Chapter 2

Network Forensics: Practice

ABSTRACT

In the last few decades, networks have grown to accommodate evolved technologies on every open system for interconnection (OSI) level. On the physical and data link layers, numerous wireless innovations introduced the mobile networks and the interconnection of smart objects. The innovations in network abstraction introduced the cloud- and software-defined networking environments. The high rate and diversity of networking innovations requires adaptations in the forensics approach, so the practice remains capable of uncovering evidence. This chapter explores the operational aspect of both the traditional and the evolved network forensics.

INTRODUCTION

This chapter overviews the evolved network forensics practice. The common tools for sensing, traffic capturing, meta-data acquisition, and forensics analysis are presented as the parts of every network forensics investigation. The advances in cloud, software-defined network, and Internet-of-Things (IoT) forensics are presented as of their specific investigative adaptations and associated challenges. Each of these subfields is discussed to identify the practical similarities that practitioners can find useful for the respective investigations. The chapter concludes by summarizing the unique role of
Network Forensics

the mobile network forensics for the present investigations and the overall evolution of the forensics field.

TRADITIONAL NETWORK FORENSICS

Network forensics in its traditional form aims to uncover evidence from Internet based communication networks. To do so, investigators collect and examine the data-in-transit itself, the logs of the supporting systems such as routers or servers, and the management data of the network. Chapter 1 outlines the techniques for forensics processing but it does not inform how they are operationalized in investigations in different networking environments. For Internet-based networks, this section details the procedures, tools, and forensics investigation challenges.

Network Sensing

Nmap

When preparing and initiating investigations, practitioners need to map the infrastructure to identify the potential sources of evidence. The most popular tool network enumeration is nmap (Lyon, 2017). Designed as a network mapping utility, nmap can be used to discover hosts (ping sweep), scan for known services and ports (Transmission Control Protocol – TCP SYN/ACK, Unsolicited Datagram Protocol - UDP or Streaming Control Transport Protocol - SCTP on a given port) or trace paths to hosts of interest (traceroute). Various scanning techniques can be specified with different TCP flags, ports for known services (e.g. 22 for Secure Shell-SSH or 53 for Domain Name Service - DNS) or a range of ports (1-65535 for all ports). The information about the active Internet Protocol (IP) addresses, associated Medium Access Control (MAC) addresses and the open ports can be complemented with the information about the version of the operating systems and the services running on the hosts. Figure 1 provides an example scan command: nmap -p 1-65535 -sV -O -ss -T4 192.168.56.0/24. The command scans all hosts on a local network (192.168.56.0/24), for all ports (-p 1-65535), checks their service version info (-sV), the operating system (-O) and the scan is executed using a TCP SYN packets (-ss) in a faster mode (-T4). The scan shows two active hosts: 192.168.56.1 (the network gateway) and the host
Mobile Public Key Infrastructures
Encyclopedia of Mobile Computing and Commerce (pp. 581-588).
www.igi-global.com/chapter/mobile-public-key-infrastructures/17139?camid=4v1a