Class : W 5:45 – 9:00 P.M.
Instructor : Dr. Anthony Chung
Office : CDM 844
Office Hours : Tu W 3:15-4:45 PM / Other times by appointment
.

Phone : (312)-362-8724
Fax : (312)-362-6116

Email : achung@cdm.depaul.edu

While email is a great means of communication, increasingly we are bombarded with a volume of emails that is getting difficult to manage. Please observe the following email etiquette so that we will be able to better focus our energy on learning and getting the most out of the class. It is also part of being professional. Some recruiters were abhorred at some of the emails received from recent recruits. It is important to form the good habit of writing appropriate emails in a professional setting.

- Under normal situation I will respond within two business days. Therefore work on your assignments early so as to give you ample time to ask questions. If I do not respond within the normal time frame, it's properly because one or more of the following etiquettes is not followed.

- Expect lab assistants to respond only during posted lab hours.

- Before sending questions via email or posting questions on the d2l discussion forum, make sure that your question is not already answered on the course syllabus, the d2l website (announcements, discussion forums, assignment information etc), or in the lecture (view the class recording if you missed a class, or if you are an OL student).

- Questions that are of general interest to the entire class should be posted on the course discussion forum.

- Be specific about the subject of the email in the mail subject heading and use proper spelling, grammar, and punctuation. Include course number in the subject. Please don't respond to an old email with a different subject when asking a new question.

- Include your full name in the message body.

- While you have my permission to address me as Anthony or Tony, you should not assume that you can address other professors on a first name basis unless you have their explicit permissions.

Course Home Page : https://d2l.depaul.edu (Open on or before March 25,2016)

Prerequisites: **TDC 477**
Note: This is a STRONG prerequisite, Students are expected to have a good knowledge of fundamental network security concepts

and the TCP/IP protocols; and configurations of routers, basic firewalls, and basic VPNs.

Required Text: There's no required text for this course

Optional Text: They are listed in the schedule below for each topic.
They are all available on DePaul's E-Library – Safari, or on the web.

The following three books are referred to the most.

- **TDC 477 text: CCNA Security 210-260 Official Cert Guide,** Santos & Stuppi, Cisco Press/Pearson, 2015. ISBN: 978-1587205668
- **LAN Switch Security – What Hackers Know About Your Switches** by Eric Vyncke and Christopher Paggen
- **Router Security Strategies: Securing IP Network Traffic Planes** by Gregg Schudel and David J. Smith

Reference:

Textbooks from TDC 463.

Course Description and Objective:

This course is an advanced class in network security. Topics include: Advanced Firewall Architecture, Network Security Auditing; Intrusion Detection and Prevention Systems; Incident Response; Honeypots; Network Infrastructure and Protocol Security: and Security Information Management.

Grading

3 Homework Assignments		**15%**
Lab Assignments (Performed on DL Pods or in Network Security Lab, except for Lab 3)		**24%**
Lab 1 – VPN as backup to T1 line	4%	
Lab 2 – Firewall failover	4%	
Lab 3 – Snort (Performed on students' own computers)	8%	
Lab 4 – Policy routing	4%	
Lab 5 – BGP AS Path attributes	4%	
PT Activities (Performed Using Packet Tracer on students own devices)		**8%**
PT Activity 1 – Layer 2 security	2%	
PT Activity 2 – Syslog, NTP, SSH	2%	
PT Activity 3 – AAA	2%	

PT Activity 4 – Comprehensive	2%	
Midterm		**20%**
Final Paper		**15%**
Class Participation		**18%**

Note: A student must score 60% or more in the midterm to pass this course.
The following scale is applied if the above condition is met, otherwise a grade of F will be assigned.

A	90-100%
A-	87-89%
B+	84-86%
B	80-83%
B-	77-79%
C+	74-76%
C	70-73%
C-	67-69%
D+	64-66%
D	60-63%
F	< 60%

Students at or above the class average (calculated from grades 60% or above) will receive at least a A-. I will modify the grading scale if the class average is below 87%.

Notes:

- **Changes to Syllabus:** This syllabus is subject to change as necessary during the quarter. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L and sent via email.

- **Late assignments will not be accepted.** I am strict about this. Homework solutions are available right after a homework is due and I cannot accept any assignments submitted after that. **All due dates and time are given in the dropboxes.** Please check the schedule and be sure of the due dates. You must use the homework submission system (drop box) through d2l. If there are problems with the submission system, you may email me a copy of the assignment BEFORE the due time.

- Class attendance is essential as lectures may cover topics outside the readings. **Attendance is expected** for this class. To earn the full participation point for each class you **must be in class for the entire duration, participate in activities such as in class exercises, occasional quizzes, discussions, and be fully engaged. Engaging in activities not related to the class, such as (but not limited to) texting/emailing during the class, or working on assignments from another class, will result in lowered participation grade.** Also if there's a **documentable** and **acceptable** reason

(such as being sick with a doctor's slip, or a note from your manager about work responsibility), make up for the participation points can be considered. **5 points** are assigned for each class with a maximum of **18 pts** total.

- Any grading questions **must be directed to me within 1 week of the posting of the grade. No grade adjustments will be made more than a week after the grade is posted. You should email me with the following information:**
  - **The assignment**
  - **The problem in question**
  - **Why you think you should get a grade rather than the one given.**
- **Wireless Internet Access Policy:** Please **do not** work on your laptops / Internet during class **except for course related activities**. If you need to do something un-related to the class, please leave the room and complete what you need to do.
- Please check DePaul's academic calendar http://oaa.depaul.edu/what/calendar.jsp for important dates such as last day to add/drop/withdraw from classes.
- **Please make sure that you read and understand DePaul's academic integrity policy: http://academicintegrity.depaul.edu/AcademicIntegrityPolicy.pdf For additional resources concerning academic quality, please check here: http://academicintegrity.depaul.edu/Resources/index.html All assignments are individual assignments. You should not work so close with another student as to produce solutions that are identical or almost identical.**
  - **Under no circumstances should you copy or use simple paraphasing of someone else's work without giving proper credits and references.**
  - **Please be aware that any written work submitted in this course may be verified using *Turn-It-In* technology in order to ensure that the work is the student's own creation and not in violation of the University's Academic Integrity Policy. Submission of work in this course constitutes a pledge that the work is original and consent to have the work submitted to verify that fact.**

- **Student Attitude:** A professional and academic attitude is expected throughout this course. Measurable examples of non-academic or unprofessional attitude include but are not limited to: talking to others when the instructor is speaking, mocking another's opinion, cell phones ringing, emailing, texting or using the internet whether on a phone or computer. If any issues arise a student may be asked to leave the classroom. The professor will work with the Dean of Students Office to navigate such student issues.

- **Civil Discourse:** DePaul University is a community that thrives on open discourse that challenges students, both intellectually and personally, to be Socially Responsible Leaders. It is the expectation that all dialogue in this course is civil and respectful of the dignity of each student. Any instances of disrespect or hostility can jeopardize a student's ability to be successful in the course. The professor will partner with the Dean of Students Office to assist in managing such issues.

- **Cell Phones/On Call:** If you bring a cell phone to class, it must be off or set to a silent mode. If you are required to be on call as part of your job, please advise me at the start of the course.

Schedule (Tentative):

Date	Topic	Readings	Assignments
3-30	Class overview; TDC 477 Review. Vulnerability Scan, Nessus.	Nessus Documentation https://docs.tenable.com/nessus/index.htm About Network Taps: • http://en.wikipedia.org/wiki/Network_tap#Companies_making_network_TAPs • http://www.lovemytool.com/blog/2007/08/span-ports-or-t.html ARP poisoning/spoofing tools: http://en.wikipedia.org/wiki/ARP_spoofing National Vulnerability Database: http://nvd.nist.gov/	
4-6	High availability FW architecture IDS/IPS (I)	**Chapter 17, Santos and Stuppi** **Network Intrusion Detection**, 3rd edition, Northcutt & Novak, Prentice Hall/SAMS – ISBN: 0735712654 (Available on Safari) https://www.snort.org/documents An example IDS load balancer: http://docs.citrix.com/en-us/netscaler/11/traffic-management/load-balancing/load-balancing-ids-servers.html Examples of free host-based IDSs http://www.ossec.net/ Patriot NG: http://www.security-projects.com/?Patriot_NG Open Source Tripwire: http://sourceforge.net/projects/tripwire/ (only monitors file changes)	**Non-graded assignments due (Prereq Assessment, academic integrity pledge and security tool usage agreement, and posting of self-introduction on discussion forum)** **HW #1 due**
4-13	IDS/IPS (II)	Mixing Wheat with the Chaff: Creating Useful Test Data for IDS Evaluation http://www2.computer.org/portal/web/csdl/doi/10.1109/MSP.2007.92	**Lab #1 due** **Final Research Paper Proposal due**

		Severity metric example: http://msisac.cisecurity.org/alert-level/	
4-20	Honeypots	http://honeynet.org Infoworld Article - "No honeyport? Don't bother calling yourself a security pro" http://www.infoworld.com/d/security/no-honeypot-dont-bother-calling-yourself-security-pro-216038 **Honeypot for Windows** Roger A. Grimes (Available on books 24X7) Policy based routing Configuring Policy-Based Routing Configuring IP Access Lists Google Hack Database (GHDB) original site: http://www.hackersforcharity.org/ghdb/?function=summary&cat=19 GHDB current site: http://www.exploit-db.com/google-dorks/ Google Hack Honeypot (GHH): http://ghh.sourceforge.net/userfaq.php	**Lab #2 due**
4-27	**No Class (I will be attending a conference out of the country)**		
5-4	Securing Switches	**LAN Switch Security – What Hackers Know About Your Switches** by Eric Vyncke and Christopher Paggen (available on Safari) About VTP: http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml	**Lab #3 due** **HW #2 due**
5-11	**Midterm**		
5-18	Securing Routers	**Router Security Strategies: Securing IP Network Traffic Planes** by Gregg Schudel and David J. Smith (available on Safari)	**Lab #4 due** **PT Activity 1 due**

		NSA Router Security Configuration Guide and Supplement http://www.nsa.gov/ia/_files/routers/C4-040R-02.pdf http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf Cisco Security Center: http://tools.cisco.com/security/center/serviceProviders.x?i=76	
5-25	BGP Security	**Chapters 8 and 9 in CCNP: Building Scalable Cisco Internetworks Study Guide (Exam 642-801)** by Carl Timm and Wade Edwards (available on Books 24X7) Cisco BGP case studies A survey of BGP Security http://ix.cs.uoregon.edu/~butler/pubs/bgpsurvey.pdf BGP community example and application: http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a00801475b2.shtml	**PT Activity 2 due** **PT Activity 3 due**
6-1	DNS Security	DNS Cache Poisoning http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html DNSSEC resources: http://www.internetsociety.org/deploy360/dnssec/?gclid=CNfAyejdzcsCFYGFaQod6j4HeQ	**Lab #5 due** **HW #3 due**
6-8	Security Information and Event Management (SIEM) Guest speaker /other topic	OSSIM http://www.alienvault.com/open-threat-exchange/projects#ossim-tab A NetworkWorld article on SIEM: http://www.networkworld.com/news/tech/2011/081211-siem.html	**Final Research Paper due** **PT Activity 4 due** **Note that the OL participation for this class (6-8) is due earlier than usual on Monday 6-13.**

- **Participation assignments are usually due in a week except for the very last class. See dropbox for due dates and times.**

Online Instructor Evaluation

Evaluations are a way for students to provide valuable feedback regarding their instructor and the course. Detailed feedback will enable the instructor to continuously tailor teaching methods and course content to meet the learning goals of the course and the academic needs of the students. They are a requirement of the course and are key to continue to provide you with the highest

quality of teaching. The evaluations are anonymous; the instructor and administration do not track who entered what responses. A program is used to check if the student completed the evaluations, but the evaluation is completely separate from the student's identity. Since 100% participation is our goal, students are sent periodic reminders over two weeks. Students do not receive reminders once they complete the evaluation.

Email

Email is the primary means of communication between faculty and students enrolled in this course outside of class time. Students should be sure their email listed under "demographic information" at http://campusconnect.depaul.edu is correct.

Academic Integrity Policy

This course will be subject to the faculty council rules on the Academic Integrity Policy

Plagiarism

The university and school policy on plagiarism can be summarized as follows: Students in this course, as well as all other courses in which independent research or writing play a vital part in the course requirements, should be aware of the strong sanctions that can be imposed against someone guilty of plagiarism. If proven, a charge of plagiarism could result in an automatic F in the course and possible expulsion. The strongest of sanctions will be imposed on anyone who submits as his/her own work a report, examination paper, computer file, lab report, or other assignment which has been prepared by someone else. If you have any questions or doubts about what plagiarism entails or how to properly acknowledge source materials be sure to consult the instructor.

Incomplete

An incomplete grade is given only for an exceptional reason such as a death in the family, a serious illness, etc. Any such reason must be documented. Any incomplete request must be made at least two weeks before the final, and approved by the Dean of the College of Computing and Digital Media. Any consequences resulting from a poor grade for the course will not be considered as valid reasons for such a request.

Students with Disabilities

Students who feel they may need an accommodation based on the impact of a disability should contact the instructor privately to discuss their specific needs. All discussions will remain confidential.

To ensure that you receive the most appropriate accommodation based on your needs, contact the instructor as early as possible in the quarter (preferably within the first week of class), and make sure that you have contacted the Center for Students with Disabilities (CSD) at:

Student Center, LPC, Suite #370

Phone number: (773)325.1677

Fax: (773)325.3720

TTY: (773)325.7296