# American Public University System

*The Ultimate Advantage is an Educated Mind*

**School of Science and Technology**
**Department of Information Technology**
**ISSC642: Intrusion Detection & Incident Handling**
**3 Credit Hours**
**8 Week Course**
**Prerequisite(s): None**

## TABLE OF CONTENTS – TOC


| | |
|---|---|
| Instructor Information | Evaluation Procedures |
| Course Description | Grading Scale |
| Course Scope | Course Outline |
| Course Objectives | Policies |
| Course Delivery Method | Academic Services |
| Course Materials | References and Additional Reading |


TOC

## INSTRUCTOR INFORMATION

*Instructor:*
Email:
*Phone*:
*Office Hours:*

TOC

## COURSE DESCRIPTION (CATALOG)

**ISSC642 – Intrusion Detection & Incident Handling**
This course examines the tenets of Intrusion Detection, Intrusion Prevention, and Incident Handling. Intrusion Detection focuses on the methods to detect attempts (attacks or intrusions) to compromise the confidentiality, integrity or availability of an information system. Also included is an analysis of the principles and practices of intrusion detection, intrusion prevention, and incident handling; network-based, host-based, and hybrid intrusion detection; identifying attack patterns; deployment of resources and responses to handle the incident, surveillance, damage assessment, risk assessment, data forensics, data mining, attack tracing, system recovery, and continuity of operation.

TOC

## COURSE SCOPE

At the end of this course, you will have a firm foundation of the field of information security. Both the technical aspects of information security, as well as security management issues will be an integral part of this course as it applies to criminal justice, political science, information systems and accounting/business systems. Ongoing

changes to the field of information security will be introduced and reviewed during this semester within Forum Posting and writing assignments.

TOC

## COURSE OBJECTIVES

After you have completed this course, you should be able to:

1. Examine the principles of intrusion detection and intrusion prevention.
2. Evaluate the principles of incident handling & reporting.
3. Compare and contrast network-based and host-based intrusion detection and intrusion protection systems.
4. Assess the various detection and prevention tools, technology, and techniques.
5. Explain the methods and techniques for recognizing and profiling attack patterns.
6. Assess the application of data mining and artificial intelligence techniques in intrusion detection and prevention.
7. Develop and incident response plan that incorporates attack tracing, evidence collection, and evidence analysis.
8. Evaluate an intrusion detection system or intrusion prevention system.

TOC

## COURSE MATERIALS

**Required Text**

The Tao of Network Security Monitoring: Beyond Intrusion Detection, by Richard Bejtlich. Publisher: Addison-Wesley Professional; 1 edition (July 22, 2004), ISBN-10: 0321246772.

Handbook for Computer Security Incident Response Teams (CSIRTs) Moira J. West-Brown. Publisher: Carnegie-Mellon University, 2nd edition (April 2003)
www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

US-CERT: United States Computer Emergency Readiness Team (nd)
www.us-cert.gov/federal/

Information Security Fundamentals. Author Peltier, Thomas R. / Peltier, Justin / Blackley, John A. CRC Press I, LLC. - this text will be required throughout the ISSC program, only 1 purchase is required.

**Software Requirements**

1. Microsoft Office Word
2. Internet browser
3. Adobe Acrobat Reader (Click here for free download)
4. Traffic monitor utilities (available from the Cnet/Zdnet software archives, etc.)

TOC

## COURSE DELIVERY METHOD

This course delivered via distance learning will enable students to complete academic work in a flexible manner, completely online. Course materials and access to an online learning management system will be made available to each student. **Online assignments are due by the Friday or Sunday of each week** and include Forum questions (accomplished in groups through a threaded Forum), examinations and quizzes (graded electronically), and individual assignments (submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

TOC.

## EVALUATION PROCEDURES

For the purposes of this course, a "**week**" is defined as the time period between Monday–Sunday, for all weeks 1 to 8. The **first week** begins on the first day of the semester and ends on midnight the following Sunday.

**PHONE CALLS:** Contact between students and faculty can occur in a number of ways: phone, fax, and electronic communications (Internet) are three examples. Students are expected to maintain routine contact with faculty throughout the course. And while the number of these may vary according to the specific course and individual student need, the University requires at least four contacts during the semester. Depending on the course, the professor may require these contacts to occur by phone. While these contacts will not be graded (unless indicated below) students should be aware that they count toward the total of required course exercises. Because of the asynchronous nature of the class, EMAIL CONTACT IS ALWAYS ACCEPTABLE!

**EMAILS: When you contact me via email, please ensure you put the title of the course (ISSC642) and the current session you are in in the subject line.** This will help me align your email within the right course so I can quickly address any questions you may have, or resolve any problems that may come up.

**EXAMINATION POLICIES AND PROCEDURES**
Quizzes are required in this course. These quizzes are not proctored. You have the quizzes in your syllabus. The grading criteria given in the student course guide will apply to the quizzes.

**Grades in this course are based on the following:**

1) **Forum Postings**: I will be posting Forum topics related to Information Security throughout the session. These postings will be directly tied to our assignments section for grading. Forum items will be posted within the Forum area of the classroom. Your responses will clearly show whether you are up to date on your readings, so be sure to keep up with course work and respond based upon same. Opinions are always welcome… however, postings providing only opinions will be graded accordingly. Your grades for Forum postings are available throughout the semester as they are graded throughout the week. Please ensure you understand the Rubric grading matrix at the end of this syllabus to guide your response and posting. I will be using this matrix to assign grades for your Forum postings.
2) **Quizes:** Worth 20% of your final grade. Detailed information and the due date for this exam are listed in your course outline. Quizzes are listed in the appropriate week of your syllabus.
3) **Idea Paper:** There will be one individual idea/concept paper throughout the session. The content for the project paper is listed under the Week 4 of your syllabus.
4) **Research Paper:** There will be one individual project paper throughout the session. The content for the project paper is listed under the Week 7 of your syllabus.
5) **Reflections Paper:** There will be one individual reflections paper throughout the session. The content for the project paper is listed under the Week 8 of your syllabus.

| GRADED EVENTS | | % OF FINAL GRADE |
|---|---|---|
| Forum Postings | Week 1 (3%), Weeks 2-7 (2% each) | 30 % |
| Tests | Quiz #1 | 15 % |
| | Quiz #2 | 15 % |
| Papers | Idea Paper | 10 % |
| | Research Paper | 20 % |
| | Reflections Paper | 10 % |
| **Total** | | **100 %** |

**Grading Scale**

Please see the **student handbook** to reference the **University's grading scale**.

## COURSE OUTLINE

TOC

| WEEK | DATES | LESSON SUBJECT | ASSIGNMENT – (*Graded) |
|---|---|---|---|
| 1 | Monday to Sunday of Week 1 | Introduction to Intrusion Detection & Incident Handling. | Course Begins<br>Required Contact Info to Professor<br>DoD Dir 8570.1<br>*Forum: Intro. & DoD 8570.1 |
| 2 | Monday to Sunday of Week 2 | Deployment considerations, Reference Intrusion Model, Full content data. | Chapters 1, 2,3, 4, & 5<br>* Forum: Network Security Monitoring Products |
| 3 | Monday to Sunday of Week 3 | Data analysis, Session data, Statistical data | Chapters 6, 7, 8<br>* Forum: Network Security Monitoring Products cont. |
| 4 | Monday to Sunday of Week 4 | Alert data<br>Midterm Exam | Chapters 9 & 10<br>* Forum: Network Security Monitoring Products cont.<br>*Quiz #1 Due (Ch 1 to 8)<br>*Idea paper due |
| 5 | Monday to Sunday of Week 5 | Best practices, Case studies for Managers, Analyst training. | Chapters 11, 12, & 13<br>* Forum: Network Security Monitoring Processes |
| 6 | Monday to Sunday of Week 6 | Discovering DNS, Session data, Examining Packets. | Chapters 14, 15, & 16<br>* Forum: DNS Concepts. |
| 7 | Monday to Sunday of Week 7 | Tools & Tactics | Chapters 17 & 18<br>* Forum: Intruder vs. Network Security Monitoring & Incident Response<br>*Research Paper Due |
| 8 | Monday to Sunday of Week 8 | Final Exam | Reading Week<br>*Quiz #2 Due (Ch 9 to 18)<br>*Reflections Paper Due |

**Course Outline – Overview**

**Course Deadlines/Milestones**

- **Participation in Forums is required for Week 1 through Week 7.**
- **End of Second Week: Chapters 1-5 completed.**
- **End of Fourth Week: Chapter 6-10 completed, and Idea paper and Midterm Exam due.**
- **End of Sixth Week: Chapters 11-16 completed.**
- **End of Seventh Week: Chapters 17-18 completed and Research Paper due**
- **Eighth Week: Reflections paper and Final Exam due.**

## Policies

Please see the **student handbook** to reference all University policies. Quick links to frequently asked question about policies are listed below.

**Drop/Withdrawal Policy**
**Plagiarism Policy**
**Extension Process and Policy**

**WRITING EXPECTATIONS**
All written submissions should be submitted in a font and page set-up that is readable and neat. It is recommended that students try to adhere to a consistent format, which is described below.

- Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
- Arial 11 or 12-point font or Times New Roman styles.
- Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations and online submission variances.

**CITATION AND REFERENCE STYLE**
Assignments completed in a narrative essay or composition format must follow APA guidelines. This course will require students to use the citation and reference style established by the American Psychological Association (APA), in which case students should follow the guidelines set forth in *Publication Manual of the American Psychological Association* (6th ed.). (2010). Washington, D.C.: American Psychological Association.

**LATE ASSIGNMENTS**
Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals I understand you must manage competing demands on your time. Should you need additional time to complete an assignment please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade.

**DISCLAIMER STATEMENT**
Course content may vary from the outline to meet the needs of this particular group.

## Academic Services

**ONLINE LIBRARY RESEARCH CENTER & LEARNING RESOURCES**
The Online Library Resource Center is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Center provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to orc@apus.edu.

- ***Charles Town Library and Inter Library Loan:*** The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- ***Electronic Books:*** You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- ***Electronic Journals:*** The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.
- ***Turnitin.com:*** **Turnitin.com** is a tool to improve student research skills that also detect plagiarism. Turnitin.com provides resources on developing topics and assignments that encourage and guide students in producing papers that are intellectually honest, original in thought, and clear in expression. This tool helps ensure a culture of adherence to the University's standards for intellectual honesty. Turnitin.com also reviews students' papers for matches with Internet materials and with thousands of student papers in its database, and returns an Originality Report to instructors and/or students.
- ***Smarthinking:*** Students have access to 10 free hours of tutoring service per year through Smarthinking. Tutoring is available in the following subjects: math (basic math through advanced calculus), science (biology, chemistry, and physics), **accounting, statistics, economics,**

**Spanish,** writing, grammar, and more. Additional information is located in the Online Research Center. From the ORC home page, click on either the "Writing Center" or "Tutoring Center" and then click "Smarthinking." All login information is available.

**TOC**

## Webliography

**ISSC642 – Intrusion Detection and Incident Handling Article References***

The Tao of Network Security Monitoring: Beyond Intrusion Detection, by Richard Bejtlich. Publisher: Addison-Wesley Professional; 1 edition (July 22, 2004), ISBN-10: 0321246772.

Handbook for Computer Security Incident Response Teams (CSIRTs) Moira J. West-Brown. Publisher: Carnegie-Mellon University, 2nd edition (April 2003) www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

US-CERT: United States Computer Emergency Readiness Team (nd). www.us-cert.gov/federal/

**Course Outline – Week by Week**

| **Week 1 - Introduction to Intrusion Detection & Incident Handling** | **TOC** |
|---|---|

**Topic:** The opening chapter's establish the foundation for understanding the broader field of intrusion detection and incident handling. This is accomplished by explaining essential concepts, and reviewing the origins of the field and its role within the field of information security.

**Learning Objectives:** By the end of this week, you should be able to:

- Understand the definition of intrusion detection and incident handling.
- Comprehend the computer/network security process and the phases of the security process cycle.
- Outline the characteristics of the intruder.
- Understand the key terms and critical concepts of intrusion detection and incident handling as presented in the chapters.
- Understand what is network security monitoring.

**Assignments:**

- **Readings:** DoD Dir 8570.1
  DoD CIO. (2010). *DoD 8570.01-M, Information Assurance Workforce Improvement Program*.
- **Send your contact info via email to professor by Saturday** (Name, email, phone numbers, best time to call, city and state/area currently residing, time zone)
- **Become familiar with AMU's on line classroom**
- **Discussion Forum:**
  1. Introduce yourself in the Discussion Board posting (NLT 260 words).
     - 1st paragraph: Your bio, including your past, current and future career, education, and certification plans. You can include classes, year in school, major, your location and time zone, government/military status, your personal interests, and any other information you may want to share with the rest of the class.
     - 2nd paragraph: How will (or will not) DOD directive 8570.1 (http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf) affect your career/education/certification plans?
     - 3rd paragraph: Please post at least three facts; two (2) TRUE and one (1) NOT TRUE, then try to guess your classmates "not true" statement. ;)
     - Due by Friday of Week 1, 11:59 PM EST.
  2. Reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 1 11:59 PM EST.

**Week 2 - Network Security Monitoring Products**
TOC

**Topic**: Chapters 3, 4, & 5 examines network security monitoring products. They examine deployment considerations, threat models and monitoring zones, accessing traffic in each zone, wireless monitoring, sensor architecture, sensor management and then moves on to address network security monitoring products, the reference intrusion model, full content data, Libpcap, Tcpdump, Tethereal, Snort as packet logger, finding specific parts of packets with Tcpdump, Tethereal, Snort, and Ethereal and concludes with a note on commercial full content collection options.

**Learning Objectives:** By the end of this week, you should be able to:

- Understand deployment considerations, threat models and monitoring zones.
- Understand wireless monitoring, sensor architecture, and sensor management.
- Familiar with network security monitoring products.
- Familiar with the reference intrusion model.
- Differentiate between Libpcap, Tcpdump, Tethereal, and Snort as packet logger.
- Finding specific parts of packets with Tcpdump, Tethereal, Snort, and Ethereal.
- Understand commercial full content collection options.

**Assignments:**

- **Readings:** Chapter 1 & 2 pages 3 – 44, Chapter 3, 4, & 5, pages 45 – 172.
- **Exercises:** Chapter 3: capture hub/network traffic, Chapter 4: TCP/IP utilities, Chapter 5: packet capture & analysis. Do not turn in.
  1. **Forum – Part 1 Case study:**
     - Look at the second paragraph on page 43. Reflect on why or why not you agree with the four listed statements. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. (due by Friday of Week 2 11:59 PM EST)
     - Rubric for this (approx. 100 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
     - Reply to at least two or more class members on the case study. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response (due by Sunday of Week 2 11:59 PM EST)
  2. **Forum Part 2– Deployment Considerations:**
     - **Describe the deployment considerations** involved with using network security monitoring products to obtain full content data. Due by Friday of Week 2 11:59 PM EST.
       Rubric for this (approx. 100 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
     - After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 2 11:59 PM EST (0.5% of grade).

**Week 3 - Network Security Monitoring Products cont.** TOC

**Topic**: Chapters 6, 7, & 8 continue to examine network security monitoring products for Additional Data Analysis purposes. Specifically, Editcap and Mergecap, Tcpslice, Tcpreplay, Tcpflow, Ngrep, IPsumdump, Etherape, Netdude, and P0f, Chapter 7 addresses Session Data, Forms of Session Data, Cisco's NetFlow, Fprobe, Ng_netflow, Flow-tools, sFlow and sFlow Toolkit, Argus, and Tcptrace. Chapter 8 addresses Statistical Data, What Is Statistical Data, Cisco Accounting, Ipcad, Ifstat, Bmon, Trafshow. Ttt, Tcpdstat, and MRTG.

**Learning Objectives:** By the end of this week, you should be able to:

- Understand Additional Data Analysis.
- Understand Session Data.
- Describe forms of session data.
- Describe the tools used to collect session data.
- Define Statistical Data.
- Grasp the fundamental aspects of what is Statistical Data.
- Describe the tools used to collect statistical data.

**Assignments:**

- **Readings:** Chapters 6, 7 & 8, pages 173-283.
- **Exercises:** Chapter 6: packet capture & analysis, Chapter 7: session data capture, Chapter 8 statistics tools. Do not turn in.
- **Forum – Additional Data Analysis, Session Data, Statistical Data:**
  1. Distinguish between full content data (including collection tools), session data (including collection tools) and statistical data (including collection tools). Due by Friday of Week 3 11:59 PM EST.
     - Rubric for this (approx. 260 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 3 11:59 PM EST.

**Week 4 - Mid Term exam / Security Network Security Monitoring Products cont.** TOC

**Topic:** Quiz #1 (Complete Quiz #1)

**Learning Objectives:** You should be able to complete the Midterm Examination by the end of this week. Also, chapters 9 & 10 cover:

- Alert data.
- Alert data tools (Bro, Prelude, Sguil).
- Making decisions with network security monitoring alert data.

**Assignments:**

- **Readings:** Chapter 9 & 10, pages 285-344.
- **Midterm Exam** – on Chapters 1-8. Due by Sunday of Week 4 11:59 PM EST.
- **Idea Paper** (see details below). Due by Sunday of Week 4 11:59 PM EST.
- **Forum – Alert data tools:**
  1. Distinguish between alert data (including generation tools) and previously covered NSM monitoring (including collection tools). Due by Friday of Week 4 11:59 PM EST
     - Rubric for this (approx. 260 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 4 11:59 PM EST.

**Idea Paper:** (Due by Sunday of Week 4, 11:59 PM EST)

1. Submit an idea paper IAW APA format on an approved topic (see pre-approved topics below). Paper organization will include:
   - Introduction.
   - Problem Statement.
   - Relevance and Significance.
   - References (at least five).
2. Pre-approved topics:
   - End user security issues.
   - Government vs. commercial organization security issues.
   - Intrusion detection
   - Incident handling
   - Data collections tools (hardware & software)
   - ID&IH Management and Legal Issues

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must by at least 3 pages double-spaced, 1" margin all around, black12 point fonts (Times New Roman, Arial, or Courier) with correct citations of all utilized references/sources, not counting any pictures, graphics, etc. A minimum of 5 references are needed. The paper will be submitted to Turnitin to check for proper citation attribution.

**Week 5 - Network Security Monitoring Processes**
TOC

**Topic**: Chapters 11, 12, & 13 examine network security monitoring processes & monitoring people. Chapter 11 specifically addresses best practices, assessment, protection, and detection & response. Chapter 12 provides case studies on monitoring, monitoring providers, and monitoring solutions. Chapter 13 introduces the concept of analyst training program (weapons and tactics, telecommunications, system administration, scripting and programming, management and policy, training in action, and periodicals and web sites).

**Learning Objectives:** By the end of this week, you should be able to:

- Identify and describe network security monitoring processes.
- Identify and describe the kills required for network security monitoring.
- List and best practices, assessment, protection, and detection & response.
- Discuss various approaches to monitoring, monitoring providers, and monitoring solutions.
- Understand the process of an analyst training program,
- Describe the components of an analyst training program, including weapons and tactics, telecommunications, system administration, scripting and programming, management and policy, training in action, and periodicals and web sites.

**Assignments:**

- **Readings:** Chapters 11, 12 & 13, pages 347-431.
- **Exercises:** Chapter 9 & 10: alert data tools, Chapter 11: packet analysis. Do not turn in.
- **Forum – Network Security Monitoring Processes:**
    1. Please look at the killing with keyboards file then answer the following questions in the context of the best practice concepts covered in chapter 11 and the security professional proficiencies covered in chapter 13. Identify what is at risk here, 5 possible threats and 5 vulnerabilities in this scenario. Discuss measures that could be taken to reduce the risks (due by Friday of Week 5, 11:59 PM EST).
        - Rubric for this (approx. 260 word) discussion assignment
            - Topic coverage/synthesis of concept
            - Reflection/application from personal experience
            - Correct APA Citations including citing the textbook
            - Writing Standards
    2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. (due by Sunday of Week 5 11:59 PM EST.

**Week 6 – DNS Concepts**
TOC

**Topic**: Chapters 14, 15, & 16 examine DNS concepts. Chapter 14 specifically addresses normal, suspicious and malicious Port 53 traffic. Chapter 15 provides case studies on harnessing the power of session data (session data from the wireless segment, session data from the DMZ segment, session data from the VLANs, and session data from the external segment). Chapter 16 introduces the concept of OSI model layer 3 and 4 packet header identification, truncated TCP options, SCAN FIN, and chained covert channels.

**Learning Objectives:** By the end of this week, you should be able to:

- Understand DNS.
- Identify normal, suspicious, and malicious Port 53 traffic.
- Describe session data from the wireless segment.
- Describe session data from the DMZ segment.
- Describe session data from the VLANs.
- Describe session data from the external segment.
- List the OSI model layers.
- Identify OSI model layer 3 and 4 packet header identification.
- Identify truncated TCP options, SCAN FIN, and chained covert channels.

**Assignments:**

- **Readings:** Chapters 14, 15, and 16, pages 433-518.
- **Exercises:** Chapter 14: DNS packet analysis, Chapter 15: session data analysis, Chapter 16 packet header analysis. Do not turn in.
- **Forum - DNS:**
  1. Network activity can be classified as normal, suspicious, or malicious. How is network activity differentiated? Provide examples. Due by Friday of Week 6 11:59 PM EST
     - Rubric for this (approx. 260 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. Due by Sunday of Week 6 11:59 PM EST.

**Week 7 - Intruder vs. Network Security Monitoring**
TOC

**Topic**: Chapters 17 & 18 examine intruders vs. network security monitoring concepts. Chapter 17 specifically addresses tools for attacking network security monitoring (Packit, IP Sorcery, Fragroute, LFT, Xprobe2, Cisco IOS Denial of Service, Solaris Sadmin Exploitation Attempt, Microsoft RPC Exploitation). Chapter 18 introduces some tactics for attacking network security monitoring (promote anonymity, evade detection, appear normal, degrade or deny collection, and self-inflicted problems in NSM). Further, the Handbook for Computer Security Incident Response Teams addresses the specifics of incidence response teams.

**Learning Objectives:** By the end of this week, you should be able to:

- Understand examine intruders vs. network security monitoring concepts.
- Identify tactics for attacking network security monitoring.
- Understand the special security precautions that must be taken when contracting non-employees.
- Understand the process of incidence response.
- Identify the specifics of incidence response teams.

**Assignments:**

- **Readings:** Chapters 17 and 18, pages 519-649, the Handbook for Computer Security Incident Response Teams pages 9-135.
- **Exercises:** Chapter 17: hacking tools. Do not turn in.
- **Research Paper** (see details below). Due by Sunday of Week 7 11:59 EST (15% of grade).
- **Forum –** Intruder vs. Network Security Monitoring & Incident Response**:**
  1. Discuss the tools and tactics for attacking network security monitoring and the considerations involved in incident response. Due by Friday of Week 7 11:59 PM EST.
     - Rubric for this (approx. 260 word) discussion assignment
       - Topic coverage/synthesis of concept
       - Reflection/application from personal experience
       - Correct APA Citations including citing the textbook
       - Writing Standards
  2. After responding, reply to at least two or more class members. Please make sure you keep your postings and responses in the thread of the original response, and do not exit to provide a separate response. (due by Sunday of Week 7 11:59 PM EST (0.5% of grade).

**Research Paper:** Due by Sunday of Week 7, 11:59 PM EST (15% of grade).

1. Submit a research paper based on your week 4 Idea Paper. Paper organization will include:
   - Introduction
     - Clearly define the problem or issue.
     - Starts out broad and becomes more and more specific.
   - Body
     - Present the relevant literature and ideas.
     - Identify relations, contradictions, gaps, and inconsistencies in the literature.
     - Possible solutions to any problem(s) identified.
   - Conclusion
   - References (at least ten).

   You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must by at least 10 pages double-spaced, 1" margin all around, black12 point fonts (Times New Roman, Arial, or Courier) with correct citations of all utilized references/sources, not counting any pictures, graphics, etc. A minimum of 10 references are needed. The paper may be submitted to Turnitin to check for proper citation attribution.
   Some sources of peer reviewed articles are:
   1. ACM digital library: http://portal.acm.org/dl.cfm

2. Google Scholar : http://scholar.google.com/
3. IEEE digital library: http://www.computer.org/portal/web/csdl/home

**Week 8 - Final Exam**
**TOC**

**Topic: Course Conclusion. Complete Quiz #2.**

**Learning Objectives: Complete the paper & Quiz #2 before the end of the course date (Sunday of Week 8 11:59 PM EST)**

**Assignment:**

- **Readings:** NONE – work on your final exam and reflection paper.
- **Quiz #2 – on Chapters 1 – 18. Due NLT Sunday of Week 8 11:59 PM EST – no exceptions)**
- **Reflections Paper** (see details below). Due by Sunday of Week 8 11:59 PM EST.

**Reflections Paper:** Due by Sunday of Week 8, 11:59 PM EST (10% of grade).

1. Submit a reflections paper on your ISS642 readings, exercises and weekly Forum posts. The paper should include:
   - A brief summary of your course experience.
   - Identify and explain relevant conceptual material (theories, concepts) from the course.
   - How the course concept/idea/theory may or will change your future actions/activities.

   You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must by at least 4 pages double-spaced, 1" margin all around, black 12 point fonts (Times New Roman, Arial, or Courier) with correct citations of all utilized references/sources, not counting any pictures, graphics, etc. APA format applies. The paper may be submitted to Turnitin to check for proper citation attribution.

## *DAVID ANDERSSON*

**Your Instructor's Bio:** Doctor Andersson has an Ed.D. (Technology Management), an Ed.S. (Computing Technology), an MS (Information Technology), and an MA (Public Administration). He has the MCT, MCSE, CCNA, CCWLANSS, Master CIW Administrator, CIW Security Analyst, CIW Security Professional, CompTIA as well as other technical certifications and currently serves as a consultant for e-commerce and business IT security for public and private organizations such as Worth Ltd. and as an Assistant Professor of CIS.

Doctor Andersson has worked as a training advisor for the New Military Technology System Special Projects Group for Raytheon, a Senior Systems Engineer for Allstate Insurance, and as a Lieutenant Colonel, Operations and Security, US Army - Kuwait, and the 2nd ACR Border Operations Officer on the East-West German border. In 1978-79 he represented the USA in the Canadian Army Trophy International Competition and in 1986 commanded the unit ranked 2nd in the USA for Operations Excellence. He is the current leader of the US-based Bronze Star Association hosted on Linkedin.

His publications include:

Andersson, D. (2009) Chapter 7 OSPF, Cisco CCNA/CCENT Exam 640-802, 640-822, 640-816 Preparation Kit. Liu, D. Editor. Rockland, MA. Syngress Publishing.

Andersson, D. (2009). Information Technology Industry Certification's Impact on Undergraduate Student Perception of Instructor Effectiveness. UMI Dissertation Publishing Group, Volume 7005A. Publication No. 3358241.

Andersson, D. and Reimers, K. (2009). IT Certifications - Does It Matter If Your IT Professors Are Certified? Certification Magazine. Chicago, IL. MediaTec Publishing (pending).

Andersson, D. and Reimers, K. (2010). Academia and IT Certifications - Program Administration Trends and Implications. The Open Education Journal, Oak Park, IL, Benham Science Publishing (pending).

Andersson, D. and Reimers, K. (2010). CIS and IT Certifications - Education Program Trends and Implications. i-Manager's Journal of Educational Technology, Nagercoli, India, i-Manager Publishing (pending).

Doctor Andersson teaching experience includes information technology topics, network security and digital forensics. His awards include the College Senate Committee for Distance Learning Program Development - 2003, Raytheon Performance Award, Allstate NBS Performance Award, Kuwait Liberation Medal, Southwest Asia Service Ribbon (3 Campaign Stars), Bronze Star, and Meritorious Service Medal. His hobbies include sailing, running, Clumber Spaniels, military history and he has a wife and two children.

He is an active and continued member of IEEE and ACM.

**ISSC642 – Intrusion Detection and Incident Handling Article References*** TOC

The Tao of Network Security Monitoring: Beyond Intrusion Detection, by Richard Bejtlich. Publisher: Addison-Wesley Professional; 1 edition (July 22, 2004), ISBN-10: 0321246772.

Handbook for Computer Security Incident Response Teams (CSIRTs) Moira J. West-Brown. Publisher: Carnegie-Mellon University, 2nd edition (April 2003) www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf

US-CERT: United States Computer Emergency Readiness Team (nd). www.us-cert.gov/federal/

**Rubrics**

**Rubric for Learner Post (Assign point value in Grade Builder)**

| Synthesis of concepts | Applications or reflections of personal experience | Clear citations | Writing standards | Timeliness |
|---|---|---|---|---|
| The response refers to course materials and shows a clear understanding of main ideas and concepts. There are no irrelevant comments and the information is on point. Ideas are clearly and properly organized. | The response provides personal examples that tie in with the course material being discussed. Reflection is evident and clearly ties in with the material presented. Insight was provided to some concept. | The response made proper reference to the course text or to other materials that were referenced or referred to in the Forum. Opinions were also included and were valid. | The writing is grammatically correct, clear and concise. The response is well formulated and easy to read and understand. Correct terminology was used when needed. | The posting was “not” submitted on time. |
| 60% | 20% | 10% | 10% | 10% (deduction) |

**Rubric for Response to another Learner**

| Synthesis of concepts | Writing standards | Timeliness |
|---|---|---|
| The other learner’s ideas, questions, concerns were addressed. The response referenced reading or lecture materials when needed. The response addressed the learner’s feelings if needed. There were no irrelevant or off-point comments. The posting reflects a clear understanding of the other learner’s ideas. | The writing is grammatically correct, clear and concise. The response is well formulated and easy to read and understand. Correct terminology was used when needed. | The posting was “not” submitted on time. |
| 80% | 20% | 10% (deduction) |

**Appendix A – Grading Rubric**

All written assignments will be assessed according to this rubric. Note that a score of 0 may be assigned in any category where your work does not meet the criteria for the beginning level.

| **APUS Assignment Rubric Graduate Level 600+** | **EXEMPLARY LEVEL 4** | **ACCOMPLISHED LEVEL 3** | **DEVELOPING LEVEL 2** | **BEGINNNIG LEVEL 1** | |
|---|---|---|---|---|---|
| FOCUS/THESIS | Student exhibits a defined and clear understanding of the assignment. Thesis is clearly defined and well constructed to help guide the reader throughout the assignment. Student builds upon the thesis of the assignment with well-documented and exceptional supporting facts, figures, and/or statements. | Establishes a good comprehension of topic and in the building of the thesis. Student demonstrates an effective presentation of thesis, with most support statements helping to support the key focus of assignment. | Student exhibits a basic understanding of the intended assignment, but the thesis is not fully supported throughout the assignment. While thesis helps to guide the development of the assignment, the reader may have some difficulty in seeing linkages between thoughts. While student has included a few supporting facts and statements, this has limited the quality of the assignment. | Exhibits a limited understanding of the assignment. Reader is unable to follow the logic used for the thesis and development of key themes. Introduction of thesis is not clearly evident, and reader must look deeper to discover the focus of the writer. Student's writing is weak in the inclusion of supporting facts or statements. | 10 |
| **CONTENT/SUBJECT KNOWLEDGE** | Student demonstrates proficient command of the subject matter in the assignment. Assignment shows an impressive level of depth of student's ability to relate course content to practical examples and applications. Student provides comprehensive analysis of details, facts, and concepts in a logical sequence. | Student exhibits above average usage of subject matter in assignment. Student provides above average ability in relating course content in examples given. Details and facts presented provide an adequate presentation of student's current level of subject matter knowledge. | The assignment reveals that the student has a general, fundamental understanding of the course material. Whereas, there are areas of some concerning in the linkages provided between facts and supporting statements. Student generally explains concepts, but only meets the minimum requirements in this area. | Student tries to explain some concepts, but overlooks critical details. Assignment appears vague or incomplete in various segments. Student presents concepts in isolation, and does not perceive to have a logical sequencing of ideas. | 20 |
| **CRITICAL THINKING** | Student demonstrates a | Student exhibits a good | Student takes a common, | Student demonstrates | 20 |

| | | | | | |
|---|---|---|---|---|---|
| **SKILLS** | higher-level of critical thinking necessary for 300-400 level work. Learner provides a strategic approach in presenting examples of problem solving or critical thinking, while drawing logical conclusions which are not immediately obvious. Student provides well-supported ideas and reflection with a variety of current and/or world views in the assignment. Student presents a genuine intellectual development of ideas throughout assignment. | command of critical thinking skills in the presentation of material and supporting statements. Assignment demonstrates the student's above average use of relating concepts by using a variety of factors. Overall, student provides adequate conclusions, with 2 or fewer errors. | conventional approach in guiding the reader through various linkages and connections presented in assignment. However, student presents a limited perspective on key concepts throughout assignment. Student appears to have problems applying information in a problem-solving manner. | beginning understanding of key concepts, but overlooks critical details. Learner is unable to apply information in a problem-solving fashion. Student presents confusing statements and facts in assignment. No evidence or little semblance of critical thinking skills. | |
| **ORGANIZATION OF IDEAS/FORMAT** | Student thoroughly understands and excels in explaining all major points. An original, unique, and/or imaginative approach to overall ideas, concepts, and findings is presented. Overall format of assignment includes an appropriate introduction (or abstract), well- developed paragraphs, and conclusion. Finished assignment demonstrates student's ability to plan and organize research in a logical sequence. Student uses at least of 5-7 references in assignment. | Student explains the majority of points and concepts in the assignment. Learner demonstrates a good skill level in formatting and organizing material in assignment. Student presents an above average level of preparedness, with a few formatting errors. Assignment contains less than 5 resources. | Learner applies some points and concepts incorrectly. Student uses a variety of formatting styles, with some inconsistencies throughout the paper. Assignment does not have a continuous pattern of logical sequencing. Student uses less than 3 sources or references. | Assignment reveals formatting errors and a lack of organization. Student presents an incomplete attempt to provide linkages or explanation of key terms. The lack of appropriate references or source materials demonstrates the student's need for additional help or training in this area. Student needs to review and revise the assignment. | 20 |
| **WRITING CONVENTIONS (GRAMMAR & MECHANICS)** | Student demonstrates an excellent command of grammar, as well as presents research in a clear | Student provides an effective display of good writing and grammar. Assignment reflects | Assignment reflects basic writing and grammar, but more than 5 errors. Key terms and concepts are | Topics, concepts, and ideas are not coherently discussed or expressed in | 20 |

| | | | | | |
|---|---|---|---|---|---|
| | and concise writing style. Presents a thorough, extensive understanding of word usage. Student excels in the selection and development of a well-planned research assignment. Assignment is error-free and reflects student's ability to prepare a high-quality academic assignment. | student's ability to select appropriate word usage and present an above average presentation of a given topic or issue. Assignment appears to be well written with no more than 3-5 errors. Student provides a final written product that covers the above-minimal requirements. | somewhat vague and not completely explained by student. Student uses a basic vocabulary in assignment. Student's writing ability is average, but demonstrates a basic understanding of the subject matter. | assignments. Student's writing style is weak and needs improvement, along with numerous proofreading errors. Assignment lacks clarity, consistency, and correctness. Student needs to review and revise assignment. | |
| **USE OF COMPUTER TECHNOLOGY/ APPLICATIONS** | Student provides a high-caliber, formatted assignment. Learner exhibits excellent use of computer technology in the development of assignment. Quality and appropriateness of stated references demonstrate the student's ability to use technology to conduct applicable research. Given assignment includes appropriate word processing, spreadsheet and/or other computer applications as part of the final product. | Assignment presents an above-average use of formatting skills, with less than 3 errors. Students has a good command of computer applications to format information and/or figures in an appropriate format. Student uses at least two types of computer applications to produce a quality assignment. | Student demonstrates a basic knowledge of computer applications. Appearance of final assignment demonstrates the student's limited ability to format and present data. Resources used in assignment are limited. Student may need to obtain further help in the use of computer applications and Internet research. | Student needs to develop better formatting skills. The student may need to take additional training or obtain help from the Educator Help Desk while preparing an assignment. Research and resources presented in the assignment are limited. Student needs to expand research scope. The number of formatting errors is not acceptable. | 10 |
| TOTAL POINTS | | | | | 100 |