等运维操作服务的活动信息。

网络安全审计主要产品与技术指标

文老师软考教育

◆运维安全审计产品的主要功能有字符会话审计、图形操作审计、数据库运维审计、文件传输审计、合规审计等。
(1)字符会话审计，审计SSH、Telnet等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户IP、设备名称、设备IP、协议类型、危险等级和操作命令等。

(2)图形操作审计，审计RDP、VNC等远程桌面以及HTTP/HTTPS协议的图形操作行为，审计内容包括访问起始和终止时间、用户名、用户IP、设备名称、设备IP、协议类型、危险等级和操作内容等。

(3)数据库运维审计，市计Oracle、MS SQL Server、IBM DB2、PostgreSQL等各主流数据库的操作行为，审计内容包括访问起始和终止时间、用户名、用户IP、设备名称、设备IP、协议类型、危险等级和操作内容等。

(4)文件传输审计，审计FTP、SFTP等协议的操作行为，审计内容包括访问起始和终止时间、用户名、用户IP、设备名称、目标设备IP、协议类型、文件名称、危险等级和操作命令等。

(5)合规审计，根据上述审计内容，参照相关的安全管理制度，对运维操作进行合规检查，给出符合性审查。

网络安全审计应用

◆安全运维保障：IT系统运维面临内部安全威胁和第三方外包服务安全风险，网络安全审计是应对运维安全风险的重要安全保障机制。通过运维审计，可以有效防范和追溯安全威胁操作。例如，通过关联分析还原堡垒机绕行运维操作。公司企业内部的运维人员如果通过堡垒主机对服务器进行操作，则符合公司企业内部的管理要求，若直接对服务器进行操作则视为非法操作，这一行为将被记录下来，通过该审计系统，管理人员可获知有运维人员在执行绕行操作。

◆数据访问监测：数据库承载企事业单位的重要核心数据资源，保护数据库的安全成为各相关部门的重要职责。数据库安全审计产品就是通过安全监测，智能化、自动地从海量日志信息中，发现违规访问或异常访问记录，从而有效降低安全管理员日志分析的工作量。

◆例如，通过分析数据库访问日志信息，可以自动发现违规访问的问题。在特定的业务环境中，用户在正常情况下应该通过前台的业务系统登录后修改后台数据库的内容。假如某个用户绕过了前台的业务系统，直接登录到数据库并篡改了其中的数据，则数据库管理人员通过分析用户访问日志信息，就可以发现该用户的数据库访问行为违背了业务逻辑，缺少与之相关的前台登录行为，从而有效识别该违规访问。

网络安全审计应用

文老师软考教育

◆网络入侵检测：网络入侵检测对网络设备、安全设备、商用系统的日志信息进行实时收集和分析，可检测发现黑客入侵、扫描渗透、暴力破解、网络蠕虫、非法访问、非法外联和DDoS攻击。例如，攻击者常对服务器进行密码破解攻击，管理员可利用日志安全审计系统，实时地收集服务器的日志，分析服务器的认证日志信息，若发现连续多次出现认证出错信息，则可以判定服务器受到密码破解攻击，并产生实时告警，提醒管理员进行处理。

◆网络电子取证：日志分析技术广泛应用于计算机犯罪侦查与电子取证，许多案件借助日志分析技术提供线索、获取证据。如某市公安机关接到该市某大学的校园网络遭到攻击，造成网络瘫痪数日的报警。侦察人员通过路由器的日志文件进行排查，确定具有嫌疑的人员的IP，并根据IP确定了相应的犯罪嫌疑人，将犯罪嫌疑人计算机内的日志文件作为其犯罪的有力证据。

谢谢！

文老师软考教育