The National Cyber League – Where Cybersecurity is a Passion

National Cyber League
EC-Council Certified Ethical Hacker (CEH)™ Syllabus

Note to Faculty

This NCL Syllabus is intended as a supplement to courses that are based on the EC-Council Certified Ethical Hacker™ (CEHv8) 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) recently collaborated with the Center for Systems Security and Information Assurance (CSSIA) to create a series of lab exercises intended to support the EC-Council CEH 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 EC-Council CEH performance-based exam objectives, a widely recognized and adopted curriculum and certification (The 2013 NCL Fall Season also includes objectives for the Computing Technology Industry Association (CompTIA) Security+™).

Akin to conditioning in athletics, or practicing layups and free throws in the gym, the NCL will host 19 virtual preparatory CEH 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 EC-Council CEH 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

Code of Ethics

International Council of E-Commerce Consultants

From: https://www.eccouncil.org/ciso/becoming-cciso/code-of-ethics

This CODE OF ETHICS expresses the consensus of the profession on ethical issues and is a means to educate both the public and those who are entering the field about the ethical obligations of all e-commerce consultants. By joining EC-Council each member agrees to:

1. Keep private any confidential information gained in her/his professional work, (in particular as it pertains to client lists and client personal information). Not collect, give, sell, or transfer any personal information (such as name, e-mail address, Social Security number, or other unique identifier) to a third party without client prior consent.

2. Protect the intellectual property of others by relying on her/his own innovation and efforts, thus ensuring that all benefits vest with its originator.

3. Disclose to appropriate persons or authorities potential dangers to any e-commerce clients, the Internet community, or the public, that she/he reasonably believes to be associated with a particular set or type of electronic transactions or related software or hardware.

4. Provide service in their areas of competence, being honest and forthright about any limitations of her/his experience and education. Ensure that she/he is qualified for any project on which he/she works or proposes to work by an appropriate combination of education, training, and experience.

5. Never knowingly use software or process that is obtained or retained either illegally or unethically.

6. Not engage in deceptive financial practices such as bribery, double billing, or other improper financial practices.

7. Use the property of a client or employer only in ways properly authorized, and with the owner's knowledge and consent.

8. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

9. Ensure good management for any project he/she leads, including effective procedures for promotion of quality and full disclosure of risk.

10. Add to the knowledge of the e-commerce profession by constant study, share the lessons of her/his experience with fellow EC-Council members, and promote public awareness of benefits of electronic commerce.

11. Conduct herself/himself in the most ethical and competent manner when soliciting professional service or seeking employment, thus meriting confidence in her/his knowledge and integrity.

12. Ensure ethical conduct and professional care at all times on all professional assignments without prejudice.

13. Not associate with malicious hackers nor engage in any malicious activities.

14. Not purposefully compromise or cause to be compromised the client organization's systems in the course of your professional dealings.

15. Ensure all penetration testing activities are authorized and within legal limits.

16. Not partake in any black hat activity or be associated with any black hat community that serves to endanger networks.

17. Not be part of any underground hacking community for purposes of preaching and expanding black hat activities.

NCL Recommended Books

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

Official Certified Ethical Hacker Review Guide
Author: Steven DeFino
ISBN-10: **1435488539**
ISBN-13: **978-1435488533**

Hands-On Ethical Hacking and Network Defense, Second Edition
Author: Michael T. Simpson
ISBN-10: **1435486099**

Ethical Hacking & Countermeasures: Attack Phases
Author: EC-Council
ISBN-10: **143548360X**
ISBN-13: **978-1435483606**

Ethical Hacking and Countermeasures: Linux, Macintosh & Mobile Systems
ISBN-10: **1435483642**
ISBN-13: **978-1435483644**

Ethical Hacking & Countermeasures: Secure Network Infrastructures
Author: EC-Council
ISBN-10: **1435483650**
ISBN-13: **978-1435483651**

Ethical Hacking & Countermeasures: Threats & Defense Mechanisms
Author: EC-Council
ISBN-10: **1435483618**
ISBN-13: **978-1435483613**

Ethical Hacking & Countermeasures: Web Applications & Data Servers
Author: EC-Council
ISBN-10: **1435483626**
ISBN-13: **978-1435483620**

NCL Syllabus Topics

- Background knowledge needed for CEHv8
- Analysis and Assessment
- Security
- Tools/Systems/Programs
- Procedures/Methodology
- Regulation/Policy
- Ethics

The table below lists sections and content of the EC-Council CEH exam and the approximate extent to which they are represented in the exam: (from EC-Council http://www.eccouncil.org/Certification/exam-information/ceh-exam-312-50):

CEH Section	% of Exam	# of Questions
Background	4%	5
Analysis/Assessment	13%	16
Security	25%	31
Tools/Systems/Programs	32%	40
Procedures/Methodology	20%	25

Regulation/Policy	4%	5
Ethics	2%	3

The above-mentioned 7 sections include the following EC-Council CEH exam content knowledge:

- **Background**
  - Networking technologies
  - Web technologies (e.g. web 2.0, Skype)
  - Systems technologies
  - Communication protocols
  - Malware operations
  - Mobile technologies (e.g. smart phones)
  - Telecommunication technologies
  - Backups and archiving (e.g. local, network)

- **Analysis/Assessment**
  - Data analysis
  - Systems analysis
  - Risk assessments
  - Technical assessment methods

- **Security**
  - Systems security controls
  - Application / file server
  - Firewalls
  - Cryptography
  - Network security
  - Physical security
  - Threat modeling
  - Verification procedures (e.g. false positive / negative validation

- Social engineering (human factors manipulation)
- Vulnerability scanners
- Security policy implications
- Privacy / confidentiality (with regard to engagement)
- Biometrics
- Wireless access technology (e.g. networking, RFID, Bluetooth)
- Trusted networks
- Vulnerabilities

- **Tools/Systems/Programs**
  - Network- / host- based intrusion
  - Network / wireless sniffers (e.g. Wireshark, Airsnort)
  - Access control mechanisms (e.g. smartcards)
  - Cryptography techniques (e.g. IPsec, SSL ,PGP)
  - Programming languages (e.g. C++, Java, C#, C)
  - Scripting languages (e.g. PHP, Java script)
  - Boundary protection appliances (e.g. DMZ)
  - Network topologies
  - Subnetting
  - Port Scanning (e.g. NMAP)
  - Domain name system (DNS)
  - Routers / modems / switches
  - Vulnerability scanner (e.g. Nessus, Retina)
  - Vulnerability management and protection systems (e.g. Foundstone, Ecora)
  - Operating environments (e.g. Linux, Windows, Mac)
  - Antivirus systems and programs
  - Log analysis tools
  - Security models
  - Exploitation tools
  - Database structures

- **Procedures/Methodology**
  - Cryptography
  - Public Key Infrastructure (PKI)
  - Security Architecture (SA)
  - Service Oriented Architecture (SOA)
  - Information security incident management
  - N-Tier application design
  - TCP/IP networking (e.g. network routing)
  - Security testing methodology

- **Regulation/Policy**
  - Security policies
  - Compliance regulations (e.g. PCI)

- **Ethics**
  - Professional code of conduct
  - Appropriateness of hacking activities

Lab Exercises

There are 19 remote lab exercises designed to:

- Reinforce the concepts covered in the EC-Council CEH content knowledge with hands-on activities
- Help prepare students for the NCL games
- Help students prepare for the EC-Council CEH professional exam
- Provide supplemental lab exercises for faculty teaching CEH and related course(s) and content

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

Lab 1: Using Active and Passive Techniques to Enumerate Network Hosts

- Introduction to Ethical Hacking
- Scanning Networks
- Enumeration
- Sniffers

Lab 2: Conducting Active and Passive Reconnaissance Against a Target

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Social Engineering

Lab 3: Using the SYSTEM account

- System Hacking

Lab 4: Poison Ivy – Remote Access Trojan

- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 5: Using the SHARK Remote Administration Tool

- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 6: Utilizing Malware - Dark Comet

- System Hacking
- Trojans and Backdoors
- Viruses and Worms

Lab 7: Breaking Windows Passwords

- System Hacking

Lab 8: Using John the Ripper to Crack Linux Passwords

- System Hacking

Lab 9: Using Spear Phishing to Target an Organization

- System Hacking
- Social Engineering
- Session Hijacking

Lab 10: Breaking WEP and WPA Encryption

- Hacking Wireless Networks

Lab 11: Using Metasploit to Attack a Remote System

- Scanning Networks
- Enumeration
- Sniffers
- Evading IDS, Firewalls, and Honeypots

Lab 12: Using Armitage to Attack the Network

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- System Hacking
- Penetration Testing

Lab 13: Exploitation with IPv6

- System Hacking

Lab 14: Creating MSFPAYLOADS

- System Hacking
- Trojans and Backdoors
- Viruses and Worms
- Penetration Testing

Lab 15: Abusing SYSTEMS

- Denial of Service

Lab 16: SQL Injection

- Hacking Webservers
- Hacking Web Applications
- SQL Injection

Lab 17: Launching a Buffer Overflow

- System Hacking
- Buffer Overflow

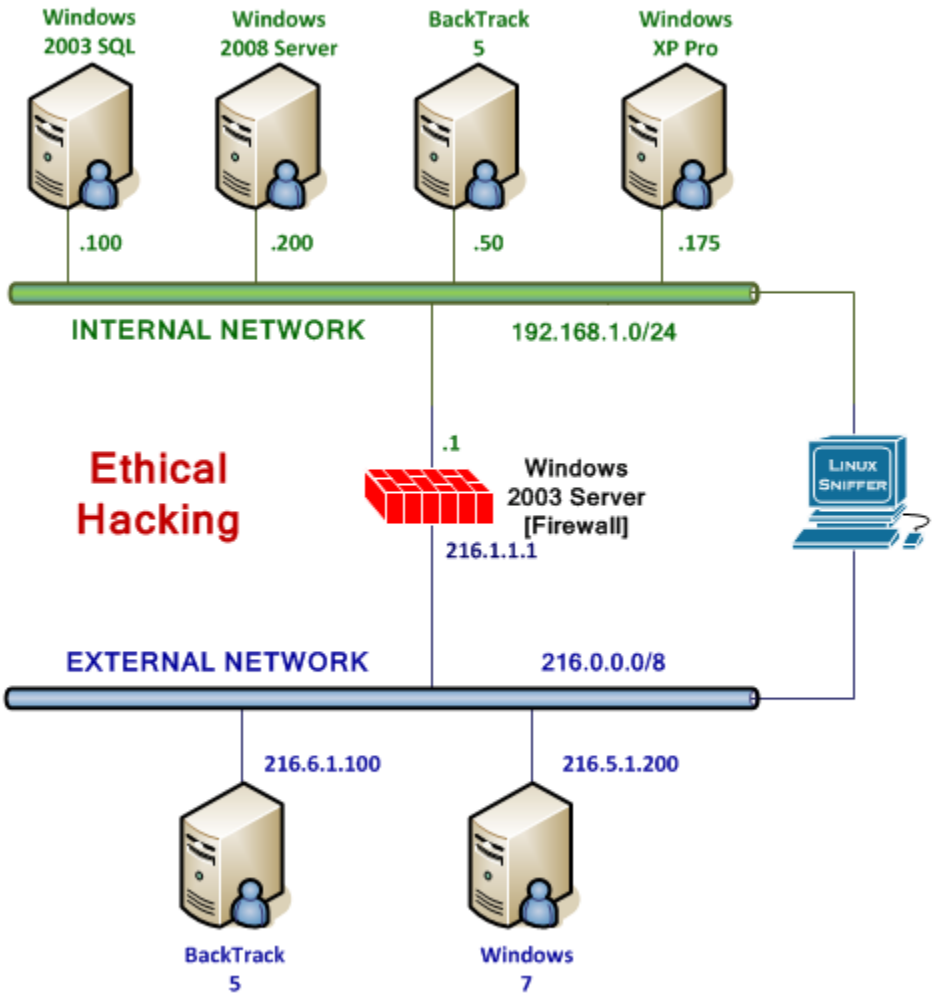
Lab 18: Intrusion Detection

- Evading IDS, Firewalls, and Honeypots

Lab 19: Using Certificates to Encrypt Email

- Cryptography

Lab Topology for Virtual Lab Exercises (available in the NCL Cyber Gymnasiums)



(From http://www.netdevgroup.com/content/cybersecurity/labs/ethical_hacking.html)

Suggested Schedule

The following suggested schedule maps the *Official Certified Ethical Hacker Review Guide* chapters with the corresponding NCL lab exercise(s) and NCL Games.

Faculty are encouraged to supplement with the more comprehensive information in the five EC-Council CEH textbooks:

Suggested Schedule (game dates subject to change)
Chapter 1: Ethical Hacking Basics
Chapter 3: Reconnaissance Information Gathering for the Ethical Hacker • **Lab 2:** Conducting Active and Passive Reconnaissance Against a Target -- Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, Social Engineering • **Lab 12:** Using Armitage to Attack the Network -- Introduction to Ethical Hacking, Footprinting and Reconnaissance, Scanning Networks, System Hacking, Penetration Testing
Chapter 4: Scanning and Enumeration • **Lab 1:** Using Active and Passive Techniques to Enumerate Network Hosts -- Introduction to Ethical Hacking, Scanning Networks, Enumeration, Sniffers • **Lab 11:** Using Metasploit to Attack a Remote System -- Scanning Networks, Enumeration, Sniffers, Evading IDS, Firewalls, and Honeypots
Chapter 5: Hacking Through the Network Sniffers and Evasion
Chapter 6: Attacking a System • **Lab 3:** Using the SYSTEM account -- System Hacking • **Lab 18:** Intrusion Detection -- Evading IDS, Firewalls, and Honeypots
Chapter 8: Web-Based Hacking Servers and Applications

- **Lab 13:** Exploitation with IPv6 -- System Hacking
- **Lab 15:** Abusing SYSTEMS -- Denial of Service
- **Lab 16:** SQL Injection -- Hacking Webservers, Hacking Web Applications, SQL Injection
- **Lab 17:** Launching a Buffer Overflow-- System Hacking, Buffer Overflow

10/19/13 Regular Season: Game #1
(Prerequisite: Mandatory Pre-Season 10/07-10/13)

Chapter 2: Cryptography 101

- **Lab 7:** Breaking Windows Passwords -- System Hacking
- **Lab 8:** Using John the Ripper to Crack Linux Passwords -- System Hacking
- **Lab 19:** Using Certificates to Encrypt Email -- Cryptography

Chapter 9: Wireless Networking Hacking

- **Lab 10:** Breaking WEP and WPA Encryption -- Hacking Wireless Networks

10/26/13 Regular Season: Game #2
(Prerequisite: Mandatory Pre-Season and Regular Season Game #1)

-**Chapter 10**: Trojans and Other Attacks

- **Lab 4:** Poison Ivy (Remote Access Trojan) -- System Hacking, Trojans and Backdoors, Viruses and Worms
- **Lab 5:** Using the SHARK Remote Administration Tool -- System Hacking, Trojans and Backdoors, Viruses and Worms
- **Lab 6:** Utilizing Malware (Dark Comet) -- System Hacking, Trojans and Backdoors, Viruses and Worms
- **Lab 14:** Creating MSFPAYLOADS -- System Hacking, Trojans and Backdoors, Viruses and Worms, Penetration Testing

-**Chapter 7**: Low Tech: Social Engineering and Physical Security

- **Lab 9:** Using Spear Phishing to Target an Organization -- System Hacking, Social Engineering, Session Hijacking

11/09/13 Post Season: NCL Conference Championship **(Prerequisite: Mandatory Pre-Season and Regular Season Games 1 & 2)**
11/16/13 Post Season: NCL National Championship **(Prerequisite: Mandatory Pre-Season, Regular Season Games 1 & 2, and NCL Conference Championship)**