Chapter 8

Network Security Auditing

Yin Pan  
Rochester Institute of Technology, USA

Bo Yuan  
Rochester Institute of Technology, USA

Sumita Mishra  
Rochester Institute of Technology, USA

ABSTRACT

As people increasingly rely on computer systems and networks for services such as online banking, online shopping, and socialization, information security for identity protection and privacy has become more important today than ever. Businesses and organizations are also obligated to provide such security to comply with state and federal laws and regulations. Managing security risks and ensuring compliance with information security regulations and industry standards have become important for businesses and organizations. Security auditing is an effective process to assess policies, procedures, and controls in identifying risks associated with networks and various operating systems. This chapter emphasizes network security audits and discusses various auditing procedures and technologies to identify and examine threats and vulnerabilities in computer networks, and to determine how to assess and manage risk posed to a network.

INTRODUCTION

We live in a connected world, increasingly dependent on computer systems and networks for news, business, social networking, and daily life activities. However, over the past decades, very little has changed in the computer system and network architectures and communications protocols, which were not initially designed for the magnitude of current networks and usages. By taking advantage of existing vulnerabilities and flaws in protocol designs and implementations, adversaries with various motives have launched cyber-attacks against businesses and organizations to steal intellectual property and personal records, which results in financial losses, damaged reputations, serious degradations of critical services, and reduced public confidence (Kraemer et al, 2009; McClure et al, 2009; Wilson, 2009). Network security is a prime concern for governments,
Network Security Auditing

Maintaining network and systems integrity, availability and security is imperative for protecting data and ensuring normal operations.

A combination of technologies such as firewalls, intrusion detection systems (IDS), and encryption, has greatly increased network security, but these are insufficient to prevent web-based attacks, social engineering attacks, social networks attacks, hidden backdoors, etc. To counter these types of attacks, security policies, procedures and controls must be set and checked regularly. Security auditing, through penetration tests (He & Body, 2005), active scanning, passive sniffing and analysis, is an effective process to measure policies, procedures and controls in identifying risks associated with networks and various operating systems (Buchanan & Gibb; Longley et al, 2008; Sayana, 2003; Wright et al, 2008; Zhang et al, 2009). Auditing creates roadmaps for organizations to build defenses and countermeasures against cyber attacks and threats. As Westcott (2007) stated, “A comprehensive security audit may not cure all of a security manager’s data woes, but it should go a long way toward reducing the risk of exposing negative consequences” (p. 8). Audits will uncover security holes that expose organizations to malicious acts.

Information system audits include auditing corporation policies, framework, operating systems and database, application software, physical security, network security, etc. Although most companies are confident about the physical security of their offices and facilities, little is known about the security of their computer networks. This chapter emphasizes on an important component of overall information systems auditing -- network security audits. Procedures and technologies to identify various network threats and vulnerabilities, and determine how to assess and manage risks posed to a network are discussed. This chapter also demonstrates the state of art techniques, through a case study, used in different phases of network auditing including network discovery, penetration, and network threat analysis and control.

BACKGROUND KNOWLEDGE FOR AUDITING

Assets, Vulnerabilities, Threats, and Risk Analysis

Information security includes activities that provide protection for information assets against risks of unauthorized access, misuse, disclosure, modification, or destruction. Information security essentially focuses on four major areas: asset, threat, vulnerability and risk (Alberts, 2003). An asset is any valuable information such as intellectual property, business intelligence, personal identities, and other mission critical data for businesses and organizations. Risk refers to the likelihood of a negative impact or consequence such as financial loss and/or reputation damages. A threat is any deliberate or accidental action that individuals, either internal or external, take to potentially harm an asset, for example, stealing personal identification and bank account information, intellectual property theft, and sabotage. Vulnerability is a defect or weakness in software or computer systems, and human nature that allows a threat to exploit and penetrate security protections. For example, a buffer-overflow vulnerability in an application may allow an attacker to seize control of a system. A social engineering attack takes advantages of weaknesses of human nature such as kindness, greedy, etc. to circumvent security protections. Asset, threat, vulnerability and risk are intertwined such that when threats and vulnerabilities occur at the same time, security can be breached, in which case the asset is harmed, and the risk is realized.

To ensure information security and reduce risks, an organization must identify critical assets and find out how susceptible the assets are to at-