SSH Compromise Detection Using NetFlow/IPFIX

January 2015
By Rick Hofstede (University of Twente), Luuk Hendriks (University of Twente)

In this presentation, the authors discuss IDS SSHCure, the first network-based IDS that detects whether an attack has resulted in a compromise.

Publisher: CERT
Abstract

Dictionary attacks against SSH daemons are a common type of brute-force attack, in which attackers perform authentication attempts on a remote machine. By now, we are used to observing a steady number of SSH dictionary attacks in our networks every day; however, these attacks should not be underestimated. Once compromised, machines can cause serious damage by joining botnets, distributing illegal content, or participating in DDoS attacks. The threat of SSH attacks was recently stressed again by the Ponemon 2014 SSH Security Vulnerability Report, which states that 51% of the surveyed companies have been compromised via SSH in the last 24 months. Even more attacks should be expected in the future; several renowned organizations, such as OpenBL and DShield, report a tripled number of SSH attacks between August 2013 and April 2014. After April 2014, the number of hosts blacklisted by OpenBL for SSH abuse continued to grow and peaks at all-time high values. These numbers emphasize the need for a scalable solution that tells security teams exactly which systems have been compromised and should therefore be taken care of. This is where our open-source IDS SShCure comes into play. SShCure is a flow-based Intrusion Detection System (IDS) and the first network-based IDS that is able to detect whether an attack has resulted in a compromise. By analyzing the aggregated network data received from edge routers, it analyzes the SSH behavior of all hosts in a network. Successful deployments—in networks ranging from Web hosting companies and campus networks up to nation-wide backbone networks—have shown that SShCure is capable of analyzing SSH traffic in real-time and can therefore be deployed in any network with flow export enabled. The latest version of SShCure features a completely overhauled compromise detection algorithm. The algorithm has been validated using almost 100 servers, workstations and honeypots, featuring an accuracy close to 100%.