主管：中华人民共和国公安部
主办：公安部第三研究所
中国计算机学会（计算机安全专业委员会）

ISSN1671-1122
CN31-1859/TN
中文核心期刊
中国科技核心期刊
中国科学引文数据库来源期刊

信息网络安全

NETINFO SECURITY

等级保护

基于上下文特征的IDS告警日志攻击场景重建方法

技术研究

容器化安全服务功能链低延迟优化编排研究

基于异常加密流量标注的Android恶意进程识别方法研究

一种基于软件定义网络的主机指纹抗探测模型

ISSN 1671-1122
07
9 771671 112200

2020年 7月 第7期
总第235期

信息网络安全
2020年 第7期 · 总第235期
中文核心期刊
中国科技核心期刊
中国科学引文数据库来源期刊

目 次

信息网络安全
2020 年 第 7 期 / 总第 235 期 /7 月 (月刊)
NETINFO SECURITY

□ 等级保护

□ 技术研究

□ 理论研究

□ 网域动态

期刊基本参数：CN31-1859/TN*2001*m*16*108*zh*P* ￥20.00*6000*10*2020-7

CONTENTS

科来网络全流量安全分析系统（TSA）

实时协议鉴别：流量识别是安全分析的第一步，决定了未知威胁的感知能力，科来TSA可以实现多达上万种协议与应用鉴别能力。

感知未知威胁：未知的网络攻击行为往往藏在正常的流量里面。通过各类元数据的恶意网络行为模型匹配技术，科来TSA可以感知隐藏在网络流量中APT攻击、特种木马、安全后门等未知威胁。

攻击回溯取证：只要是网络攻击，就一定会产生网络流量数据。科来TSA不仅保存网络行为和主机行为，同时还保存全部原始数据包数据，并提供PB级数据的秒级搜索，为安全事件的分析与取证提供更多依据。

CSNA网络分析认证

网络分析技术是网络管理的关键技术，**CSNA**认证培训致力于让用户掌握该项技术，提升解决网络安全问题和网络运维问题的能力。

CSNA-A： 通过培训，提升学员解决网络安全问题和网络运维问题的能力，使学员能熟练运用相关产品为用户提供全面的网络分析服务。

CSNA-E： 通过培训，掌握常见协议原理，理论结合实操，使学员充分了解网络分析思路并掌握网络分析技巧，熟练使用各种网络分析工具进行网络分析，达到独立进行网络故障排查及分析定位的目标。

CSNA-S： 通过培训，使学员在安全数据包实战中掌握未知攻击的异常行为及分析思路，见识各类罕见的高级网络攻击方法，从而提高针对高级未知网络攻击的对抗能力。

科来®

科来成立于2003年，是以网络分析技术为核心的高新科技企业，一直致力于网络分析技术的研究与推动，将网络分析技术应用于网络安全态势分析、网络故障诊断、网络性能优化等领域，并提供网络分析认证培训和相关技术服务。

电话：400-6869-069　　官网：www.colasoft.com.cn