Kutztown University
Kutztown, Pennsylvania

Computer Science Department
College of Liberal Arts and Sciences

I. Course Description: CSC 580: Selected Topics in Computer Science: Intrusion and Anomaly Detection

This course covers important issues in the detection of intrusions and anomalies. Topics covered include intrusion detection systems, intrusion prevention systems and anomaly and misuse detection on hosts and networks. A variety of tools, techniques, and methodologies for monitoring computer systems and networks will be discussed. Students will learn how to identify and respond to computer system and network intrusions.

3 s.h. 3 c.h. Prerequisite: None.

II. Rationale

As computer and network utilization increases, so does the number of attempts to hack into the networks and their computer systems. Unauthorized users are trying to affect the operation of these systems and networks, steal data and crimple organizations. There has been an increase in identity theft and international concern for governmental systems. It is important for computer science professionals to understand the differences between normal and abnormal use and be able to respond to anomalies.

III. Course Objectives

Upon completion of the course the student will be able to:

A. Describe Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs).
B. Identify anomalies in computer systems and network traffic.
C. Explain the implementation details of intrusion detection systems and methodologies.
D. Analyze intrusion detection approaches and systems.
E. Develop techniques and tools to create intrusions.
F. Implement intrusion detection practices and systems.

IV. Course Assessment

The course assessment will be a subset of tests, projects, papers, presentations, quizzes, homework, team assignments and final exam.

V. Course Outline

A. Network Protocols
    a. Transport layer
    b. Network layer

B. Security Overview
    a. Threats
    b. Vulnerabilities
    c. Risks

C. Network Traffic Analysis

D. Network Security
    a. Overview
    b. Tools
    c. Methodologies

E. Intrusions
    a. Types
    b. Identification
    c. Tools
    d. Detection
    e. Penetration testing

F. Intrusion Detection Systems
    a. Overview
    b. Types
        i. Host-Based
        ii. Network-Based
        iii. Signature Detection
        iv. Anomaly Detection
    c. Intrusion Prevention Systems

VI. Instructional Resources

Beale, J., Baker, A.R., and Esler, J. *Snort: IDS and IPS Toolkit*. Syngress. 2007. *

Bejtlich, Richard. *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press. 2013.

Bhattacharyya, Dhruba Kumar and Kalita, Jugal Kumar. *Network Anomaly Detection: A Machine Learning Perspective*. Chapman and Hall/CRC. 2013.

Bhange, Anup and Marhas, Manmeet Kaur. *Anomaly Detection in Network Traffic; A Statistical Approach: Flood and Flash Crowd Anomaly in Network Traffic.* LAP LAMBERT Academic Publishing. 2012.

Caswell, B., Beale, J., and Baker, A. *Snort IDS and IPS Toolkit (Jay Beale's Open Source Security).* Syngress. 2007.

Chappell, Laura and Combs, Gerald. *Wireshark ® 101: Essential Skills for Network Analysis (Wireshark Solutions).* Laura Chappell University. 2013.

Chappell, Laura and Combs, Gerald. *Wireshark Network Analysis: The Official Wireshark Certified Network Analysis Study Guide*. Second Edition. Laura Chappell University. 2012.

Cisco Learning Institute. *Security+ Guide to Network Security Fundamentals.* Thomson/Course Technology. 2003. *

Cole, E., Krutz, R., and Conley, J.W. *Network Security Bible.* John Wiley. 2009. *

Du, Sumeet and Du, Xian. *Data Mining and Machine Learning in Cybersecurity,* Auerbach Publications. 2011.

Engebretson, Patrick. *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Syngress. 2011.

Fung, Carol and Boutaba, Raouf. *Intrusion Detection Networks: A Key to Collaborative Security*. Auerbach Pubications. 2013.

Gregg, Michael. *Build Your Own Security Lab: A Field Guide for Network Testing*. Wiley. 2008. *

Gregg, Michael and Watkins, Stephen. *Hack the Stack: Using Snort and Ethereal to Master the 8 Layer of an Insecure Network*. Syngress Pub. 2006. *

Harrington, Jan L. *Network Security: A Practical Approach*. Elsevier. 2005. *

Henry, Kevin M. *Penetration Testing: Protecting Networks and Systems*. IT Governance Pub. 2012. *

Hosmer, Chet. *Python Forensics: A workbench for inventing and sharing digital forensic technology.* Syngress. 2014.

Kar, Dulal Chandra and Syed, MahBubur Rahman (editors). *Network Security, Administration, and Management: Advancing Technology and Practice.* Information Science Reference. 2011. *

Kim, Peter. *The Hacker Playbook: Practical Guide to Penetration Testing*. CreateSpace Independent Publishing Platform. 2014.

Krawetz, Neal. *Introduction to Network Security*. Charles River Media. 2007. *

Long, Johnny. *Pentration Tester's Open Source Toolkit.* Syngress Pub. 2006. *

Lyon, Gordon Fyodor. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Nmap Project. 2009.

Maiwald, Eric. *Network Security: A Beginner's Guide*. McGraw-Hill Professional Publishing. 2002. *

Maynor, David and Mookey, K.K. *Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research.* Syngress. 2007. *

McClure, S., Scambray, J., and Kurtz, G. *Hacking Exposed: Network Security Secrets & Solultions.* McGraw-Hill/Osborne. 2005. *

National Institute of Standards and Technology (NIST). *Guide to Intrusion Detection and - Prevention Systems (IDPS)*. CreateSpace Independent Publishing Platform. 2013.

O'Connor, T. J. *Violent Python: A Cookbook for Hackers, Forensic Analysts, Pentration Testers and Security Engineers*. Syngress. 2012.

Pale, Paulino Calderon. *Nmap 6: Network Exploration and Security Auditing Cookbook.* Packt Pub. 2012. *

Pathan, Al-Sakrib Khan. *The State of the Art in Intrusion Prevention and Detection*. Auerbach Publications. 2014.

Rash, M., Orebaugh, A., Clark, G., Pinkard, B., and Babbin, J. *Intrusion Prevention and Active Response*. Syngress. 2005. *

Sanders, Chris. *Applied Network Security Monitoring: Collection, Detection, and Analysis*. Syngress. 2013.

Sanders, Chris. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.* Second Edition. No Starch Press. 2011.

Schiffman, Mike. *Building Open Source Network Security Tools: Components and Techniques*. Wiley Pub. 2003. *

Seagren, Eric. *Secure Your Network for Free: Using Nmap, Wireshark, Snort, Nessus, and MRTG.* Syngress. 2006. *

Seitz, Justin. *Black Hat Python: Python Programming for Hackers and Pentesters*. No Starch Press. 2014.

Trost, Ryan. *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century.* Addison-Wesley Professional. 2009.

U.S. Department of Commerce. *Guide to Intrusion Detection and Prevention Systems (IDPS).* CreateSpace Independent Publishing Platform. 2014.

Whitman, Michael. *Guide to Network Security*. Course Technology. 2013. *

Yu, Zhenwei and Tsai, Jeffrey J. P. *Intrusion Detection: A machine learning approach*. Imperial College Press. 2011. *

* Available in KU's library