

COURSE TITLE: LINUX SECURITY ADMINISTRATION

COURSE NUMBER: NITA 412

PREREQUISITE: BEDU 212 OPEN SOURCE PLATFORM AND NETWORK ADMINISTRATION

CATALOG DESCRIPTION

Students examine the infrastructure and configuration of complex Linux-based networks as a basis for creating such a network. The course includes implementing selected special servers in the network and testing various configurations for performance and security. Students identify the vulnerabilities of a complex network, apply security controls, and troubleshoot problems in complex networks. Ethical, legal, and professional conduct and security policy are discussed in the course.

COURSE OBJECTIVES

Upon completion of the course, students will be able to:

1. Apply appropriate theory and design principles to the development of complex (n-tiered) networks.
2. Build complex networks using Linux servers for mixed environments (both Linux and Microsoft clients).
3. Install selected networked application server software on Linux servers (e.g., email server).
4. Explain vulnerabilities of Linux networks, the most prevalent threats to security, and the security controls used to defend networks.
5. Perform a range of attacks in a closed, self-contained network laboratory.
6. Correct the results of successful attacks.
7. Implement controls to prevent or lessen the impact of attacks.
8. Take positions on the ethical, legal, and other professional conduct expected of information security and assurance professionals.
9. Create/modify network security policies for organizational environments.

OUTLINE OF CONTENT

1. Brief review of Linux networking fundamentals
 - a. Client services
 - b. Network services
 - c. Storage and file-sharing services
2. Design of n-tiered networks
 - a. Network infrastructure
 - b. Special servers
 - c. Evaluation of various configurations of servers and clients
3. Configuring basic services in the complex network
4. Configuring major network services in the complex network
5. Security administration practices

- a. Monitoring and auditing
- b. Continuity planning and disaster recovery
- c. Major attacks on Linux networks
- d. Detection and correction practices
- e. Controls
6. Configuring network security
 - a. Connectivity
 - b. Firewalls, proxy servers, and Web services
 - c. Honeypots
7. Professional, ethical, and legal conduct
8. Network security policies

STUDENT ASSIGNMENTS, EVALUATION, AND GRADING

Concept tests (25%)

Biweekly tests allow the student to demonstrate their understanding of n-tiered network architecture, design principles, security concepts, and security administration.

Laboratory exercises (25%)

These exercises permit students to re-configure selected components of complex networks. These exercises include security activities as well as troubleshooting problems in network configuration. These activities require use of the NITA laboratory both in and outside of class time. Exercises follow presentation of theory.

Building the network (35%)

Students will demonstrate their ability to install and configure complex networks that accomplish the goals established by the instructor. This work will require one or more teams of students. Students will resolve problems built into Linux networks to demonstrate their ability to deal with both network problems and security vulnerabilities.

Network security administration plan (15%)

As a capstone course requirement students must prepare a written plan for security an n-tiered Linux network for an organization approved by the instructor and present the plan to the class. This plan must includes appropriate security policies that should be adopted by the organization. This may be done individually or by teams of two students.

BIBLIOGRAPHY

(Note: The available resources on Linux platform and network administration are vast, including a number of major Websites that support administrators. This bibliography

primarily demonstrates that resources on the course topics are published and available from a variety of major publishers. Among the Web sites are those of professional organizations that promulgate codes of professional conduct for IT professionals. These include the ACM, Certification Institute for System Security Professionals (CISSP), Association for Information Technology Professionals (AITP), and others.)

Bauer, M. D. (2005). *Linux server security (2d ed.)*. O'Reilly.

Blancharski, D. (1998). *Network security in a mixed environment*. Foster City, CA: IDG Books.

Cole, E. & Krutz, R. L. (2005). *Network security bible*. Indianapolis, IN: Wiley Publishing

Corbet, J., Rubini, A. & Kroah-Hartman, G. (). *Linux device drivers, 3d edition*. O'Reilly.

Fadia, A. (2002). *Network security: A hacker's perspective*. Portland, OR: Premier Press.

Garfinkle, S., Schwartz, A. & Spafford, (2003). G. *Practical Unix and Internet security (3d ed.)*. O'Reilly.

Hart-David, G. (2001). *Internet piracy exposed*. Alameda, CA: SYBEX.

Kaeo, M. (2003). *Designing network security*. Cisco Press.

Mann, S. (with Krell, M.). (2002). *Linux TCP/IP network administration*. Upper Saddle River, NJ: Prentice-Hall PTR.

Limoncelli, T. & Hogan, C. (). *The practice of system and network administration*. Addison Wesley/Pearson Education.

Negus, C. (2005). *Linux bible, 2005 edition*. Indianapolis, IN: Wiley Publishing.

Noonan, W. J. & Love, P. (2005). *Hardening network security*. New York: McGraw-Hill, Inc.

Northcutt, S. & Zeltser, L. (2005). *Inside network perimeter security*. Upper Saddle River, NJ: Pearson Education.

Poulson, K. L.. (2000). *Hackproofing your network*. Rockland, MA: SYNGRESS.

Sawicki, E. (2006). *Advanced guide to Linux networking and security*. Boston, MA: Thomson Learning/Course Technology.

Smith, P. G. (2005). *Linux network security*. Rockland, MA: Charles River Media.

Stallings, W. (1995). *Internet security handbook*. Foster City, CA: IDG Books.

Taylor, T. (ed.). (2002). *Security complete*. Alameda, CA: SYBEX.

Viega, J. (2002). *Network security with OpenSSL*. O'Reilly.