Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity

Cisco IOS (the software that runs the vast majority of Cisco routers and all Cisco network switches) is the dominant routing platform on the Internet and corporate networks. This widespread distribution, as well as its architectural deficiencies, makes it a valuable target for hackers looking to attack a corporate or private network infrastructure. Compromised devices can disrupt stability, introduce malicious modification, and endanger all communication on the network. For security of the network and investigation of attacks, in-depth analysis and diagnostics are critical, but no book currently covers forensic analysis of Cisco network devices in any detail.

Cisco Router and Switch Forensics is the first book devoted to criminal attacks, incident response, data collection, and legal testimony on the market leader in network devices, including routers, switches, and wireless access points.

Why is this focus on network devices necessary? Because criminals are targeting networks, and network devices require a fundamentally different approach than the process taken with traditional forensics. By hacking a router, an attacker can bypass a network?s firewalls, issue a denial of service (DoS) attack to disable the network, monitor and record all outgoing and incoming traffic, or redirect that communication anywhere they like. But capturing this criminal activity cannot be accomplished with the tools and techniques of traditional forensics. While forensic analysis of computers or other traditional media typically involves immediate shut-down of the target machine, creation of a duplicate, and analysis of static data, this process rarely recovers live system data. So, when an investigation focuses on live network activity, this traditional approach obviously fails. Investigators must recover data as it is transferred via the router or switch, because it is destroyed when the network device is powered down. In this case, following the traditional approach outlined in books on general computer forensics techniques is not only insufficient, but also essentially harmful to an investigation.

Jargon buster: A network switch is a small hardware device that joins multiple computers together within one local area network (LAN). A router is a more sophisticated network device that joins multiple wired or wireless networks together.

* The only book devoted to forensic analysis of routers and switches, focusing on the operating system that runs the vast majority of network devices in the enterprise and on the Internet
* Outlines the fundamental differences between router forensics and traditional forensics, a critical distinction for responders in an investigation targeting network activity
* Details where network forensics fits within the entire process of an investigation, end to end, from incident response and data collection to preparing a report and legal testimony

Download | **Size:** 9.54 MB |

If you want get the unzip password, you need to become VIP member. Then send a request to ciscobibles@gmail.com.