

FLORIDA STATE COLLEGE AT JACKSONVILLE

COLLEGE CREDIT COURSE OUTLINE

COURSE NUMBER: CET 2662

COURSE TITLE: Techniques of Computer Hacking and Incident Handling

PREREQUISITE(S): CET 2687 or CTS 1120

COREQUISITE(S): None

CREDIT HOURS: 4

CONTACT HOURS/WEEK: 4

CONTACT HOUR BREAKDOWN:

Lecture/Discussion: 3

Laboratory: 1

Other _____:

FACULTY WORKLOAD POINTS: 4

STANDARDIZED CLASS SIZE ALLOCATION: 24

CATALOG COURSE DESCRIPTION:

This course provides the fundamental knowledge necessary for a student to become proficient in understanding the techniques of computer hacking and how to respond to hacking related incidents. In addition, the focus of the course is designed to prepare the student to respond to Zero-day exploits where vendor services such as virus scanning and intrusion detection are rendered useless. The course will cover the origin and history of hacking examining in detail the techniques used by early hackers. The course will then shift to today's vulnerabilities and concerns in an attempt to predict and prepare the student for tomorrow's exploits. Prerequisite is CET2687 (Security+) or CNT1400 (Fundamentals of Information Security).

SUGGESTED TEXT(S): Hack I.T. (Klevinsky, Laliberte, Gupta) Addison-Wesley (Current Edition)

IMPLEMENTATION DATE: Spring Term, 2008 (20082)

REVIEW OR MODIFICATION DATE: Spring Term, 2008 (20082)
Fall Term, 2008 (20091)

COURSE TOPICS	<u>CONTACT HOURS PER TOPIC</u>
I. Incident Handling	12
II. Windows Exploits	8
III. Virus Exploits	8
IV. Password Exploits	8
V. General Exploits	8
VI. Denial of Service Attacks	8
VII. Hands-on Tests	8
Total:	<u>60</u>

PROGRAM TITLE: IT Security

COURSE TITLE: Techniques of Computer Hacking and Incident Handling

CIP NUMBER: 1506120106 AS

LIST PERFORMANCE STANDARD ADDRESSED:

NUMBER(S): TITLES(S):

05.0 Demonstrate an understanding of network access control systems and methodology-The student will be able to:

- 05.10 Analyze methods of server attack, including brute force, denial of service, spoofing, spamming, sniffers, hackers, and crackers
- 05.11 Demonstrate an understanding of the different types of intrusions and the different methods of intrusion detection, including data extraction, sampling, recognition and traffic analysis
- 05.12 Monitor the network using various forms of intrusion detection resources to detect attacks
- 05.13 Investigate audit trails for signs of network intrusions
- 05.14 Perform penetration testing to find weaknesses in the access control systems.

06.0 Describe cryptography concepts, standards, and applications-The student will be able to:

- 06.01 Demonstrate an understanding of the encryption/decryption process.
- 06.02 Demonstrate an understanding of the basic functions involved in key management including creation, distribution, verification, revocation, destruction, storage, recovery, and life span of keys.
- 06.03 Utilize various forms of cryptography, digital certificates, and digital signatures to achieve confidentiality, integrity, authentication, and non-repudiation in an enterprise data communications network.
- 06.04 Discuss the creation and use of digital certificates and digital signatures to provide authentication of users and verification of data integrity in network communications.
- 06.05 Employ cryptographic algorithms such as DES, RSA, MD5 and DSA.
- 06.06 Identify the strengths and weaknesses of cryptographic algorithms and the effects of key length.
- 06.07 Implement current popular key distribution methods including manual, Kerberos™, and Internet Security Association and Key Management Protocol (ISAKMP).
- 06.08 Utilize application and network-based protocols such as Secure Socket Layer (SSL), Secure HyperText Transfer Protocol (SHTTP), and Internetworking Protocol Security (IPSEC).
- 06.09 Describe the use of hardware components such as smart cards and tokens.

07.0 Perform telecommunications and network security activities - The student will be able to:

- 07.01 Utilize protocol layering models such as the Open Systems Interconnection (OSI) model in analyzing network security threats.
- 07.02 Evaluate the security implications involved with the various physical media types such as fiber optics, twisted pair, and wireless communications.
- 07.03 Describe security concerns with using certain network topologies such as star, bus, mesh, and ring.
- 07.05 Employ network monitors and packet sniffers to identify security threats.

LIST PERFORMANCE STANDARD ADDRESSED:

NUMBER(S): TITLES(S):

07.07 Discuss the security vulnerabilities of the Transmission Control Protocol/Internetworking Protocol (TCP/IP) protocol stack.

10.0 Demonstrate an understanding of e-commerce-The student will be able to:

10.06 Discuss the steps necessary to maintain transaction integrity.

13.0 Design and implement physical security measures-The student will be able to:

13.01 Identify the physical threats to an enterprise's resources that include the employees, facilities, data, equipment, support systems, media, and supplies they utilize.

13.02 Diagnose an enterprise's physical vulnerabilities to threats from natural disasters such as fire, flooding, and power loss.

13.03 Specify possible countermeasures to physically protect an enterprise's resources and sensitive information.

13.04 Develop a list of physical facility requirements to secure the premises.

13.05 Evaluate the applicability of technical controls such as smart cards, access logs, and intrusion detection systems.

14.0 Perform operations and security management practices-The student will be able to:

14.08 Compare the advantages and disadvantages of internal versus external audits.

14.10 Identify different types of monitoring including event, hardware, and illegal software.

14.13 Perform penetration testing activities including sniffing, eavesdropping, dumpster diving, and social engineering.

14.14 Understand principles of risk management and asset valuation.

15.0 Employ applications and systems development security techniques- The student will be able to:

15.06 Analyze local environment application issues including viruses, Trojan horses, logic bombs and worms.

15.09 Compare different forms of data/information storage including primary, secondary, real, virtual, random, volatile, and sequential.

15.11 Understand the difference between supervisory and user modes of operation.

15.12 Identify various levels of application integrity including network, operating system, database, and file level integrity.

15.13 Define the various types of computer viruses and malicious code and the roles that hackers, crackers, phreaks, and virus writers play in developing and utilizing malicious code.

LIST PERFORMANCE STANDARD ADDRESSED: (Continued)

NUMBER(S): TITLES(S):

- 17.0 Describe ethical issues, pertinent laws, and how to conduct investigations-The student will be able to:
- 17.01 Understand the major categories and types of laws as to how they relate to E-commerce, including criminal law, civil law and administrative law.
 - 17.03 Describe abnormal and suspicious activity as it relates to database and e-commerce security.
 - 17.04 Analyze potential data security threats such as fraud or collusion.
 - 17.06 Identify the major categories of computer crime and attacks, including military, business, financial, terrorist, grudge and "fun" attacks.
 - 17.08 Discuss major ethical and legal issues related to Internet use.
- 18.0 Perform general organizational computing workplace competencies-_The student will be able to:
- 18.01 Follow oral and written instructions.
 - 18.05 Interpret appropriate information from graphics, maps, or signs.
 - 18.06 Demonstrate self-motivation and responsibility to complete an assigned task.
 - 18.08 Identify and discuss issues contained within professional codes of conduct.
 - 18.09 Identify and discuss intellectual property rights and licensing issues.
 - 18.10 Identify potential sources of employee/employer or employee/employee conflict and discuss possible approaches to resolve such disagreements.
- 20.0 Perform documentation and technical reference activities-The student will be able to:
- 20.01 Use technical vocabulary appropriately
 - 20.02 Locate information in printed and online technical references



NOTE: Use either the Tab key or mouse click to move from field to field. The box will expand to accommodate your entry.

Section 1	
COURSE PREFIX AND NUMBER: <u>CET 2662</u>	SEMESTER CREDIT HOURS (CC): <u>4</u> CONTACT HOURS (NCC): _____
COURSE TITLE: <u>Techniques of Computer Hacking and Incident Handling</u>	

Section 2
TYPE OF COURSE: (Click on the box to check all that apply)

<input type="checkbox"/> AA Elective	<input checked="" type="checkbox"/> AS Required Professional Course	<input type="checkbox"/> College Prep
<input type="checkbox"/> AS Professional Elective	<input type="checkbox"/> AAS Required Professional Course	<input type="checkbox"/> Technical Certificate
<input type="checkbox"/> Other _____	<input type="checkbox"/> PSAV	<input type="checkbox"/> Apprenticeship
<input type="checkbox"/> General Education: (For General Education courses, you must also complete Section 3 and Section 7)		

Section 3 (If applicable)
INDICATE BELOW THE DISCIPLINE AREA FOR GENERAL EDUCATION COURSES:

<input type="checkbox"/> Communications	<input type="checkbox"/> Social & Behavioral Sciences	<input type="checkbox"/> Mathematics
<input type="checkbox"/> Natural Sciences	<input type="checkbox"/> Humanities	

Section 4
INTELLECTUAL COMPETENCIES:

<input checked="" type="checkbox"/> Reading	<input checked="" type="checkbox"/> Speaking	<input checked="" type="checkbox"/> Critical Analysis	<input checked="" type="checkbox"/> Quantitative Skills	<input type="checkbox"/> Scientific Method of Inquiry
<input checked="" type="checkbox"/> Writing	<input checked="" type="checkbox"/> Listening	<input type="checkbox"/> Information Literacy	<input type="checkbox"/> Ethical Judgment	<input checked="" type="checkbox"/> Working Collaboratively

Section 5	
LEARNING OUTCOMES	METHOD OF ASSESSMENT
• The student will be taught the principles of industry standard security penetration testing .	The course requires the student to perform penetration testing in a closed network laboratory environment. Using tools of the trade the student will evaluate the security of a network and computer facility.
• The student will learn to perform network analysis .	Each student will be required to install, configure, and utilize the network analysis tool Ethereal . They will be required to create and implement the proper filter for the specific capture or display function.
• The student will learn to evaluate the security of a computer facility .	Each student will be required to install, configure, and utilize security evaluation products including Scanners, Nmap, SuperScan 3&4.0, LanGurd, Nessus, and WHCC.
• The student will be taught to recognize the existence of a malware or spyware infection and to mitigate its effect.	Each student will be required to install, configure, and analyze the effects of Trojans Programs including Netbus, BO2k, and SubSeven.
• The student will be taught to understand the effects of a Distributed Denial of Service attack and mitigating methods for dealing with an attack.	Each student will be required to install, configure, launch, and analyze Denial of Service malware including Flooders, Nukers, and DoSers.
• The students will be taught to use Command Line Utilities from the DOS operating system to support their penetration testing.	Each student will be required to install, configure, and test Command Line Utilities from Sysinternals .com and other Open Systems software sources.
• The student will be taught to recognize the process used by malware authors to implement some of the most devastating attacks on the Internet community in recent years.	The student will revise the source code , compile, and execute the following attack tools: SQL-Slammer Exploit, MSBlaster-Nachi Exploit, ISSX Exploit, and Jill-Kill Exploit. The student will be required to evaluate the process and detail the results.

Section 5 (Continued)

Section 5		
	LEARNING OUTCOMES	METHOD OF ASSESSMENT
•	The student will utilize the information and techniques learned in the previous classes to protect a network or computer facility using <i>Intrusion Detection Systems</i> .	Each student will be required to install, configure, and test the product <i>SNORT Intrusion Detection System</i> . The student will create attack signatures of known malware, install, and execute the process. The lab will be evaluated based on the accuracy of the detection process.

Section 6

Name of Person Completing This Form: Cheryl Schmidt

Date: 3/13/2008