

Federal Reserve Board of Governors

**Course Description for
Network Security Hands-On
(S&R Technology Lab)**

Last Revised: June 2009

Network Security Hands-On (S&R Technology Lab)

The Board of Governors of the Federal Reserve System is proud to offer technology-related courses developed and hosted by the S.T.R.E.A.M./Technology Lab at the Federal Reserve Bank of Chicago, Chicago, Illinois. For over nine years, the S.T.R.E.A.M./Technology Lab has pursued a unique approach to examiner technology training by combining hands-on exercises with lectures. Learning materials are based on applicable FFIEC Examination Handbooks and other examiner guides. The exercises reinforce concepts by allowing participants to interact with various vendor software applications, operating systems, and security appliances widely used in the financial industry and observing how they work. Each participant has a PC at their disposal in the state-of-the-art facility which supports teleconferencing, audio/video recordings, and interactive participant response systems.

Type of Participant Targeted

The Network Security course is a 4-day course intended for examiners with IT examination responsibilities but who may not have had university training in information technology. At least one year of field examination experience is preferred.

Prerequisites

None required.

Course Overview

This course provides participants with a technical grounding in networking concepts and technologies that are critical to IT operations in financial institutions, including TCP/IP networking protocols and common network infrastructures and configurations. The course examines key network perimeter security tools, including firewalls and intrusion detection systems (IDS).

Course Objectives

After completing the course, the participant, at a minimum, will be able to demonstrate the following skills:

- Explore, map, and analyze realistic TCP/IP networks using a variety of diagnostic software tools
- Implement, test, and maintain common firewall types and architectures in a simulated E-banking setting
- Identify different IDS products currently available, effectively implement and manage these systems, and understand the controls needed for maintaining an IDS infrastructure
- Discuss examination procedures outlined in the IT Examination Handbook produced by the FFIEC

Post-Course Intervention

Participants will learn the essential components that comprise a network. For each technical element (e.g.; firewalls and intrusion detection systems), participants should be provided with opportunities to review appropriate controls.

Overview of Network Security Curriculum

Subject	Approximate Class Hours
Network Attack Vectors	1.0
Anti-Virus and Spyware Exercises	1.0
Microsoft Baseline Security Analyzer Exercise	1.0
Perimeter Defense: Firewalls	2.0
Password Cracking Exercise	.5
Network Diagramming and Exercises	3.0
Router Exercise	1.0
Wireless Networking and Exercises	1.5
Protocols	.75
Encapsulation and Exercises	2.0
NMap Exercise	.75
DNS/FTP/Telnet Exercises	2.5
Firewalls and Exercises	2.5
Intrusion Detection/Prevention Systems	2.5
IDS/IPS Exercises	2.5
Total Lecture & Exercise Hours	24.50 (*)

(*) Note: The total number of hours and topics may vary from class to class.
28 Continuing Professional Education (CPE) Credits may be earned.

Learning Objectives

Examiners should be able to articulate the key risk elements associated with operating and managing a production network. Good network security starts with an accurate risk assessment. Accuracy in this case means that consideration should be given to potential risks for each system (internal and external) and that all systems should be inventoried. Change management is critical as is ensuring that hosts are hardened according to corporate guidelines. Remote access also needs to be managed to include some form of monitoring and logging. Finally, the financial institution must be able to articulate a risk mitigation strategy; this should be reviewed to ensure that new applications and/or systems are treated from a holistic perspective, and that controls for all systems are re-evaluated for effectiveness periodically.

By module, the participant, at a minimum, will able to do the following:

Module	Learning Objectives
Network Attack Vectors	<ul style="list-style-type: none">• Identify and understand the technical implications of the latest network attack vectors• Assess effectiveness of alternative mitigation techniques
Perimeter Defense: Firewalls	<ul style="list-style-type: none">• Evaluate and assess appropriate implementation of firewall controls relative to the complexity of a given network• Use network configuration and sound design of firewall architecture through multiple filter points, active firewall monitoring and management and integrated security monitoring
Network Diagramming	<ul style="list-style-type: none">• Review the elements of layered security and understand how network devices are used to separate zones of risk
Protocols	<ul style="list-style-type: none">• Illustrate the OSI model by following a packet from encapsulation on one computer to de-encapsulation on another• Examine the various protocol characteristics and evaluate the risk associated with using protocols in a production environment
IDPS Systems	<ul style="list-style-type: none">• Distinguish between alert and block versus alert and pass strategies• Identify sound practices associated with current state-of-the-art intrusion detection and prevention system (IDPS) devices

Class Size

The optimal class size for the Network Security course offerings is approximately 25 participants. To provide sufficient variety of interaction among class participants, the minimum class size should be 10 participants.

Instructors

Network Security courses include one or more instructor(s) from the Federal Reserve System and may also include instructors from an external agency. This course may require from 3-5 total instructors.