

**Class :** Online recordings available on Wednesday at 5:45pm each week  
**Instructor :** Dr. Anthony Chung  
**Office :** Online through Skype ([achung@depaul.edu](mailto:achung@depaul.edu))  
**Office Hours :** M to Th 3:00-3:45 PM  
**Email :** [achung@depaul.edu](mailto:achung@depaul.edu)

**IMPORTANT:**

While email is a great means of communication, increasingly we are bombarded with a volume of emails that is getting difficult to manage. In order to manage emails to better serve both the students and the professor. **Pay attention to ALL of the following:**

- **You MUST include TDC577 (case insensitive) in the subject line of the email as they will be directed to the appropriate mailbox where I check for emails related to this course.**
- I meet with students through Skype, answer student emails, and respond to discussion forums etc **during my office hours.** In this way, you know exactly when you expect to hear from me by these means of communications. If you contact me close to the end of my office hours I may have to respond during the next office hours period. If you do not hear from me after two office hours periods, check to make sure that you included TDC577 in the subject, email me again, or call to leave a message.
- I am guaranteed to be available through Skype during the office hours hours. If I cannot make some office hours due to special circumstances, announcements will be made on d2l.

Depending on the complexity of your questions, **sometime we can get more out of meeting by skype interactively rather than by emails.**

- Given my response time frame and office hours, you should **work on your assignments early so as to give you ample time to ask questions.**
- 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 are 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.
  - 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.

- In addition to including TDC577 in the subject line, **be specific about the subject of the email in the mail subject heading and use proper spelling, grammar, and punctuation. DO NOT 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 could 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 27, 2020)

**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 referenced 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 and TDC 477.**

### **Course Description and Objective:**

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

**Learning Outcomes:**

After this course you should be able to:

- Explain the functions of the technologies covered in this course and how they mitigate network security threats.
- Configure and deploy examples of the technologies.
- Design network and security infrastructure to use these technologies for defense in depth.
- Design overall communication and security infrastructure
- Explain threats to security of networking devices such as routers and switches.
- Secure routers and switches against these threats.
- Explain weaknesses in protocols such as BGP and DNS.
- Explain how BGPsec and DNSSEC provide security for these protocols.

**Grading**

**4 Homework Assignments** **20%**

**Lab Assignments** **26%**

Lab 1 – VPN as backup to T1 line (On Packet Tracer)	6%
Lab 2 – 3-site VPN (On Packet Tracer)	6%
Lab 3 – Snort (Performed on student's own computer)	10%
Lab 4 – Snort and SEIM (student's own computer)	4%

**Midterm** **20%**

**Final** **16%**

**Class Participation** **18%**

**Extra Credits - PT Activities** (Performed Using Packet Tracer on students own devices) **8%**

PT Activity 1 – AAA	2%
PT Activity 2 – Layer 2 security	3%
PT Activity 3 – Syslog, NTP, SSH	3%

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%

**Important Notes on Grading:**

- Student **must** score 60% or above in each exam to pass the course. **This is a strict requirement.**
- The maximum total is 108, but will be capped at 100.
- Students at or above the class average (calculated from grades 60% or above) will receive at least an A-. I will modify the grading scale if the class average is below 87%.

**Notes:**

- **Tips for online learning:**

DePaul has created this document with tips to be a successful online student:

[https://drive.google.com/file/d/1qGG\\_cnVtqknOp9ENRMI5yt51\\_gtY6-cO/view](https://drive.google.com/file/d/1qGG_cnVtqknOp9ENRMI5yt51_gtY6-cO/view)

This is DePaul's general website for student success:

<https://resources.depaul.edu/student-success/Pages/default.aspx>

Here is a useful link from Northwestern University -

<https://www.northeastern.edu/graduate/blog/tips-for-taking-online-classes/>

- **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 submissions policy:**
  - **Late homework assignments (HW1 to 4) 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 submission boxes.** 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 BY the due time.
  - **Late lab assignments/PT activities will be accepted with the following penalty:**
    - Up to one day late : -10%
    - Up to two days late: - 30%
    - Up to three days late: -50%
    - No lab assignments/PT activities are accepted after 3 days.

- **About Class Participation**

- Viewing of recorded lectures is expected.
- For every lecture module there will be a **participation quiz**. The questions will be on the “in class” exercises and certain points that we emphasized in the recordings. Students are allowed to take the quiz **up to 10 times** before the quiz is due and the **highest** score will be used towards the final grade. To do well in the quiz you are recommended to
  - Take notes while viewing the lecture, especially on points not in the slides but were filled in within the lecture videos, and points where I emphasized that students should write down.
  - When an “in class” exercise is given, students should attempt to work through the exercise. There will be one or more submission boxes for the “in class” exercises. They must be submitted before you can watch the remaining parts of the lecture.
  - Make sure that you get the answers of the in class exercises. Some quiz questions will be on the in class exercises.

Here's a link from Columbia about the importance of note taking (and resources)

<https://www.cc-seas.columbia.edu/node/31875>

Although you can choose to take notes using your laptop or by hand, here's an article on recent research showing the advantage of taking notes by hand.

<http://www.npr.org/2016/04/17/474525392/attention-students-put-your-laptops-away>

- 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.**
- About Exams (Online):
  - Study guides will be provided a week before the exam.
  - Exams are closed books and notes.
  - You are given 2 1/2 hours for the exams.
    - **Midterm – on Wednesday May 6, at 5:45pm**
    - **Final – on Wednesday at 5:45pm**
  - **For students enrolled in the original OL section** – contact me if you have a valid and documented reason for taking the exam at a different time.
- Please check DePaul's academic calendar  
<https://academics.depaul.edu/calendar/Pages/default.aspx> 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: [https://offices.depaul.edu/academic-affairs/faculty-resources/teaching/academic-integrity/Documents/Academic%20Integrity%20Policy\\_Spring%202016.pdf](https://offices.depaul.edu/academic-affairs/faculty-resources/teaching/academic-integrity/Documents/Academic%20Integrity%20Policy_Spring%202016.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 paraphrasing of someone else's work, including course materials and lecture slides, without giving proper credits and references.
  - Please be aware that any written work (assignments and exams) 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 for online interactions.
- **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.

**Schedule (Tentative):**

**Note: All assignments are due at 11:59pm.**

Date	Topic	Readings	Assignments
4-1	Class overview; TDC 477 Review.  High availability FW architecture	Lecture slides	
4-8	IDS/IPS (I)	<b>Chapter 17, Santos and Stuppi</b>  <b>Network Intrusion Detection</b> , 3 <sup>rd</sup> edition, Northcutt & Novak, Prentice Hall/SAMS – ISBN: 0735712654	<b>Non-graded assignments due (Academic integrity pledge and security tool</b>

		<p>(Available on Safari)</p> <p>About Network Taps:</p> <ul style="list-style-type: none"> <li>• <a href="http://en.wikipedia.org/wiki/Network_tap#Companies_making_network_TAPs">http://en.wikipedia.org/wiki/Network_tap#Companies_making_network_TAPs</a></li> <li>• <a href="https://observer.viavisolutions.com/includes/popups/taps/tap-vs-span.php">https://observer.viavisolutions.com/includes/popups/taps/tap-vs-span.php</a></li> <li>• <a href="http://www.networkcomputing.com/networking/span-port-vs-tap-latency-impact/1358909399">http://www.networkcomputing.com/networking/span-port-vs-tap-latency-impact/1358909399</a></li> </ul> <p>ARP poisoning/spoofing tools:  <a href="http://en.wikipedia.org/wiki/ARP_spoofing">http://en.wikipedia.org/wiki/ARP_spoofing</a></p> <p>National Vulnerability Database:  <a href="http://nvd.nist.gov/">http://nvd.nist.gov/</a></p> <p><a href="https://www.snort.org/documents">https://www.snort.org/documents</a></p> <p>An example IDS load balancer:  <a href="http://docs.citrix.com/en-us/netScaler/11/traffic-management/load-balancing/load-balancing-ids-servers.html">http://docs.citrix.com/en-us/netScaler/11/traffic-management/load-balancing/load-balancing-ids-servers.html</a></p> <p>Examples of free host-based IDSs  OSSEC <a href="https://ossec.github.io/">https://ossec.github.io/</a>  Patriot NG: <a href="http://www.security-projects.com/?Patriot_NG">http://www.security-projects.com/?Patriot_NG</a>  Open Source Tripwire:  <a href="http://sourceforge.net/projects/tripwire/">http://sourceforge.net/projects/tripwire/</a> (only monitors file changes)</p>	<p>usage agreement, and posting of self-introduction on discussion forum)  HW #1 due</p> <p>4-1 participation due</p>
4-15	IDS/IPS (I) Contd.		Lab #1 due
	IDS/IPS (II)	IDS Evasion - <a href="http://insecure.org/stf/secnet_ids/secnet_ids.html">http://insecure.org/stf/secnet_ids/secnet_ids.html</a>	4-8 participation due
4-22	IDS/IPS (II) Contd.	Severity metric example: <a href="http://msisac.cisecurity.org/alert-level/">http://msisac.cisecurity.org/alert-level/</a>	Lab #2 due
	Security Information and Event Management (SIEM)	<p>A NetworkWorld article on SIEM:  <a href="https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html">https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html</a></p> <p>OSSIM <a href="http://www.alienvault.com/open-threat-exchange/projects#ossim-tab">http://www.alienvault.com/open-threat-exchange/projects#ossim-tab</a></p> <p>Splunk <a href="https://www.splunk.com/">https://www.splunk.com/</a></p>	4-15 participation due

4-29	Honeypots	<a href="#">Configuring Policy-Based Routing</a> <a href="#">Configuring IP Access Lists</a> <a href="http://honeynet.org">http://honeynet.org</a> <p>Infoworld Article - "No honeypot? Don't bother calling yourself a security pro"</p> <a href="http://www.infoworld.com/d/security/no-honeypot-dont-bother-calling-yourself-security-pro-216038">http://www.infoworld.com/d/security/no-honeypot-dont-bother-calling-yourself-security-pro-216038</a> <p><b>Honeypot for Windows</b> Roger A. Grimes (Available on books 24X7)</p> <p>Google Hack Database (GHDB):</p> <a href="https://www.exploit-db.com/google-hacking-database/">https://www.exploit-db.com/google-hacking-database/</a> <p>Google Hack Honeypot (GHH):</p> <a href="http://ghh.sourceforge.net/userfaq.php">http://ghh.sourceforge.net/userfaq.php</a>	<b>Lab #3 due</b> <b>HW #2 due</b> <b>4-22 participation due</b>
5-6	<b>Midterm</b>		<b>4-29 participation due</b>
5-13	Securing Switches	<p><b>LAN Switch Security – What Hackers Know About Your Switches</b> by Eric Vyncke and Christopher Paggen (available on Safari)</p> <p>About VTP:</p> <a href="http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml">http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml</a>	<b>Lab #4 due</b> <b>PT Activity 1 (extra credit) due</b>
5-20	Securing Routers	<p><b>Router Security Strategies: Securing IP Network Traffic Planes</b> by Gregg Schudel and David J. Smith (available on Safari)</p> <p>Cisco Security Center:</p> <a href="http://tools.cisco.com/security/center/serviceProviders.x?i=76">http://tools.cisco.com/security/center/serviceProviders.x?i=76</a>	<b>PT Activity 2 (extra credit) due</b> <b>HW #3 due</b> <b>5-13 participation due</b>

5-27	TCP/IP Protocol Security  BGP Security	A survey of BGP Security <a href="http://ix.cs.uoregon.edu/~butler/pubs/bgpsurvey.pdf">http://ix.cs.uoregon.edu/~butler/pubs/bgpsurvey.pdf</a>  MANRS (Mutually Agreed Norms for Routing Security) <a href="https://www.manrs.org/">https://www.manrs.org/</a>	Lab #5 due  5-20 participation due
6-3	DNS Security       Course Wrap-up and Final Review	DNS Cache Poisoning <a href="http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html">http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html</a>  DNSSEC resources: <a href="http://www.internetsociety.org/deploy360/dnssec/?gclid=CNfAyejdzcsCFYGFaQod6j4HeQ">http://www.internetsociety.org/deploy360/dnssec/?gclid=CNfAyejdzcsCFYGFaQod6j4HeQ</a>	PT Activity 3 due (extra credit)  HW #4 due  5-27 participation due
6-10	<b><u>Final</u></b>		6-3 participation due

### 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