Proceedings of the 10th Colloquium for Information Systems Security Education
University of Maryland, University College
Adelphi, MD June 5-8, 2006

Practical Curriculum for the Future ISSO

Gerald Clevenger, *Instructor* and Tammy Alexander, *Program Coordinator,* Fountainhead College of Technology

Abstract – In order to effectively perform in today's fast paced environment, the Information Systems Security Officer (ISSO) must be well prepared to deal with technical, regulatory and legal issues as well as policy oriented concerns. A multi-disciplinary curriculum is therefore required to properly prepare the Information Assurance (IA) degree seeking student for the many challenges the future ISSO will face. To address this issue, Fountainhead College of Technology has implemented a bachelor degree program that attempts to simulate the "real-world" corporate or government agency environment. This paper provides an overview of the program methodology, coursework and labs required for the Bachelor of Applied Science in Network Security & Forensics (BASNSF) program.

Index terms – information security curriculum development, INFOSEC coursework, IA curriculum, hands-on training

I. Introduction

The field of Information Security is relatively new. Many information security subject matter experts have migrated to information security after years of system or network support careers, while the Corporate Information Officer (CIO) or Designated Accrediting Authority (DAA) were more likely project managers with strong IT backgrounds. The result has been the development of Information Assurance (IA) standards that reflect not only the quality assurance standards of project management, but also the procedures utilized in managing an enterprise network or datacenter. The BASNSF program at Fountainhead College of Technology (FCT) couples the skills of project management with technical enterprise network and system management to fulfill the requirements for a career in IA and information security.

This paper provides an overview of the BASNSF program to include required courses, prerequisites, methodology, results and future work.

II. Program Overview

The goal of the BASNSF program is to simulate a site information security team with the responsibility for the development and implementation of an effective enterprise information security program. The coursework consists of a physical site risk assessment, Business Continuity and Disaster Recovery Plan, and System and Network Security Plans in order to complete a Site Automated Information Security Handbook. In each instance, the completion of the security plan requires implementation of a system or network security project. In order to procure resources for the projects students must propose, plan, implement, and document each project. By requiring students to develop project proposals, presentations, and implementation plans for a secure enterprise network and to implement those proposals and projects, the students can experience day-to-day issues such as patch management, account management, and vulnerability mitigation.

As with a real site security program group, the BASNSF program is susceptible to the day-to-day concerns of funding, zero day worms and viruses, intrusion attempts, and various audits and assessments.

Current events can change the focus of a class session by introducing challenges such as the latest worm, local weather event or service outage. Just as with a "real-world" site security organization, zero day alerts and events help to demonstrate the need for incident planning and response as well as the value of lessons learned.

III. Program Prerequisites

The BASNSF program provides 66 semester credit hours of instruction, which compliments any accredited post-secondary computer-centric associate's degree. Prospective students that have a non computer-centric associate's degree or higher that wish to enroll in the program must be able to demonstrate a proficiency in computer and network technologies, such as 3 CompTIA, any 2 Microsoft, any 2 Novell, or any 1 Cisco certification or at the discretion of the Institute.

Classes meet 20 hours per week for 4 semesters (60 weeks), assuming the entrance criteria has been met.

The BASNSF degree is awarded upon completion of 126 semester credit hours in the following areas: 94 technical (60 from technical occupational associate program and 34 security classes) in addition to 32 general education classes.

The course of study is intended for students who are interested in complementing their previous associate level technical training and experiences with additional security

and general education courses in order to gain both the award of a bachelor's degree and network security oriented job placement.

The program is designed to provide quality training in the essentials of network security & forensics including: the comprehension and appreciation of security issues and forensic studies, the development of effective communication, interpersonal and critical thinking skills, and an understanding of security and how it influences business operations.

The program length is usually 16 to 32 months, depending on preexisting credits.

IV. Program Methodology

The BASNSF program is based upon the Certified Information Systems Security Professional (CISSP) [1] industry standard security certification and the Committee on National Security (CNSS) [2] standards. Associate and bachelor level technology instructors work together closely to define a cohesive curriculum to allow reinforcement of IA principles throughout the student's college career. For example, many of the associate technology curriculum course elements are mapped to CNSS standards 4011 and 4013 which are focused on the technical aspects of IA. The bachelor level IA concentration courses have elements mapped to CNSS standards 4011, 4012, 4013 and 4014A that are focused on technical as well as policy and regulatory issues. Technology instructors also maintain an ongoing dialogue to ensure coursework continuity. Due to these factors, students that attend the entire Information Technology associate degree program followed by the BASNSF degree program receive the maximum overall program benefit.

Students generally move through the program in cohorts of approximately 18 - 20 students. In the first course, NSF 401 (Security Management Practices), students are introduced to a company called NSF, Inc. They are then given a document that contains a description, history, network design and diagram, and Active Directory design and diagram of NSF, Inc. Many (although not all) of the projects, labs and exercises are based on the NSF, Inc. infrastructure document. The capstone project is the final result of the entire program - a website containing a comprehensive NSF, Inc. Site Security Plan with supporting documentation - which is a culmination of all of the documentation created throughout the NSF courses.

In addition to the documentation development for the NSF, Inc. site, the second major project for the students of the December 2005 graduating class was to design, configure, and implement the network security and forensics lab. This project was completed solely by students of the BASNSF degree program.

Semester projects are determined by the most current needs of the lab, advances in technology, or updates in operating systems and tools.

NSF, Inc. is indeed run like a true corporation. The designated CIO is the instructor, and the CIO assigns roles such as VPN Administrator, Project Manager, Network Architect and Physical Security Site Manager for each student. Throughout the program, documentation is developed for NSF, Inc. according to current course requirements. Each document that is developed must be accompanied by a proposal. Students are required to work in teams and are held accountable for their individual roles, as well as group (departmental) projects. For example, as with a "real world" corporation, documentation is not merely submitted for a grade, but project team members must agree upon and submit a formal proposal for approval (sign off) by key members, including the NSF, Inc. CIO.

V. Coursework

Each BASNSF course normally consist of a group project along with a performance based individual technical demonstration or lab. The group project requirements include a proposal, project plan, and needed documentation such as forms or checklist. Projects are proposed, planned, and implemented solely by the students under the direction of the designated CIO. In addition to team projects, individual labs and presentations, each student is required to submit a semester project approved by the instructor.

A. NSF 401: Security Management Practices

Security Management Practices is the first BASNSF course. It is designed to reintroduce students to the basics of network security practices and models. Coverage includes formulation of risk management and understanding of business objectives. The class includes the formulation of a security program in any business environment. Security policy principles are introduced in this course and the interrelationship of laws, the legal system, security policy and procedures are explored. Current requirements organizations face to protect themselves, privacy concerns, and written policy enforcement are covered. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

As previously mentioned, in NSF 401 the students are introduced to NSF, Inc. and given a comprehensive description of the company's network schema and history.

The first section of NSF 401 addresses risk assessment and the need for policies and procedures. Project teams are established for the development of policies and procedures for the NSF, Inc. Students are provided with an overview of project planning and project management and sample project plans with work breakdown structure and responsibility matrix are provided to each group. The project team will follow the development of an NSF, Inc. security handbook or web page.

The second section of NSF 401 involves an introduction to change management. Students are required to research and discuss current change management plans as a prelude to NSF 405 – Operations Security.

B. NSF 403: Security Models and Architecture

Concepts relating to the design, testing and implementation of a computer system and network infrastructure are presented. Students learn a variety of methods of securing the flow of data on Automated Information Systems (AIS), as well as the best practices to employ when developing computer systems and designing network architecture. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

NSF 403 introduces the concept of Information System security modes of operation, security models (no read up, no write down) Trusted Computer Evaluations Criteria (TCEC) [3] as well as certification and accreditation. An introduction of the National Security Agency (NSA) approved Information Assessment Methodology (IAM) [4] and Information Evaluation Methodology (IEM) [5] in the assessment and evaluation of the NSF, Inc. infrastructure is also provided. Systems must undergo certification and accreditation and be submitted to the DAA (Instructor).

Class projects are focused on securing the NSF Inc. site with group policies (e.g., develop group policies to implement the site policies such as warning banners and the NSF, Inc. security template.)

C. NSF 404: Telecommunications and Network Security

Through presentation of interesting case studies, this course illustrates the interaction of network security principles to communication protocols and technologies. Understanding the types of incidents likely to occur in a given environment will assist the students in preparation of interactive lab exercises. Students interactively learn in a test environment to recognize, examine and determine the cause of potential incidents that are likely to occur on a network infrastructure. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

The goal of NSF 404 is to develop a perimeter protection plan for NSF, Inc. Students start with the implementation of a border router to filter out noise. They then propose and implement network monitoring and a Demilitarized Zone (DMZ) for public access to certain content and develop a Firewall Plan. Deployment of a SNORT [6] Intrusion Detection System is a required project for this course. The installation and configuration of the Firewall solution is demonstrated in NSF 412 – Operations Systems Hardening.

D. NSF 405: Operations Security

Presenting the methodology and tools with which students can successfully audit and investigate security issues in the network environment, Operations Security offers students the opportunity to gain a broad understanding from a larger enterprise viewpoint. Planning of successful operational level practices and the usage of tools and methods for investigating network incidents are covered. This course contains 3 semester credit hours (45 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

NSF 405 presents methodology to maintain a secure environment through the use of policies and procedures to assure the continued assessment and evaluation of information resources. Emphasis is given to develop a continual vulnerability assessment and mitigation process, including patch management and change management for all network resources. The results of the vulnerability assessment and evaluation should emphasize the importance of patch management. The importance of policy enforcement for remote connection is discussed and solutions explored. Technologies for policy enforcement such as 802.1X [7] and User Quarantine are also addressed. Implementation of a Microsoft Server Update Service [8] is a required lab for this course. Configuration control and change management policies and procedures must also address patch management solutions for Linux systems and network devices. Weekend reading focuses on the most current patch management articles in order to demonstrate the need for patch management of network devices.

E. NSF 406: Physical Security & Access Control

Securing access to organizations assets and buildings is a vital part of security policy development and implementation. This course offers a thorough understanding of different types of sensor technology and their usage, introducing students to a variety of methods and equipment used to maintain access control from a

network security perspective, including both physical and technical controls. Physical security methodology and access control techniques used to protect organizations from internal and external threat agents are examined. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

NSF 406 provides students with an introduction to physical access, asset management through physical security, personnel management, and physical security risk assessments. ADT [9] security service sends a guest speaker each year to demonstrate motion detectors, video surveillance and monitoring, biometrics, and cyber locks.

Physical access control projects include the implementation of an access control system utilizing biometrics. Students conduct a risk assessment of the facility and submit a report with recommendations for security improvements. Recommendations usually include both procedural and technical solutions for risk mitigation. The risk assessment is used as the basis of the Disaster Recovery Plan (DRP) developed in NSF 408 – Disaster Recovery & Business Continuity.

F. NSF 407: Application & System Development

Relevant issues relating to the secure development and deployment of software on a network infrastructure and AIS are addressed. This course also covers concerns with the distribution of network operating systems and services on a network, along with the potential pitfalls and strategies employed when implementing software onto a network infrastructure. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

This course is an introduction to secure applications including malware and database security. Students are introduced to open database connectivity and object oriented programming. NSF 407 is composed primarily of hands-on labs utilizing several 'victim' computers to demonstrate the various tools available to discover and exploit vulnerabilities. Metasploit framework is used to compromise systems to demonstrate the need for application security. Individual labs utilize freely available exploitation resources and tools to demonstrate methods used to discover various exploits. A review of the White Hat Code of Ethics may be advisable during the NSF 407 lab activities.

G. NSF 408: Disaster Recovery & Business Continuity

A solid understanding of determining threats to the business and the design and implementation of countermeasures is provided. The course focus is on protecting the resources of the business and developing contingency plans. The decisions and responsibilities of maintaining secure network services and resources in an organization's infrastructure are covered. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

The importance of business continuity and disaster recovery require preparing for disasters, equipment failure and malfunction, and user errors as well as destruction or loss of data due to information security incidents such as system compromise, sabotage, and deliberate acts performed to damage or delete valuable data. Students are required to develop business continuity plans, disaster recovery plans, and incident response teams to react to potential compromise of data.

H. NSF 409: Cryptography

This course is designed to introduce students to the basics of cryptography and the practical application in software, hardware and communication protocols. The class features evaluation of different encryption technology and hands-on labs and exercises. The fundamentals and application of cryptography methods are introduced. Labs consist of assigned practice, projects and/or case studies relating to topics covered. Course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

This course is designed to introduce students to practical applications of cryptography. Emphasis is given to public key infrastructure and IPSec. A historical overview of the development of certain ciphers tracks the development of DES from the Lucifer cipher to the recent adoption of AES. Each student is required to research and submit a presentation covering a choice of cryptographic algorithm or innovation that resulted in a significant contribution to modern cryptography. Weekend assignments include the evaluation and discussion of the NIST Crypto Toolkit [10].

Labs during NSF 409 include the installation of Pretty Good Privacy (PGP) [11] and the use of encrypted communications for internal e-mail. The class is required to implement IPSec on the NSF Inc. network. Ethereal [12] is utilized to monitor traffic both before and after the implementation of an IPSec policy.

I. NSF 410: Law, Investigations & Ethics

Students are given a firm foundation of the relationship between the laws and the legal system and security policy and procedures. Students gain an understanding of the

different requirements currently placed upon organizations to protect themselves to include privacy concerns and the enforcement of written policy. Knowledge is integrated with design, writing and implementation of usable security policies and procedures. Management's objectives and goals in a business environment are presented. This course contains 2 semester credit hours (30 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

This course is designed to give the student a firm foundation of the relationship between the laws and legal system as it relates to security policies and procedures. Students gain an understanding of the various current regulatory requirements placed upon organizations to protect their information resources. Lab exercises for NSF 410 include the demonstration and proper use of evidence collection procedures and the use of chain of custody forms to maintain positive control of digital evidence.

J. NSF 412: Operating Systems Hardening

This course is designed to introduce students to operating system hardening and general operating system protection characteristics. Typical characteristics of design, functions and implementation assurance for Windows, Linux and Cisco operating systems are presented. The student will gain an understanding of how operating systems function and how to evaluate their security weaknesses. This course contains 3 semester credit hours (45 clock hours) of lecture and 1 semester credit hour (30 clock hours) of laboratory work.

The objective of this course is to introduce the student to operating systems that will be encountered in the work environment. The student will also be exposed to weaknesses of these operating systems and some of the techniques that can be used to protect or "harden" them. Operating systems covered include Microsoft Windows 2000/2003/XP, Linux and Cisco IOS.

K. NSF 413: Computer Forensics

Methods for acquiring, converting and analyzing data in the interest of determining potential legal evidence are presented. Preservation, identification, extraction and documentation of computer evidence, as well as a basic understanding of computer forensics and the use of industry standard computer forensic tools are presented. Sophisticated technology tools and procedures are introduced to guarantee the accuracy in digital evidence preservation and processing. This course contains 2 semester credit hours (60 clock hours) of laboratory work.

The focus of this course is to introduce students to the proper methods of evidence gathering, examination, and reporting. Students utilize tools including Access Data Ultimate Toolkit [13], Sleuth kit [14], and Encase [15] to examine computer media and generate reports on any evidence discovered. NSF 413 combines lectures in evidence gathering techniques and chain of custody with instructional demonstrations of the use of windows file properties to establish a timeline of files attributes. Additionally, instructional cases on vendor supplied training software are used to demonstrate the proper methods for review and retrieval of information from storage media using both Access Data Forensics Tool Kit and Encase. Required projects for NSF 413 include the confiscation of a hard drive using proper evidence gathering techniques, chain of custody procedures, drive imaging, media examination, and results reporting.

VI. Program Results

At the end of the program, each student will have been a part of developing the following plans, policies, and procedures for the entire corporation of NSF, Inc. to include:

- Project Charter
- Site Security Plan
- System Security Plan
- Change Management Plan
- Anti-virus Policy and Procedure
- Various Implementation Plans (Linux, AD, VPN, Radius, etc.)
- Security Awareness Plan
- Acceptable Use Policies

An example of the final project documentation developed by BASNSF students can be viewed on the web [16].

VII. Conclusion

With this practical methodology, the BASNSF Program accurately prepares the future ISSO not only for the technical tasks involved in developing security policy, procedures and plans, but allows the student to learn how to work as part of a team in the IA development process. Students graduate with an in-depth understanding of how to prepare security documentation in accordance with governing rules and regulations. Additionally, upon graduation they are comfortable with the procedures required for submitting and gaining approval for proposals in a government, as well as a corporate environment.

VIII. REFERENCES

[1] *CISSP examination* (n.d.). Retrieved April 19, 2006, from https://www.isc2.org/cgibin/content.cgi?category=1331
[2]*The committee on national security systems* (n.d.).Retrieved April 19, 2006, from http://www.cnss.gov/
[3]*Department of defense trusted computer system evaluation criteria* (1985). Retrieved March 19, 2006, from http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
[4] *INFOSEC assurance training and rating program* (n.d.). Retrieved March 19, 2006, from http://www.iatrp.com/iam.cfm
[5] *INFOSEC assurance training and rating program* (n.d.). Retrieved March 19, 2006, from http://www.iatrp.com/iem.cfm
[6] Snort.org (n.d.). Retrieved March 19, 2006, from http://www.snort.org
[7] IEEE Standards Catalog (n.d.). *IEEE 802 standards* list. Retrieved March 19, 2006, from http://grouper.ieee.org/groups/802/802info.html
[8] *Windows server update services* (n.d.). Retrieved March 19, 2006, from http://www.microsoft.com/windowsserversystem/updateservices/default.mspx
[9] *ADT security services* (n.d.). Retrieved March 19, 2006, from http://www.adt.com/adt
[10] Computer Security Research Center (2003). *Cryptographic toolkit*. Retrieved March 19, 2006, from http://csrc.nist.gov/CryptoToolkit
[11] *Pretty good privacy* (n.d.). Retrieved March 19, 2006, from http://www.pgp.com
[12] *Ethereal* (n.d.). Retrieved April 19, 2006, from http://www.ethereal.com/
[13] Access Data (n.d.). *Ultimate toolkit*. Retrieved March 19, 2006, from http://www.accessdata.com/products/utk
[14] *The sleuth kit* (2005). Retrieved March 19, 2006, from http://www.sleuthkit.org/sleuthkit/
[15] *Encase forensic* (n.d.). Retrieved March 19, 2006, from http://www.guidancesoftware.com/products/ef_index.asp
[16] *Course documents* (2005). NSF Network Security. Information Assurance. Retrieved April 18, 2006, from http://srv5.fountainheadcollege.com/studentweb/nsf/docs.shtml