Network Protocol Analysis 2023-2024 Catalog

[ARCHIVED CATALOG]

CSIA 210 - Network Protocol Analysis

PREREQUISITES: NETI 104 - Introduction to Networking or NETI 109 - Networking I
PROGRAM: Cyber Security/Information Assurance
CREDIT HOURS MIN: 3
LECTURE HOURS MIN: 2
LAB HOURS MIN: 2
DATE OF LAST REVISION: Fall, 2014

Offers in-depth coverage of all the salient models, protocols, services, and standards that govern TCP/IP and that guide its behavior on modern networks. Specific guidance is given to reinforce the concepts introduced and to help prepare students to interact with TCP/IP on the vast majority of networks in use today. As a hands-on course, students are provided first hand experience in installing, configuring, analyzing, using, and managing TCP/IP on a network. Included are case projects that pose problems and require creative solutions that should prepare students for the kinds of situations faced on a real, live network.

MAJOR COURSE LEARNING OBJECTIVES: Upon successful completion of this course the student will be expected to:

1. Develop an understanding of basic IP packet structures.
2. Explore and explain the Data Link and Network Layer Protocols examining packet/frame types, hardware addresses, and the Neighbor Discovery Protocol.
3. Analyze routing and routed protocols with considerations for both IPv4 and IPv6 protocols and behaviors.
4. Examine ICMP testing and troubleshooting methods, security issues, and ICMP message types and codes.
5. Explain how neighbor discovery works on IPv6 networks.
6. Describe various auto-addressing schemes and mechanisms used on IPv4 and IPv6 networks.
7. Explain key services used to resolve symbolic, human-readable network names, and addresses into machine-intelligible network addresses.
8. Examine the common and appropriate uses of the TCP and UDP protocols.
9. Describe issues and techniques that apply when IPv4 and IPv6 must coexist on the same networks.
10. Examine tunneling mechanisms and protocols.
11. Understand, plan, deploy, and use IPv6 on modern TCP/IP networks.
12. Appraise general network security basics with a particular emphasis on IP security topics.
13. Review key topics including perimeter security, infrastructure security, and host device security.

COURSE CONTENT: Topical areas of study include -

- Headers
- Payloads
- ARP
- RARP
- IPv4
- IPv6
- RIPv1/ v2

- OSPF
- EIGRP
- BGP
- DHCPv4 /v6
- APIPA
- Host/interface address determination
- Stateless and stateful address auto configuration
- ISATAP
- 6to4
- Teredo
- OSI Model
- TCP/IP Model
- WireShark
- TCPdump
- Nmap

Course Addendum - Syllabus (Click to expand)
