The National Cyber League – Where Cybersecurity is a Passion

National Cyber League
CompTIA Security+™ Syllabus

Note to Faculty

This NCL Syllabus is intended as a supplement to courses that are based on the CompTIA Security+™ curriculum/exam, or courses that include similar knowledge and skills.

A primary goal of the NCL is to seamlessly integrate hands-on lab exercises and challenging cybersecurity games into higher education curriculum. The NCL uses a game analogy to describe our events because we believe that we are providing a fun environment that allow students (AKA **players**) to test their knowledge and skills against other players -- just like a game!

This NCL Syllabus is not intended as a replacement to an existing course, but can provide supplemental hands-on lab exercises aligned with the NCL games. We encourage college faculty to look at ways to include this syllabus as part of the lab component of their course(s). While CompTIA Security+™ and EC-Council Certified Ethical Hacker (CEH)™ performance-based exam objectives are the foci of the 2013 NCL Fall Season, faculty and students in related security courses can also benefit from adding hands-on labs and NCL games as part of their course assignments. As educators, we understand the importance of aligning exercises to an academic calendar (e.g., semesters). We welcome feedback to help us to best support faculty and their instructional goals.

Network Development Group (NDG) collaborated with the Center for Systems Security and Information Assurance (CSSIA) to create a series of lab exercises intended to support the CompTIA Security+™ curriculum. As an NDG partner, the NCL is able to take full advantage of this collaboration and offer these excellent hands-on labs to all NCL players and coaches.

We suggest that faculty use the lab assignments in this syllabus as ungraded homework for students, and the NCL games as graded assignments.

Through the NCL, college faculty will be able to infuse virtual cyber lab exercises into their courses and be better prepared to coach competitive cyber teams. Please contact Dr. Dan Manson (dmanson@csupomona.edu) if you have questions about using the labs and games in your fall courses.

2013 Fall Season

The 2013 NCL Fall Season will be will partially based on the CompTIA Security+™ performance-based objectives, a widely recognized and adopted curriculum and certification (The 2013 NCL Fall Season also includes objectives for the EC-Council CEH™).

Akin to conditioning in athletics, or practicing layups and free throws in the gym, the NCL will host 16 virtual preparatory CompTIA Security+™ lab exercises in Cyber Gymnasiums across the country, which students can use to develop and practice hands-on skills for the NCL Games and the CompTIA Security+™ exam.

Players will be participating in a type of computer security game called a *Capture-the-Flag* (CTF). In CTF games, players race to answer security-related challenges, often searching for digital “flags" hidden on servers, in encrypted text, or in applications. Challenges within the CTF are open-ended and require expertise and skills in a wide range of security-related topics: computer forensics, cryptography, network penetration testing, web security, and system/network administration. When a player submits a flag, they receive points for solving the challenge. The player or team with the highest cumulative score at the end of the game wins.

The NCL will also host a Regular Season, comprised of a mandatory Pre-Season assessment (October 7th-13th), 2 Regular Season games, optimized for individuals (October 19th and October 26th), and 2 Post Season games for teams: the NCL Conference Championship (November 9th) and the NCL National Championship (November 16th).

These games will be created and optimized for individuals and teams and are designed to provide hands-on experiences and challenges to help students to develop and improve cybersecurity skills and problem-solving abilities. All games will be conducted remotely, in virtual Cyber Stadiums, equally accessible to all.

Who Can Participate?

- Individuals currently enrolled as a student at an U.S. accredited 2- or 4-year college/university
- All teams must have a faculty/mentor coach
- Registration fee is $20 per individual participant and $25 per participating team
- Players are expected to commit to the entire season
- There are no prerequisite skills for participation, but successful Bronze-level players will have completed the preparatory exercises; Silver- and Gold-level players a cross-section of intermediate knowledge and skills in computer science, networking, systems administration, and information security

The Mt. SAC Cyber Defense Team (from left to right): Lam Cun, Yinfeng Cai, Philip Weniger, Jimmy Tu, Ray Wu, Chris Nila, Brian Baligad, Robert Murray, and Professor Jim Gau

NCL Recommended Text

The syllabus topics provided below are based on the following textbook:

Security+ Guide to Network Security Fundamentals, 4e
Author: Mark Ciampa
Publisher: Course Technology
ISBN-10: 1111640122
ISBN-13: 9781111640125

NCL Syllabus Topics

- Introduction to Security
- Malware and Social Engineering Attacks
- Application and Network Attacks
- Vulnerability Assessment and Mitigating Attacks
- Host, Application, and Data Security
- Network Security

- Administering a Secure Network
- Wireless Network Security
- Access Control Fundamentals
- Authentication and Account Management
- Basic Cryptography
- Advanced Cryptography
- Business Continuity
- Risk Mitigation

The table below lists the domain areas measured by the CompTIA Security+™ examination and the approximate extent to which they are represented in the exam:

CompTIA Security+™ Domain	% of Examination
1.0 Network Security	21%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	21%
4.0 Application, Data and Host Security	16%
5.0 Access Control and Identity Management	13%
6.0 Cryptography	11%
Total	**100%**

Within these six domains are the following CompTIA Security+™ performance-based exam objectives:

- **1.0 Network Security**:
  - Objective 1.2: Apply and implement secure network administration principles
  - Objective 1.4: Implement and use common protocols
  - Objective 1.6: Implement wireless network in a secure manner

- **2.0 Compliance and Operational Security**:
  - Objective 2.2: Carry out appropriate risk mitigation strategies
  - Objective 2.3: Execute appropriate incident response procedures
  - Objective 2.7: Execute disaster recovery plans and procedures

- **3.0 Threats and Vulnerabilities**:
  - Objective 3.1: Analyze and differentiate among types of malware
  - Objective 3.2: Analyze and differentiate among types of attacks
  - Objective 3.5: Analyze and differentiate among types of application attacks
  - Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques
  - Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities

- **4.0 Application, Data and Host Security**:
  - Objective 4.2: Carry out appropriate procedures to establish host security

- **5.0 Access Control and Identity Management**:
  - Objective 5.3: Implement appropriate security controls when performing account management

- **6.0 Cryptography**:
  - Objective 6.2: Use and apply appropriate cryptographic tools and products
  - Objective 6.4: Implement PKI, certificate management and associated components

Lab Exercises

There are 16 remote lab exercises designed to:

- Reinforce the concepts covered in the CompTIA Security+™ performance-based exam objectives
- Help prepare students for the NCL games
- Help students prepare for the CompTIA Security+™ exam
- Provide supplemental lab exercises for faculty teaching CompTIA Security+™ and Network Security-related classes

The lab exercises can be completed anytime, anyplace, via the virtual NCL Cyber Gymnasiums. Instructions for accessing these lab exercises will be made available separately.

The lab exercises listed as follows are mapped to the appropriate CompTIA Security+™ domain and performance-based exam objective:

- **1.0 Network Security**:
  - Objective 1.2: Apply and implement secure network administration principles:
    - **Lab Exercise 1**: *Network Devices and Technologies - Capturing Network Traffic*
    - **Lab Exercise 2**: *Secure Network Administration Principles - Log Analysis*

- Objective 1.4: Implement and use common protocols:
  - **Lab Exercise 3**: *Protocols and Default Network Ports - Transferring Data Using TCP/IP*
  - **Lab Exercise 4**: *Protocols and Default Network Ports - Connecting to a Remote System*
- Objective 1.6: Implement wireless network in a secure manner:
  - **Lab Exercise 5**: *Secure Implementation of Wireless Networking*

- **2.0 Compliance and Operational Security**:
  - Objective 2.3: Execute appropriate incident response procedures:
    - **Lab Exercise 6**: *Incident Response Procedures*

- **3.0 Threats and Vulnerabilities**:
  - Objective 3.1: Analyze and differentiate among types of malware
    - **Lab Exercise 7**: *Analyze and Differentiate Types of Malware*
  - Objective 3.2: Analyze and differentiate among types of attacks:
    - **Lab Exercise 8**: *Analyze and Differentiate Types of Attacks Using Window Commands*
  - Objective 3.5: Analyze and differentiate among types of application attacks:
    - **Lab Exercise 9**: *Analyze and Differentiate Types of Application Attacks*
  - Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques:
    - **Lab Exercise 10**: *Mitigation and Deterrent Techniques - Anti Forensics*

        - **Lab Exercise 11**: *Mitigation and Deterrent Techniques - Password Cracking*
    - Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities:
        - **Lab Exercise 12**: *Discovering Security Threats and Vulnerabilities*

- **4.0 Application, Data and Host Security**:
    - Objective 4.2: Carry out appropriate procedures to establish host security:
        - **Lab Exercise 13**: *Importance of Data Security - Data Theft*
        - **Lab Exercise 14**: *Importance of Data Security - Securing Data Using Encryption Software*

- **5.0 Access Control and Identity Management**:
    - Objective 5.3: Implement appropriate security controls when performing account management:
        - **Lab Exercise 15**: *Authentication, Authorization and Access Control*

- **6.0 Cryptography**:
    - Objective 6.2: Use and apply appropriate cryptographic tools and products:
        - **Lab Exercise 14**: *Importance of Data Security - Securing Data Using Encryption Software*
        - **Lab Exercise 16**: *General Cryptography Concepts*

Suggested Schedule

The following suggested schedule maps the *Security+ Guide to Network Security Fundamentals, 4e* textbook chapters with the corresponding NCL lab exercise(s) and NCL Games:

Suggested Schedule (game dates subject to change)
-**Chapter 1**: Introduction to Security
-**Chapter 2**: Malware and Social Engineering Attacks
-**Chapter 3**: Application and Network Attacks --***Lab 8****: Analyze and Differentiate Types of Attacks Using Windows Commands* --***Lab 7****: Analyze and Differentiate Types of Malware* --***Lab 9****: Analyze and Differentiate Types of Application Attacks (Tasks 2-4)* --***Lab 12****: Discovering Security Threats and Vulnerabilities (Task 3)* --***Lab 13****: Importance of Data Security - Data Theft* --***Lab 6****: Incident Response Procedures (Task 1)*
-**Chapter 4**: Vulnerability Assessment and Mitigating Attacks --***Lab 12****: Discovering Security Threats and Vulnerabilities (Tasks 1-2)* --***Lab 11****: Mitigation and Deterrent Techniques - Password Cracking* --***Lab 1****: Network Devices and Technologies - Capturing Network Traffic*
10/19/13 Regular Season: Game #1 **(Prerequisite: Mandatory Pre-Season 10/07-10/13)**
-**Chapter 5**: Host, Application, and Data Security --***Lab 10****: Mitigation and Deterrent Techniques - Anti-Forensics* --***Lab 2****: Secure Network Administration Principles - Log Analysis*
-**Chapter 6**: Network Security
-**Chapter 7**: Administering a Secure Network

--***Lab 3***: *Protocols and Default Network Ports - Transferring Data Using TCP/IP* --***Lab 4***: *Protocols and Default Network Ports - Connecting to a Remote System* --***Lab 9***: *Analyze and Differentiate Types of Application Attacks (Task 1)*
-**Chapter 8**: Wireless Network Security --***Lab 5***: *Secure Implementation of Wireless Networking*
-**Chapter 9**: Access Control Fundamentals --***Lab 15***: *Authentication, Authorization, and Access Control*
10/26/13 Regular Season: Game #2 **(Prerequisite: Mandatory Pre-Season and Regular Season Game #1)**
-**Chapter 11**: Basic Cryptography --***Lab 16***: *General Cryptography Concepts*
-**Chapter 12**: Advanced Cryptography --***Lab 14***: *Importance of Data Security - Securing Data Using Encryption Software*
11/09/13 Post Season: NCL Conference Championship **(Prerequisite: Mandatory Pre-Season and Regular Season Games 1 & 2)**
-**Chapter 13**: Business Continuity
-**Chapter 14**: Risk Mitigation --***Lab 6***: *Incident Response Procedures (Tasks 2-3)*
11/16/13 Post Season: NCL National Championship **(Prerequisite: Mandatory Pre-Season, Regular Season Games 1 & 2, and NCL Conference Championship)**