

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



9 771671 112200

2020年 7月 第7期

总第235期

□ 等级保护

- 1 基于上下文特征的 IDS 告警日志攻击场景重建方法 姜楠, 崔耀辉, 王健, 吴晋超

□ 技术研究

- 11 容器化安全服务功能链低延迟优化编排研究 徐玉伟, 赵宝康, 时向泉, 苏金树
- 19 基于字节码搜索的 Java 反序列化漏洞调用链挖掘方法 杜笑宇, 叶何, 文伟平
- 30 基于异常加密流量标注的 Android 恶意进程识别方法研究 徐国天
- 42 一种基于软件定义网络的主机指纹抗探测模型 张涛, 芦斌, 李玎, 何康
- 53 面向云平台虚拟层的安全态势评估关键技术研究 余晴, 郑崇辉, 杜晔
- 60 Android 系统应用程序 DEX 文件保护方法研究 袁晓筱, 罗森林, 杨鹏
- 70 基于改进 Border-SMOTE 的不平衡数据工业控制系统入侵检测 张晓宇, 王华忠
- 77 混合 Gabor 的轻量级卷积神经网络的验证码识别研究 刘静, 张学谦, 刘全明

□ 理论研究

- 85 云环境下 Docker 容器隔离脆弱性分析与研究 边曼琳, 王利明

□ 网域动态

- 96 中国科学技术大学在“神威·太湖之光”上首次实现千万核并行第一性原理计算模拟
- 97 清华大学微电子所实现新型神经网络
- 98 北京交通大学计算机学院信息通信网络研究所荣获 IEEE ICC 2020 最佳论文奖
- 99 重庆大学大数据与软件学院在数据驱动的事件流系统监控定量验证研究方面取得新进展

CONTENTS

1	Context-based Attack Scenario Reconstruction Model for IDS Alarms	JIANG Nan, CUI Yaohui, WANG Jian, WU Jinchao
11	Low-latency Optimal Orchestration of Containerized Security Service Function Chain	XU Yuwei, ZHAO Baokang, SHI Xiangquan, SU Jinshu
19	Java Deserialization Vulnerability Gadget Chain Discovery Method Based on Bytecode Search	DU Xiaoyu, YE He, WEN Weiping
30	Android Malicious Process Identification Method Based on Abnormal Encrypted Traffic Annotation	XU Guotian
42	A Host Fingerprint Anti-detection Model Based on SDN	ZHANG Tao, LU Bing, LI Ding, HE Kang
53	Research on Key Technologies of Security Situation Assessment for the Virtual Layer of Cloud Platform	YU Qing, ZHENG Chonghui, DU Ye
60	Research on Android Application DEX File Protection Method	YUAN Xiaoxiao, LUO Senlin, YANG Peng
70	Intrusion Detection of ICS Based on Improved Border-SMOTE for Unbalance Data.....	ZHANG Xiaoyu, WANG Huazhong
77	Research on Captcha Recognition of Lightweight Convolutional Neural Network with Gabor	LIU Jing, ZHANG Xueqian, LIU Quanming
85	Analysis and Research on Vulnerability of Docker Container Isolation in Cloud Environment.....	BIAN Manlin, WANG Liming

敬告:

本期所有文字和图片未经本刊书面许可, 不得转载。

本刊已被中国科技核心期刊、中国科学引文数据库来源期刊、中国学术期刊全文数据库、中文科技期刊数据库(全文版)等数据库收录, 如果作者不同意文章被收录, 请在来稿时向本刊声明, 本刊将做适当处理。



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。



科来成立于2003年，是以网络分析技术为核心的高科技企业，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

