Network Vulnerability Assessment and Risk Mitigation (3-2)

**Course Goal:** This course is designed to involve you directly with the methodologies and techniques used for vulnerability assessments and follow on mitigation. These methodologies will be reviewed in-depth as they are applied from the vantage point of an evil hacker. Common vulnerabilities will also be studied. Lab exercises will be used to improve your detailed knowledge of security threats and the methods used to exploit them, leading you to knowledge of the methodologies and motives used by those who will attack the networks you may someday have to defend.

**Learning Outcomes:** Upon successful completion of this course, you will be able to:

- Describe the methodology used to assess the vulnerability of an organization connected to the Internet, to include:
  - Footprinting
  - Scanning
  - Enumerating
  - Gaining Access
  - Escalating Privileges
  - Pilfering
  - Covering Tracks
  - Creating Back Doors
  - Denials of Service
- Employ the common tools of the trade used during the assessment and in mitigation.
- Define and describe current types of vulnerabilities, how they leave an organization open to a threat, and how to protect against them.
- Use a distribution of Linux to compile new tools and use such applications as `vi` and `nmap`.
- Explain why hackers hack (their motivations), the different types of hackers, and some of the history of hackers and their exploits.
- Complete an assessment of the lab network, to include a full mapping of the network, vulnerabilities that lie therein, and exploits that could be used to threaten the network.

**Course Format:** This course is designed so that the majority of the resources used in the teaching of the course will be supplied from the EC Council's Certified Ethical Hacking materials, as well as supplemental materials delivered online. These resources will be supplemented with discussions in class and videos with key subject matter experts in the field. You will be expected to have read assigned readings ahead of class time, as some of the lectures will have an open-forum style, where key questions on the reading will be discussed and class participation evaluated. Your preparation time will averages two to four hours per week, mostly reading assignments, with some additional time (up to thee or four hours per week) required for the lab projects.

**Textbook:** EC Council's Certified Ethical Hacker (CEH) Courseware, currently in its eighth edition. Additional readings will be posted to the Sakai site or distributed in class. Course organization on the Sakai site will be reviewed during the first class meeting. Specifically, we will explore where these course documents can be found as well as the tools that you will be expected to use on the site.

A weekly schedule is on the next page.
**Weekly Schedule:**

<table>
<thead>
<tr>
<th>Week</th>
<th>Module</th>
<th>Lab</th>
</tr>
</thead>
</table>
| 1    | 1-Introduction  
2-Hacking Laws  
22-Linux Hacking | 01-04 Hacking for Dummies  
01-06 Ethical Hacking  
01-NPS01 Lock-picking  
01-NPS02 Remote Lab Access  
01-NPS03 Intro to DOS Commands  
02-01 Visit the US Cybercrime Website  
22-NPS01 Introduction to Linux |
| 2    | 3-Footprinting  
4-Google Hacking | 03-NPS01 Footprint a Target  
04-04 Internet_for_Research.pdf |
| 3    | 5-Scanning | 05-NPS01 Scanning |
| 4    | 6-Enumeration | 06-NPS-1 Enumeration |
| 5    | Catch up | 01-NPS03 Intro to DOS Commands  
05-NPS01 Scanning  
06-NPS01 Enumeration |
| 6    | 7-System Hacking | Lab 07-NPS01 Gaining Access NAT10  
Lab 07-NPS02 Remote Applications  
  - 07-15 Alchemy Remote Executor Tool  
  - 07-02 PwDump3  
Lab07-NPS03 Password Cracking:  
  - 07-08 LCP  
Lab 07-NPS04 (AG) Hiding Files:  
  - 07-11 NTFS Streams  
  - 07-13 NTFS ADS Spy  
  - 07-25 Masker Steganography Tool  
  - 07-28 SNOW Steganography Tool |
| 7    | 8-Trojans & Back Doors  
9-Viruses & Worms  
10-Sniffers  
11-Social Engineering | 10-NPS01 ARP Poisoning |
| 8    | 14-Denial of Service  
15-Session Hijacking  
16-Hacking Web Servers | 15-NPS01 Session Hijacking  
16-NPS01 IIS Traversal |
| 9    | 17-Web Apps  
18-Password Cracking  
19-SQL Injections  
24-Buffer Overflows | Lab 24-NPS01 Metasploit  
Final Project |
| 10   | 20-Wireless  
21-Physical Security  
13-Hacking Email | Final Project |
| 11   | Final Project | Final Project |