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

Course Outline for CNT 7502

WIRESHARK, TCP/IP ANALYSIS AND NETWORK TROUBLESHOOTING

Effective: Fall 2008

I. CATALOG DESCRIPTION:
CNT 7502 — WIRESHARK, TCP/IP ANALYSIS AND NETWORK TROUBLESHOOTING — 4.00 units

Course is geared to teach solid network management skills using the WiresharkTM network analyzer. The class provides a logical troubleshooting approach to capturing and analyzing data frames. Armed with this knowledge, students can effectively troubleshoot, maintain, optimize and monitor network traffic and keep your network operating at its peak performance.

3.00 Units Lecture 1.00 Units Lab

Strongly Recommended
CIS 50 - Intro to Computing Info Tech

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. CIS50

IV. MEASURABLE OBJECTIVES:

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

A. demonstrate an understanding of the OSI model;
B. describe the components of the TCP/IP protocol suite;
C. install and configure Wireshark for Windows, Linux or Apple OS X;
D. identify and discuss the advantages and limitations of closed source and open source network analysis software and hardware;
E. capture and display network traffic;
F. demonstrate an understanding TCP and UDP frame structure;
G. outline the steps necessary to observe and capture network traffic in common LAN topologies;
H. demonstrate an understanding of Windows, Linux and Apple OS X IP ports and TCP operational similarities and differences;
I. demonstrate the ability to discover system and application characteristics through packet analysis;
J. discuss and evaluate security and authentication at the packet level;
K. demonstrate an understanding of TCP-IP windowing;
L. demonstrate the use of Wireshark and other network monitoring tools in evaluating VoIP;
M. describe and demonstrate troubleshooting methods for common TCP problems.

V. CONTENT:
A. Introduction to Network Analysis
1. Concepts
2. Uses
3. Sniffing
4. Network Data
5. History of analyzers
B. OSI Model
1. Physical
2. Data Link
3. Network
4. Transport
5. Session

6. Presentation
7. Application

C. Ethernet
1. 802.3
2. CSMA/CD
3. 802.2
4. 802.11

D. TCP/IP Suite
1. IP
2. TCP / UDP
3. ARP
4. ICMP

E. Networks
1. Wiring / Standards
2. Routers
3. Switches / Bridges
4. Hubs
5. Wireless

F. Wireshark
1. History
2. Development
3. Installation / configuration
4. Basic operation

G. Filters
1. Capture
2. Display
3. Logical operators
4. Boolean expressions
5. Hidden fields

H. Sniffing
1. Hubbing out
2. Port mirroring
3. NICs
4. Promiscuous mode
5. Hardware
6. Software

I. Protocol dissection
1. DNS
2. ARP
3. NTP
4. HTTP
5. ICMP
6. SNMP
7. SMTP

J. Network Security
1. Preventing sniffing
2. DDOS
3. War Driving
4. SYN floods
5. Man in the Middle attacks
6. ARP poisoning
7. Switch attacks

K. Case Studies
1. Baselining networks
2. Attack profiles
3. Common TCP problems
4. Dissecting Malware / Worms

L. Other Wireshark tools
1. Tshark
2. H.225 counters
3. HTTP statistics
4. editcap
5. mergecap
6. text2pcap
7. dumpcap

VI. METHODS OF INSTRUCTION:
A. **Lecture** -
B. **Demonstration** -
C. **Research** -
D. **Lab** -
E. Assigned reading
F. **Discussion** -

VII. TYPICAL ASSIGNMENTS:
A. Reading / listening to presentations and readings 1. Presentations and lectures a. Example: Lecture on Wireshark installation 2. Selected current online readings a. Example: Read Wireshark configuration tutorial, at www.wireshark.org B. Search for relevant material and read 1. Students use search engines to find readings relevant for each module a. Example: Find resources describing DDOS attacks, select 3 to read C. Provide comments regarding curriculum 1. Discussion and response questions accompany each module a. Example: “Discuss how FTP transmits names and passwords compared to FTPS.” D. Answer comments and questions from fellow students and Instructor 1. Students must participate in group discussion a. Example: On the Apple.com web site, research the commonly used IP ports and compare and contrast with Windows XP

VIII. EVALUATION:
A. **Methods**

B. **Frequency**

1. Frequency:
    a. 6-10 module assignments
    b. Weekly discussion of group work
    c. 6-10 module quizzes
    d. 6-10 labs
    e. 1 final project
2. Typical quiz question:
    a. What is the difference between Wireshark and Ethereal?
    b. Describe the operation of ARP and RARP
3. Final exam

IX. TYPICAL TEXTS:

1. Angela Orebaugh, Gilbert Ramirez, Jay Beale *Wireshark & Ethereal Network Protocol Analyzer Toolkit.*, Syngress Press, 2007.
2. Chris Sanders *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems.*, O'Reilly Media, 2007.

X. OTHER MATERIALS REQUIRED OF STUDENTS:

A. Students require access to a computer connected to the Internet, with word processing and browser software, and an email address.