基于 SDN 的一种隐藏端口检测方法

刘玉明 1，王　勇 1,2，俸　皓 1,2
（1 桂林电子科技大学 计算机与信息安全学院, 广西 桂林 541004；
2 桂林电子科技大学 广西云计算与复杂系统高校重点实验室 广西 桂林 541004）

摘　要：考虑基于 SDN 架构的网络环境，并针对当前检测隐藏端口的方法的不足，提出一种全新的基于 SDN 架构的隐藏端口检测方法.利用 SDN 集中控制的特性，通过内存映射流表项的方法来实时提取主机的连接信息，并结合主机代理的信息进行交叉视图检测，同时在检测过程中引入检测状态机，使得准确检测出部署环境下所有主机的隐藏端口.实验结果表明，该方法能高效地检测主机恶意程序隐藏的端口，并具有良好的兼容性和系统性能.

关键词：隐藏端口；木马；　SDN；交叉视图检测

A Method of Detecting Hidden Ports Based on SDN

LIU Yu-ming 1, WANG Yong 1,2, FENG Hao 1,2
(1 School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, China; 2 Guangxi Colleges and Universities Key Laboratory of Cloud Computing and Complex Systems, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract：This paper proposes a method of hidden-ports detection based on SDN, with the characteristics of controlling the whole network, the controller could retrieve all the sessions' information, combined with the customized data received from proxy, the controller could find all the sessions from hidden-ports based on the cross-view of full information and visible information. As the experiment shows, this method could detect all the hidden-ports effectively and compatibly.

Key words：hidden ports；　trojan; SDN; cross-view

作者简介：
刘玉明　男，（1991-），硕士研究生.研究方向为信息安全、云安全.E-mail:367137144@qq.com.
王　勇　男，（1964-），博士，教授.研究方向为云计算、计算机网络技术及应用、信息安全等.
俸　皓　男，（1978-），博士研究生.研究方向为计算机网络、无线传感器网络、软件定义网络及云计算等.