NORTH CAROLINA CENTRAL UNIVERSITY
SCHOOL OF LIBRARY AND INFORMATION SCIENCES

LSIS 5442-OL1 Network Security

FALL 2012

CLASS DATES:
Dates: 8/21, 8/28, 9/4, 9/11, 9/18, 9/25, 10/2, 10/9, 10/16, 10/23, 10/30, 11/6, 11/13, 11/20, 11/27, 12/4
Time: Tuesdays, 6:30PM-9:00PM
Online Course. Course content delivered via Blackboard and Blackboard Collaborate (formerly Elluminate) systems.

INSTRUCTOR: Gabriel Peterson, PhD
Office: 323 Shepard Library Building
Office hours: Monday and Wednesday 4:00-6:00 pm or by appointment
Phone: 530-6746
E-mail: gpeterson@nccu.edu

Class Website: Blackboard: https://nccu.blackboard.com/

Course Description:
The fundamental concepts of network security will be addressed. Topics include cryptography, encryption, authentication, denial-of-service attacks, worms, viruses, intrusion detection, firewalls, virtual private network, web security, and access control of the network systems. Practical application of security analysis tools is emphasized.

Students Learning Outcomes:
Upon completion of SLIS 5442, students will be able to:

- Analyze security vulnerabilities in computer systems and
- Identify and deploy the appropriate defense of such weaknesses.
- Utilize modern security tools and the Linux operating system.
- Specify primary areas of network defense
- Demonstrate the defense of networks and network equipment
- Use information security tools, deploy them, collect & analyze data and demonstrate competency by securing a computer network.
Course introduction:
This course is intended to give students a practical understanding of the tools and skills required of a network security analyst. Such tools are often perceived by networks (and their administrators) as being security threats. Hence, it is vital that you obtain permission to do any network analysis. (Thus, it is best to use your home network environment, assuming you have a few nodes and Wi-Fi.)

Network security tools used by professionals are typically Unix or Linux-based. Though we will also examine their Windows-based analogs, the preferred operating system for servers and multi-user environments is Unix/Linux, so you must know how to use the tools appropriate to the environment you are likely to find when working. You must therefore start using Linux, either as an installed operating system it as a live boot CD or USB drive. (If you cannot make a live boot USB or CD, please let me know and I will provide one for you.)

Go here for information about obtaining and installing Ubuntu for your laptop. [http://www.ubuntu.com/download/help/create-a-usb-stick-on-windows](http://www.ubuntu.com/download/help/create-a-usb-stick-on-windows)

I suggest version 12.04. (Remember to get the one appropriate to your architecture – when in doubt, choose the 32-bit x86 offering.)

I strongly recommend that you install Linux on a secondary laptop or acquire a fresh hard drive for your laptop and cleanly install a dual boot system. You may use a live boot USB drive, but it is not the preferred approach. (live USB is deprecated because you will need to learn how to install and make permanent changes on it as well as learning Linux; it’s an added layer of complexity that, unless you are already experienced, you don’t really need.) Alternatively, you may opt to use the free VirtualBox technology.

COURSE REQUIREMENTS:
Required Textbook/ readings:
- Inside Cyber-Warfare By Jeffrey Carr  
  O’Reilly Publishing  
  ISBN-10: 0596802153

- Secrets and Lies by Bruce Schneier  
  Wiley publishing, inc.  
  ISBN-10: 0471453803

- Network Security Bible by Eric Cole  
  Publisher: Wiley; 2 edition (September 8, 2009)  

OTHER READINGS AS ASSIGNED (Documents will be available on Blackboard)

REQUIRED TECHNOLOGY
You must have the following installed and operational by the first class session.

- Hardware: A computer with a microphone and Internet access
- Course materials and communication are hosted and distributed online using the campus Blackboard system ([https://nccu.blackboard.com/](https://nccu.blackboard.com/)). Please login and (if you are unfamiliar with Blackboard), work through the orientation/tutorial.
● Blackboard Collaborate is web/Java based, so you will not need to install Blackboard Collaborate software. Instead you will access Blackboard Collaborate by directing your Java-enabled browser to the Blackboard Collaborate website, [http://www.blackboard.com/Platforms/Collaborate/Overview.aspx](http://www.blackboard.com/Platforms/Collaborate/Overview.aspx)

**Hardware requirements:**
In order to use the technology that underpins this class you must have (at the minimum)

● A laptop equipped with wireless internet capability
● A blank USB drive, minimum size 4Gb, formatted as FAT32

**Software requirements**
● A distribution of Linux installed or available via live boot USB or DVD
● Firefox with Java 6

**The student will:**

Complete all assigned readings prior to class.
Complete all assignments on time. No late assignments will be accepted without the instructor’s knowledge.
Demonstrate increasing understanding and comfort with network security fundamental concepts

**PERFORMANCE EVALUATION**
Student’s performance will be evaluated based on the following course requirements. Academic dishonesty in any form will result in a grade of “F” for the assignment or exam in which it was demonstrated.

<table>
<thead>
<tr>
<th>Assignments/ tests</th>
<th>Due</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Assignment 1 (VirtualBox)</td>
<td>8/28</td>
<td>10%</td>
</tr>
<tr>
<td>2) Assignment 2 (Linux)</td>
<td>9/4</td>
<td>10%</td>
</tr>
<tr>
<td>3) Quiz 1</td>
<td>9/18</td>
<td>10%</td>
</tr>
<tr>
<td>4) Assignment 3(Traceroute/Tor)</td>
<td>9/25</td>
<td>10%</td>
</tr>
<tr>
<td>5) Assignment 4 (nmap/zenmap)</td>
<td>10/9</td>
<td>10%</td>
</tr>
<tr>
<td>6) Quiz 2</td>
<td>10/23</td>
<td>10%</td>
</tr>
<tr>
<td>7) Assignment 5(Wireshark)</td>
<td>11/6</td>
<td>10%</td>
</tr>
<tr>
<td>8) Assignment 6 (snort/IDS)</td>
<td>11/27</td>
<td>10%</td>
</tr>
<tr>
<td>7) Final Exam</td>
<td>12/11</td>
<td>20%</td>
</tr>
</tbody>
</table>

**Grading Scales:**
Points totals converted to letter grades:

<table>
<thead>
<tr>
<th>A</th>
<th>90-100</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>80-89</td>
</tr>
<tr>
<td>C</td>
<td>70-79</td>
</tr>
<tr>
<td>F</td>
<td>Below 70</td>
</tr>
</tbody>
</table>
Student Support Services for Students with Disabilities

Students with disabilities (physical, psychological, learning disability, etc.) who would like to request accommodations need to register with the Office of Student Support Services in Suite G20 in the Student Services Building or by contacting Kesha Lee, Director at (919)530-6325 or klee@nccu.edu. If you are already registered in the office, you will need to return to the office each semester to review your information and receive updated accommodations.

POLICIES

- **Attendance:** This class is held online in weekly live sessions via Elluminate. (www.elluminate.com) Participation in these weekly sessions is required. Attendance will be taken in each class session; University attendance policies apply.

- **Communication:** Course materials and announcements will be distributed on Blackboard. In order to communicate with the instructor properly, a student should use email registered on Blackboard. If you have any problems with this, please contact me during the first week of the semester. I will be communicating with you via Blackboard as well as email.

- **Submissions:** Exams and assignments will be hosted and distributed on Blackboard. (https://nccu.blackboard.com/). All student work must be submitted by the due date specified in the syllabus to the Assignments section of the Blackboard course shell. No submissions will be accepted via email.

- **Due dates:** All assignments MUST be received by the indicated due dates. Late assignments will NOT be accepted unless prior arrangements were made based on a proper reason.

- **Incomplete grade policy:** An incomplete may be given at the instructor’s discretion only when small portion of the course requirements are not completed due to some problems which are beyond your control but could be fully justified by documents (e.g., serious illness, family emergency) and when the student has notified the instructor before the deadline for filing final grades.

- **A grade of “I” requires a plan of action with a timeline & remaining assignments required to complete the student grade in a timely manner (within one year), otherwise the grade of “I” will convert to a permanent grade of “F”.

- **Plagiarism:**
  - NCCU and the School of Library and Information Sciences do not tolerate any form of cheating or plagiarism.
As a graduate student, you should know what cheating and plagiarism are, but if you are not sure about what constitutes cheating or plagiarism, see the following resources:

- Georgetown University ([http://gervaseprograms.georgetown.edu/hc/plagiarism.html](http://gervaseprograms.georgetown.edu/hc/plagiarism.html))
- Purdue University ([http://owl.english.purdue.edu/handouts/print/research/r_plagiar.html](http://owl.english.purdue.edu/handouts/print/research/r_plagiar.html))

At the least, plagiarism will earn you an F or a zero on the assignment. It may earn you an F in the course or even lead to your dismissal from the University.

---

**SCHEDULE**

**Weekly Readings & Assignments**

<table>
<thead>
<tr>
<th>Date</th>
<th>Plan &amp; Readings</th>
</tr>
</thead>
</table>
| 8/21  | Topic: Part 1, Introduction  
Read:  
- The Network Security Bible, Ch 1  
- Secrets and Lies, Part 1  
Assignment #1: VirtualBox |
| 8/28  | Topic: Linux, Virtual Machines  
Read:  
- The Network Security Bible, Ch 2-3  
- Secrets and Lies, Part 2  
Assignment #2: Linux Fundamentals  
Due: Assignment #1 – VirtualBox (Submit to Blackboard) |
| 9/4   | Topic: Part 2.1 – Security principles & management  
Read:  
- The Network Security Bible, Ch 4-5  
- Secrets and Lies, Part 3  
Due: Assignment #2: Linux Fundamentals (Submit to Blackboard) |
| 9/11  | Topic: Part 2.2 – Access control  
Read:  
- The Network Security Bible, Ch 6 & 7 |
<p>| 9/18  | Quiz #1 – Available on Blackboard. Due by 6PM 9/25 |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Reading</th>
<th>Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/25</td>
<td>Part 3.1 – Web &amp; system security</td>
<td>• <strong>The Network Security Bible</strong>, Ch 8-11</td>
<td>Assignment #3: Traceroute/Tor (Submit to Blackboard)</td>
</tr>
<tr>
<td>10/2</td>
<td>3.2 Server security &amp; the DNS</td>
<td>• <strong>The Network Security Bible</strong>, Ch 12-14</td>
<td></td>
</tr>
<tr>
<td>10/9</td>
<td>4.1 Networks</td>
<td>• <strong>The Network Security Bible</strong>, Ch 15-16</td>
<td>Due: Assignment #3: Anonymization: Traceroute//Tor (Submit to Blackboard)</td>
</tr>
<tr>
<td>10/16</td>
<td>4.2 Firewalls &amp; intrusion Detection</td>
<td>• <strong>The Network Security Bible</strong>, Ch 17-19</td>
<td>Assignment #4: nmap/zenmap (Submit to Blackboard)</td>
</tr>
<tr>
<td>10/23</td>
<td>Quiz #2 – Available on Blackboard. <strong>Due by 6PM 10/24</strong></td>
<td></td>
<td>Due: Assignment #4: nmap/zenmap (Submit to Blackboard)</td>
</tr>
<tr>
<td>10/30</td>
<td>Part 5 – Secure Communication</td>
<td>• <strong>The Network Security Bible</strong>, Ch 20-22</td>
<td>Assignment #5: Wireshark (Submit to Blackboard)</td>
</tr>
<tr>
<td>11/13</td>
<td>Part 7.1 – Integrated Cyber Security</td>
<td>• <strong>Inside Cyber-Warfare</strong> Chapters 3-4</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/20</td>
<td>No Class - Thanksgiving Holiday</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Read:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● The Network Security Bible, Ch 26-27</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Inside Cyber-Warfare Chapters 5-6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12/4</td>
<td>Final Exam - Quiz #2 – Available on Blackboard. Due by 6PM 12/6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ASSIGNMENTS:**

Each of these assignments requires that you use software that some systems will find hostile. You MUST use your own network or one where you have explicit permission from the administrator to use these tools.

Each of these tools requires that you download, install and configure it and then learn how to execute with appropriate syntax. Man pages and online documentation will be essential. In each case, you are responsible for producing relevant output that can be analyzed and explained. Error messages and “no response” output are not acceptable. Results should be saved as screenshots or text and then explained in a well-written analysis of 250-500 words.

**SUBMISSIONS:** Results should be uploaded to the “Assignments” section of the Blackboard system.

Each assignment has 3 components:

1. In your own words, describe what the program does and why you (a security analyst) would use it. That is, what information does it provide you, and under what circumstances would you select the tool.

2. Download, install, run and collect useful output from the program or programs listed in the assignment. Save output as text or screenshots, as appropriate.

3. Interpret your findings. Describe the meanings of all of the output. What information is being provided by the program and what do the data indicate?

**CRITERIA:**
Points are awarded proportionally for each component of the exercise. If you successfully describe, collect and interpret data, you will receive full credit. Submit all assignments to Blackboard.

Assignment #1: VirtualBox
1. Download a copy of Ubuntu 12.04 and create a live boot USB drive. Instructions are available from: http://www.ubuntu.com/download/help/create-a-usb-stick-on-windows
2. In Windows (or whatever system you are using) download and install VirtualBox and install Ubuntu 12.04 inside VirtualBox.

Assignment #2: Linux Fundamentals
1. Learn how to “pipe” command line output to a text file
2. Create a new user & password in Linux
3. Create a group called security
4. Add the new user to the security group
5. Download and install the program TrueCrypt (http://www.truecrypt.org/)
6. Create an encrypted file in the new user’s home directory

Assignment #3: Traceroute/Tor
1. Use the “ping” command on www.example.com
2. Use the “Traceroute” command on www.example.com
3. Install the Tor browser (Available from: https://www.torproject.org/)

Assignment #4: nmap/zenmap
1. Download and install the program zenmap (http://nmap.org/zenmap/)
2. Run zenmap, save the data and interpret the findings

Assignment #5: Wireless security/wireshark
1. Download and install the program wireshark (http://www.wireshark.org/)
2. Run wireshark, save the data and interpret the findings

Assignment #6: Intrusion detection/snort
1. Download and install the program wireshark (http://www.snort.org/)
2. Run snort, save the data and interpret the findings