Las Positas CurricUNET
Las Positas College

Las Positas College
3000 Campus Hill Drive
Livermore, CA 94551-7650
(925) 424-1000
(925) 443-0742 (Fax)

Course Outline for CNT 7501

WHITEHAT HACKER PENETRATION TESTING

Effective: Fall 2008

I. CATALOG DESCRIPTION:
CNT 7501 — WHITEHAT HACKER PENETRATION TESTING — 4.00 units

WhiteHat and Pen testing training covers the concepts, use and appropriate application of Penetration Testing software and utilities in Ethernet networks. Students will explore the ethical use of security tools and countermeasures. Students are required to sign the "White Hat Oath" agreement of Ethical and Professional Conduct. The course will include: Hacking methods, tools, their use and detection; penetration testing and countermeasures; exploits, vulnerability assessment in computers and networks, hands-on practice in a sandbox environment. Tools used include Wireshark, Whitehat/Pentest tools for Windows, OSX, Linux.

3.00 Units Lecture 1.00 Units Lab

Strongly Recommended
CNT 67 - Wi-Fi, Cisco & CWNA

CNT 69 - Network Security; CompTIA Security + Certification

CNT 62A - Cisco Networking Academy CCNA I

CNT 57 - MS Server Advanced Services MCSA III
or

CNT 55 - Installing & Configuring Windows Server MCSA I
or

-

Grading Methods:
Letter or P/NP

Discipline:

	MIN
Lecture Hours:	54.00
Lab Hours:	54.00
Total Hours:	108.00

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 2

III. PREREQUISITE AND/OR ADVISORY SKILLS:

Before entering this course, it is strongly recommended that the student should be able to:

A. CNT67
B. CNT69
C. CNT62A
D. CNT57
E. CNT55

IV. MEASURABLE OBJECTIVES:

Upon completion of this course, the student should be able to:

A. demonstrate the identification and exploitation of system vulnerabilities
B. demonstrate understanding of and describe the roles of WhiteHat hacking and Penetration Testing
C. determine appropriate methods to identify assets and good security policies
D. determine appropriate methods to identify assets and good security policies
E. assemble a suite of application tools suited to a network environment
F. understand the process of analyzing network security assets and vulnerabilities to determine, and test a protection strategy
G. understand the concepts and characteristics of Windows security vulnerabilities
H. demonstrate the ability to configure and use basic Penetration Testing tools

I. understand the OSI model as it relates to WhiteHat Hacking
J. create a security management and exploit mitigation strategy

V. CONTENT:
- A. Networking Review
  1. Computer Networking Concepts
  2. TCP/IP and OSI Networking Models
  3. The physical layer and datalink layers
  4. The network layer
  5. The upper layers
  6. Fundamentals of IP, TCP and UDP
- B. Network Devices and Routing
  1. Routers, Switches
  2. LAN cabling, standards and topologies
  3. IP Routing Protocols
- C. Hacking and Security Today
  1. Types of Hackers
  2. Motivations and Goals
  3. Skills and Myths
- D. WhiteHat, BlackHat and Pen Testing
  1. Ethics and Professionalism
  2. Security Oath of Office
  3. Policy
  4. Development and Documentation
  5. User Training and Policy maintenance
- E. Packet Sniffers -
  1. Configuration and Packet Capture
  2. Building and using a display filter
  3. Following a TCP data stream
  4. Analyzing a TCP login and time sequence
- F. File Hex Editing tools
  1. Installation, configuration
  2. Selecting and opening files
  3. How to identify interesting file content
- G. Port Scanning
  1. Installation and configuration
  2. Scanning and reconnaisance
  3. Worm and Virus signatures
  4. Locating rogue servers
- H. Deception, Interception with honeypots
  1. Installation and configuration
  2. OS impersonation
  3. Server services
  4. Trapping and tracking
  5. Remediation, pros and cons
- I. System Auditing
  1. Installation and configuration
  2. Best practices for tests
  3. Local system audits
  4. Network/Remote system audits
- J. Password Cracking
  1. Installation and configuration
  2. Best practices for passwords
  3. Authentication test configurations
  4. Windows
  5. Unix
- K. Arp Poisoning / MiM attacks
  1. Installation and configuration
  2. Arp attacks - poisoning, spoofing
  3. Man in the middle attacks

VI. METHODS OF INSTRUCTION:
- A. **Lecture** - 1. Password best practices and policy 2. Authentication testing - password cracking
- B. **Lab** - Skill building lab exercises and projects 1. Ethereal packet trace lab a. Install and configure Ethereal on your computer b. Open the application and begin capturing packets c. Stop, save, and name the file d. Identify protocols present on the network
- C. Homework assignments from textbook 1. Read the chapter on Honeypots 2. Examine the case study and answer the relevant questions for discussion in class

VII. TYPICAL ASSIGNMENTS:

A. Lecture 1. Password best practices and policy 2. Authentication testing - password cracking B. Homework assignments from textbook 1. Read the chapter on Honeypots 2. Examine the case study and answer the relevant questions for discussion in class C. Skill building lab exercises and projects 1. Ethereal packet trace lab a. Install and configure Ethereal on your computer b. Open the application and begin capturing packets c. Stop, save, and name the file d. Identify protocols present on the network

VIII. EVALUATION:
- A. **Methods**
- B. **Frequency**
  1. Frequency
     - a. Module quizzes, mid-term and a final examination
     - b. Weekly lab assignments to develop and demonstrate understanding, problem solving and interpretation skills

IX. TYPICAL TEXTS:
1. Laura Chappell *WhiteHat Hacking.*, PodBooks, 2003.
2. Klevinsky *Hack I.T..*, Addison Wesley, 2006.
3. NSA security guides www.nsa.gov/snac/

X. OTHER MATERIALS REQUIRED OF STUDENTS: