CSE 804 Network and Internet Security

Internet architecture, security flaws on the Internet, **Attacks on networks**: DDOS attacks, reflection attacks, amplification attacks, wireless security, WEP cracking, DNS hijacking, routing attacks, case study: NTP DDOS attack, spamhaus DDOS attack. **Network security at different layers of the OSI and TCP/IP models**: firewalls, security protocols (in particular, IPsec, SSL, and Kerberos), Denial of Service (DoS) attacks/ detection/prevention, viruses and worms, DNS, email & Voice Over IP (VoIP) security, wireless infrastructure security. **Network Intrusion Detection and Analysis**: NIDS/NIPS functionality, Modes and types of NIDS, NIDS/NIPS evidence acquisition, snort rules and alerts, Case study. **Formal methods for modeling and analyzing authorization and access control systems**. **Designing Enterprise systems for Access Control, Authentication and Auditing (AAA)**: Designing networks on selected protocols to support business operations while maintaining identified levels of network security. Supporting secondary network connectivity (wireless, VPNs, BYOD devices, partner networks, cross-domain and other connectivity types). Overview of Information and Network Security Technologies. Overview of Critical Infrastructural Components and Attacks (e.g., Smart Grid, medical systems, smart homes and others), Anomaly detection and attack graphs.

Textbook and Reference:

Textbook:
– *Gary McGraw*, **Information Security: Principals and Practice**, 2nd Edition, John Wiley & Sons, Inc Publication, ISBN 978-0-470-62639-9.

– *Occupytheweb*, **Getting Started Becoming a Master Hacker**, V 1.3.

– *Occupytheweb*, **Networks Basics For Hackers**, V 1.0, InfoSec Press 2023.

– *Occupytheweb*, **Linux Basics For Hackers**, V 1.0, 1st Edition, ISBN-10: 1-59327-855-1.