Advanced Network Analysis using Wireshark

Table of Contents

Instructor: Dr. W. L. Eaton
OFFICE: 213 F in the Advanced Technology Center
OFFICE PHONE: 904-598-5657
EMAIL: weaton@fscj.edu

Hours

Monday **9:00 AM to 5:00 PM**
Tuesday **9:00 AM to 5:00 PM**
Wednesday **9:00 AM to 5:00 PM**
Thursday **9:00 AM to 5:00 PM**
Friday **9:00 AM to 12:00 PM**

Topical Course Outline

DAY	Topics	Chapter References	Dates
Monday Morning	The world of network analysis – Introduction to Wireshark – Defining global and personal preferences – Colorizing traffic – Defining time values and interpreting summaries	Chapter 1-2, 5-7 Week-1 In-class Lab Week-1 Online Lab	**6-23-2014**
Monday Afternoon	Interpreting basic trace file statistics – Following TCP/UDP data streams and reassembling data – Customizing Wireshark profiles – Saving exporting and printing packets – Using the expert system	Week-2 In-class Lab Week-2 Online Lab Timed-Test Lab	**6-23-2014**

Tuesday Morning	Capture traffic – Creating and applying capture filters – Creating and applying display filters – Creating custom profiles	Week-3 In-class Lab Week-3 Online Lab Timed-Test-2 Lab Capture The Flag	**6-24-2014**
Tuesday Afternoon	Wireless Network Analysis – 802.11 WLAN using AirPcap– Spectrum Analysis with WiSPY2.4	Week-4 In-class Lab Week-4 Online Lab Timed-Test-3 Lab	**6-24-2014**
Wednesday Morning	Advanced protocol Analysis. Concentration on troubleshooting advanced network protocols and problems.	Chapters 16 – 20 Wireless Network Setup Individual Wireless Lab Preview of Protocols Lab Timed-Test 4	**6-25-2014**
Wednesday Afternoon	Advanced protocol Analysis Continued. TCP, DNS, HTTP, FTP, DHCP, VoIP and Email protocols	Chapters 14, 15, 22, Protocol Analysis Lab Week-6 Online Lab	**6-25-2014**
Thursday Morning	Introduction to IPV6 network analysis – Cisco Embedded Packet Capture- Network Baselining – Advanced network problem analysis	Chapters 28,29, & 30 IPv6 Lab Advanced Protocol Lab Week-7 Online Lab Timed-Test 6	**6-26-2014**
Thursday Afternoon	On-the-Wire & Command-line Tools Final Examination	Hands-on practical timed examination	**6-26-2014**
Friday	Command-line Tools Security Profiles Wireshark Version 1-10 Preview	Command-line Lab	**6-27-2014**

Instructor's Bio

In February of 2005 Dr. Eaton retired from his position as Chief Security Officer for the City of Jacksonville and accepted a full professorship at FSCJ' s Advanced Technology Center. In addition to CSO, Dr. Eaton managed the City's Data Center Operations and Radio Technologies Group. He has over 35 years of computer and networking experience. Prior to his employment with the City, he held the position of Senior Systems Field Engineer for the Unisys Corporation. At Unisys Dr. Eaton's duties as Branch Support Manager included installation and maintenance of both mainframe hardware and system software. Dr. Eaton retired from the Unisys Corporation after 20

years of employment. In addition to teaching he currently serves as a forensics/network security consultant and SME (Subject Matter Expert) for ***Mulholland Forensics LLC, FD3 Technology Inc., WJXT Channel 4 NEWS,*** and ***First Coast News Channel 12***

Education

Doctor of Philosophy in Business Administration
With a specialization in ***Computer and Information Security***
NorthCentral University, Arizona)
ΆΦΣ (Alpha Phi Sigma, National Criminal Justice Honor Society)
ΔΜΔ (Delta Mu Delta, International Honor Society in Business)
Master of Science in Network Security
Capitol College of Maryland – *Honors*
Bachelor of Science in Computer Science
Grantham University, *summa cum laude*
(ΔΣT Delta Epsilon Tau Honor Society)
Associate of Science in Electronics Engineering Technology
Grantham College of Engineering

Certifications and Credentials

WCNA (Wireshark Certified Network Analyst)
CNX (Certified Network Expert – Networking Analyst)
CISSP (Certified Information Systems Security Professional)
CEH (Certified Ethical Hacker, EC-Council)
GCFA (GIAC Computer Forensics Analysis)
CCE (Certified Computer Examiner – Computer Forensics Specialist)
Security + (CompTIA)
Network + (CompTIA)
Certified Risk Assessment Trainer (Carnegie Mellon Software Engineering Institute)
FCC (First Class Federal Communications Commission - Radio/Telephone License)
ISO-FDLE (Information Security Officer, Florida Department of Law Enforcement) (Inactive)
CCNP (Cisco Certified Network Professional)
CCNA (Cisco Certified Network Associate)
CCDP (Cisco Certified Design Professional)
CCDA (Cisco Certified Design Associate)
MCSE (Microsoft Certified System Engineer)

Publications

Sniffer Pro Network Optimizations and Troubleshooting Handbook
(Syngress Publishing, Co-author).
Snort 2.0 Intrusion Detection
(Syngress Publishing, Co-author)

Professional Organizations

ISFCE (International Society of Forensic Computer Examiners)
ACFEI (American College of Forensics Examiners Institute)
DFWG (Digital Forensics Working Group)
ABA (American Bar Association)
IEEE (Institute of Electrical and Electronic Engineers)
ACM (Association for Computing Machinery)
AFIO (Association of Former Intelligence Officers)
ISSA (Information System Security Association)
InfraGard (FBI/Industry Security Consortium)
JITC (Jacksonville Chamber of Commerce IT Council)