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

Course Outline for CNT 7501

ETHICAL HACKING

Effective: Fall 2018

I. CATALOG DESCRIPTION:
CNT 7501 — ETHICAL HACKING — 3.00 units

This course introduces the network security specialist to the various methodologies for attacking a network. Students will be introduced to the concepts, principles, and techniques, supplemented by hands-on exercises, for attacking and disabling a network. These methodologies are presented within the context of properly securing the network. The course will emphasize network attack methodologies with the emphasis on student use of network attack techniques and tools and appropriate defenses and countermeasures. Students will receive course content information through a variety of methods: lecture and demonstration of hacking tools will be used in addition to an virtual environment. Students will receive a hands-on practical approach in penetration testing measures and ethical hacking.

2.50 Units Lecture 0.50 Units Lab

Strongly Recommended
CNT 52 - Networking Fundamentals
with a minimum grade of C

Grading Methods:
Letter or P/NP

Discipline:
- Computer Service Technology

	MIN
Lecture Hours:	45.00
Expected Outside of Class Hours:	90.00
Lab Hours:	27.00
Total Hours:	162.00

II. NUMBER OF TIMES COURSE MAY BE TAKEN FOR CREDIT: 1

III. PREREQUISITE AND/OR ADVISORY SKILLS:

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

A. CNT52
1. list and explain the layers of the OSI model and the TCP/IP Stack and desribe the roles of protocol layers in data networks;
2. describe and differentiate the devices, protocols, and services used to support communications in data networks and the Internet;
3. calculate both IPv4 and IP6 subnets, and segment a large network into smaller parts;
4. evaluate the importance of addressing and naming schemes at various layers of data networks in IPv4 and IPv6 environments;
5. design and assemble an Ethernet network and a wireless network, including routers, switches, and cables;
6. explain Ethernet topologies, and relevant IEEE hardware and software specifications;
7. describe the major functions of LAN hardware protocols such as Ethernet; and WAN protocols such as T-series, DSL, ATM, and Frame Relay;
8. build a router and switch topology; and configure the devices to communicate with computers;
9. compose CISCO command-line interface (CLI) commands to perform basic router and switch configration;
10. identify the responsibilities of a LAN system administrator;
11. draw typical network diagrams, using software tools such as Microsoft Visio;
12. monitor the network activity using monitoring tools to view packets and analyze traffic.

IV. MEASURABLE OBJECTIVES:

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

A. Describe and apply the tools and methods a "hacker" uses to break into a computer or network.
B. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.
C. Practice and use safe techniques on the World Wide Web.

D. Analyze a capture of data transmission, using network analyzers (WireShark, nmap, snort)
E. Interpret data collected by scanning a network with various tools, and identify the legitimate packets.
F. Secure network equipment (computers, switches and routers) both physically and digitally.
G. Identify a network attack and remedy it by using hardware and software intrusion detection systems.

V. CONTENT:

A. Ethical Hacking Overview
   1. Introduction to Ethical Hacking
      a. The Role of Security and Penetration Testers
      b. Penetration-Testing Methodologies
      c. Certification Programs for Network Security Personnel
   2. What You Can Do Legally
      a. Laws of the Land
      b. Is Port Scanning Legal?
      c. Federal Laws
   3. What You Cannot Do Legally
      a. Get It in Writing
      b. Ethical Hacking in a Nutshell

B. TCP/IP Concepts Review
   1. Overview of TCP/IP
      a. The Application Layer
      b. The Transport Layer
      c. The Internet Layer
   2. IP Addressing
      a. Planning IP Address Assignments
      b. IPv6 Addressing
   3. Overview of Numbering Systems
      a. Reviewing the Binary Numbering System
      b. Reviewing the Octal Numbering System
      c. Reviewing the Hexadecimal Numbering System

C. Network and Computer Attacks
   1. Malicious Software (Malware)
      a. Viruses
      b. Macro Viruses
      c. Worms
      d. Trojan Programs
      e. Spywaref. Adware
   2. Protecting Against Malware Attacks
      a. Educating Your Users
   3. Intruder Attacks on Networks and Computers
      a. Denial-of-Service Attacks
      b. Distributed Denial-of-Service Attacks
      c. Buffer Overflow Attacks
      d. Ping of Death Attacks
      e. Session Hijacking
   4. Addressing Physical Security
      a. Keyloggers
      b. Behind Locked Doors

D. Footprinting and Social Engineering
   1. Using Web Tools for Footprinting
      a. Conducting Competitive Intelligence
      b. Analyzing a Company's Web Site
      c. Using Other Footprinting Tools
      d. Using E-mail Addresses
      e. Using HTTP Basics
      f. Other Methods of Gathering Information
   2. Using Domain Name System Zone Transfers
   3. Introduction to Social Engineering
      a. The Art of Shoulder Surfing
      b. The Art of Dumpster Diving
      c. The Art of Piggybacking
      d. Phishing

E. Port Scanning
   1. Introduction to Port Scanning
      a. Types of Port Scans
   2. Using Port-Scanning Tools
      a. Nmap
      b. Unicornscan
      c. Nessus and OpenVAS
   3. Conducting Ping Sweeps
      a. Fping
      b. Hping
      c. Crafting IP Packets
   4. Understanding Scripting
      a. Scripting Basics

F. Enumeration
   1. Introduction to Enumeration
   2. Enumerating Windows Operating Systems
      a. NetBIOS Basics
      b. NetBIOS Enumeration Tools
      c. Additional Enumeration Tools
   3. Enumerating the NetWare Operating System
      a. NetWare Enumeration Tools
   4. Enumerating the *nix Operating System
      a. UNIX Enumeration

G. Programming for Security Professionals
   1. Introduction to Computer Programming
      a. Programming Fundamentals
   2. Learning the C Language

a. Anatomy of a C Program
3. Understanding HTML Basics
a. Creating a Web Page with HTML
4. Understanding Perl
a. Background on Perl
b. Understanding the Basics of Per
c. Understanding the BLT of Perl
5. Understanding Object-Oriented Programming Concepts
a. Components of Object-Oriented Programming
b. An Overview of Ruby

H. Desktop and Server OS Vulnerabilities
1. Windows OS Vulnerabilities
a. Windows File Systems
b. Remote Procedure Call
c. NetBIOS
d. Server Message Block
e. Common Internet File System
f. Null Sessions
g. Web Services
h. SQL Server
i. Buffer Overflows
j. Passwords and Authentication
2. Tools for Identifying Vulnerabilities in Windows
a. Built-in Windows Tools
3. Best Practices for Hardening Windows Systems
a. Patching Systems
b. Antivirus Solutions
c. Enable Logging and Review Logs Regularly
d. Disable Unused Services and Filtering Ports
e. Other Security Best Practices
4. Linux OS Vulnerabilities
a. Samba
b. Tools for Identifying Linux Vulnerabilities
c. More Countermeasures Against Linux Attacks

I. Embedded Operating Systems: The Hidden Threat
1. Introduction to Embedded Operating Systems
2. Windows and Other Embedded Operating Systems
a. Other Proprietary Embedded OSs
b. *Nix Embedded OSs
3. Vulnerabilities of Embedded OSs
a. Embedded OSs Are Everywhere
b. Embedded OSs Are Networked
c. Embedded OSs Are Difficult to Patch
d. Embedded OSs Are in Networking Devices
e. Embedded OSs Are in Network Peripherals
f. Supervisory Control and Data Acquisition Systems
g. Cell Phones, Smartphones, and PDAs
h. Rootkits
i. Best Practices for Protecting Embedded OSs

J. Hacking Web Servers
1. Understanding Web Applications
a. Web Application Components
b. Using Scripting Languages
c. Connecting to Databases
2. Understanding Web Application Vulnerabilities
a. Application Vulnerabilities and Countermeasures
b. Assessing Web Applications
3. Tools for Web Attackers and Security Testers
a. Web Tools

K. Hacking Wireless Networks
1. Understanding Wireless Technology
a. Components of a Wireless Network
2. Understanding Wireless Network Standards
a. The 802.11 Standard
b. An Overview of Wireless Technologies
c. Additional IEEE 802.11 Projects
3. Understanding Authentication
a. The 802.1X Standard
4. Understanding Wardriving
a. How It Works
5. Understanding Wireless Hacking
a. Tools of the Trade
b. Countermeasures for Wireless Attacks

L. Cryptography
1. Understanding Cryptography Basics
a. History of Cryptography
2. Understanding Symmetric and Asymmetric Algorithms
a. Symmetric Algorithms
b. Asymmetric Algorithms
c. Digital Signatures
d. Sensitive Data Encryption
e. Hashing Algorithms
3. Understanding Public Key Infrastructure
a. Components of PKI
4. Understanding Cryptography Attacks
a. Birthday Attack
b. Mathematical Attacks
c. Brute-Force Attack
d. Man-in-the-Middle Attack
e. Dictionary Attack

f. Replay Attack
g. Understanding Password Cracking

M. Network Protection Systems
1. Understanding Routers
a. Understanding Routing Protocols
b. Understanding Basic Hardware Routers
c. Understanding Access Control Lists
2. Understanding Firewalls
a. Understanding Firewall Technology
b. Implementing a Firewall
c. Understanding the Cisco Adaptive Security Appliance Firewall
d. Using Configuration and Risk Analysis Tools for Firewalls and Routers
3. Understanding Intrusion Detection and Prevention Systems
a. Network-Based and Host-Based IDSs and IPSs
b. Web Filtering
c. Security Incident Response Teams
4. Understanding Honeypots
a. How Honeypots Work

N. LABS
1. Using Active and Passive Techniques to Enumerate Network Hosts
2. Conducting Active and Passive Reconnaissance Against a Target
3. Using the SYSTEM account
4. Poison Ivy – Remote Access Trojan
5. Using the SHARK Remote Administration Tool
6. Utilizing Malware - Dark Comet
7. Breaking Windows Passwords
8. Using John the Ripper to Crack Linux Passwords
9. Using Spear Phishing to Target an Organization
10. Breaking WEP and WPA Encryption
11. Using Metasploit to Attack a Remote System
12. Using Armitage to Attack the Network
13. Exploitation with IPv6
14. Creating MSFPAYLOADS
15. Abusing SYSTEMS
16. SQL Injection
17. Launching a Buffer Overflow
18. Intrusion Detection19. Using Certificates to Encrypt Email

VI. METHODS OF INSTRUCTION:
A. **Demonstration** -
B. **Lecture** -
C. **Lab** -

VII. TYPICAL ASSIGNMENTS:
A. Reading Assignments
1. Textbook readings and online supporting webpages to inform the student on the tools and methods a "hacker" uses to break into a computer or network.
B. Projects, Activities, and other Assignments
1. Hands-on lab assignments on the shared NETLAB+ remote lab system on how to defend a computer and a LAN against a variety of different types of security attacks.
2. Troubleshooting non expected outcomes.
C. Writing Assignments
1. Worksheets and Lab Reports to support the lab assignments and document the results of those lab assignments.

VIII. EVALUATION:
A. **Methods**

1. Exams/Tests
2. Quizzes
3. Lab Activities

B. **Frequency**

1. Weekly objective quizzes and lab projects
2. The final comprehensive exam and the skills-based assessment will be administered during the final week of class

IX. TYPICAL TEXTS:
1. Simpson, Michael. *Hands-On Ethical Hacking and Network Defense.* 3rd ed., Delmar Cengage Learning, 2016.
2. Oriyano , . *CEH v9: Certified Ethical Hacker Version 9 Study Guide.* 3 ed., Sybex, 2016.
3. Walker, Matt . *CEH Certified Ethical Hacker All-in-One Exam Guide.* 3 ed., McGraw-Hill Education, 2016.

X. OTHER MATERIALS REQUIRED OF STUDENTS: