CSC 431 / 631:

Cyber Security Operations Syllabus

|  |  |
| --- | --- |
| Instructor Frank M. Olmstead Phone (202)630-2763 EmailOffice Location Remote - Virginia Office Hours Enter Hours, Days | Course Overview **Cyber Security Operations -****Introduce the fundamental cyber security operations to secure systems****through monitoring, detecting,****investigating, analyzing, and responding to security events. Secure systems from cyber security risks, threats, and vulnerabilities. Prepare students for additional certifications beyond the CCNA. Three hours of combined lecture and lab in a computer lab setting**  **frank.olmstead@lsus.edu**  **No purchase required. Weekly reading excerpts will be provided from the book; Ten Strategies of a World-Class Cybersecurity Operations Center by Carson Zimmerman, ISBN: 978-0-692-24310-7**   * **Normally after business day hours (0800-1600 Eastern) for phone conversations, emails answered between 12-24 hours.**   Grading -  Week Zoom (attendance) - 5%  Weekly forum posts - 20%  Take home project (week 4 only) - 20%  Quiz - 25%  Final - 30% |

# Course Schedule

|  |  |  |
| --- | --- | --- |
| Week | Subject | Practice Problems |
| Week 1 | Security Operations | Forum Questions |
| Week 2 | Types of reporting  • I&W  • AS&W  Malware Analysis  • Types  • Process (Overview)  Developing rules  Day in the life – BEC Example | Forum Questions / Create Yara signature |
| Week 3 | Types of Investigations  • OSINT Methodology  • Active & Passive Collection of Information  OSINT Uses  • Where to Start  • OSINT Process  Keeping yourself Safe during OSINT gathering  Resources  • Plug-in & Extensions  • Techniques and Tooling  Email Investigations | Enter practice problems |
| Week 4 | Network Detection & Response  Network Design with Security in Mind  Network Security Monitoring (NSM)  Email Encryption  • Secure Email Providers | Network Design Practical |
| Week 5 | Hashing  • Demo & exercise  Network Security Monitoring (NSM) | Encryption Practical |
| Week 6 | Threat Intelligence  • Bad actors  • Tools  PCAP |  |
| Week 7 | SPAM  Threats  • Phishing / Spear Phishing / Whaling / Vishing / Smishing  DKIM  SPF  Email header (SPF & DKIM) |  |
| Week 8 | Domains  •Domain Names  •Domain Registrations  •URL Structure  DNS  •What is it  •Record types  DNS Requests  •Hosts file (example)  •DNS Requests (non-Authorative example)  •DNS Requests (Authorative example) |  |
| Week 9 | Major DNS attack types  • DoS  • DDoS  • DNS Amplification  • Zero-day attack  DNS Poisoning  DNS Tunneling  Fast-flux DNS attack  DNS Sinkhole |  |
| Week 10 | Ransomware  • What is it ?  • How it works ?  • Sp@m  • Exploit Kits  • How it spreads ?  • Why is Ransomware so effective?  Ransomware - Responding to an Infection  Ransomware - Best Security Practices  Should you pay ? |  |
| Week 11 | Virus  • Common types  • What are they / how do they spread  • What are the most common types  Protecting Sensitive Information  • Passwords / Browsers / Extensions  Ransomware  TOR |  |
| Week 12 | Shodan |  |
| Week 13 | Attribution Models  • Kill Chains  • The Diamond Model  • MITRE ATT&CK Framework |  |

# Exam Schedule

|  |  |
| --- | --- |
| Week | Subject |
| Week 10 | Quiz (weeks 1 thru 9) |
| Week 12 | Final |
|  |  |
|  |  |

# Homework Policy

Weekly reading and forum post replies – due the following week on class day