Class : Online recordings (pre-class and/or post-class),
and Zoom on Wednesdays at 5:45pm each week (except for exams)

- Pre-Class Recordings are available by the Friday night before.
- Zoom Recordings will be available by noon the following day.
- Post-Class Recordings, if any, will be available the following afternoon.
- We will meet the full period by Zoom for the first lecture. Pre-class videos (usually about 1 hour long) will be available before remaining lectures and students must go through the corresponding video before attending a Zoom class meeting. The Zoom meeting will be 2 hours (plus a 10-minute break) starting from second week.

- We will stay engaged with each other using the following tools:
  - Flipgrid – a video discussion forum.
  - D2l discussion forum in text
  - Zoom Office Hours
  - Emails
  - Announcements on d2l

It is highly recommended to subscribe to announcements and discussion forums to get latest information/discussion.

Instructor : Dr. Anthony Chung
Office : Online via Zoom (Link to join in d2l)
Office Hours : M 5:00-6:00 PM / W 3:00- 4:00 PM / F 10:00-11:00 AM
Email : achung@depaul.edu

IMPORTANT:

- **Cisco Modeling Lab (CML) Version 2.1.1 –** we will be using this environment for the preliminary lab and three of the four labs. The NET program committee has decided that this is the best solution for students to be able to remotely perform labs that involve configuration of Cisco devices. This will be used in many NET courses. Students are responsible for purchasing a license ($199 a year).

- **Packet Tracer Version 8** –We will be using Packet Tracer for PT Activities. If you do not already have this version, and/or are not already enrolled in Cisco Networking Academy, follow this link https://www.netacad.com/courses/packet-tracer to enroll and/or download Packet Tracer.

- **Respondus Lockdown Browser + Zoom Live Monitoring –** we will be using this tool for exams. More information is provided in the Appendix.

- **Email and Other Forms of Communications -**

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 NET577 (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 Zoom, 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 NET577 in the subject, email me again, or call to leave a message.

- I will be available through Zoom during the office 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 Zoom interactively rather then by emails.**

- Given my response time frame and office hours, you should **work on your assignments early so as to give yourself 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 NET577 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 <u>your full name</u> 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, 2021)

Prerequisites: **TDC/NET 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 – O'Reilly for Higher Education (Formerly Safari) - https://go.oreilly.com/depaul/

The following three books are referenced the most.

- **TDC/NET 477 text: CCNA Security 210-260 Official Cert Guide,** Santos & Stuppi, Cisco Press/Pearson, 2015. ISBN: 9780134077857
- **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/NET 463 and TDC/NET 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

3 Homework Assignments		**30%**
Lab Assignments		**34%**
Preliminary Lab – Setting up CML	5%	
Lab 1 – VPN as backup to T1 line (On CML)	8%	
Lab 2 – 3-site VPN (On CML)	6%	
Lab 3 – Snort (Performed on student's own computer)	10%	
Lab 4 – Traffic redirection (On CML)	5%	
Midterm (must achieve 50% or more to pass this course)		**20%**
Class Participation		**16%**

Note: All the above add up to 100%

==========

Extra Credits - PT Activities (Performed Using Packet Tracer)		**8%**
PT Activity 1 – AAA	2%	
PT Activity 2 – Layer 2 security	3%	
PT Activity 3 – Syslog, NTP, SSH	3%	
Final - Optional : Replace midterm grade if it is better. See notes below.		**20%**
Week 10 Participation - Optional : Replace lowest participation grade if it is better.		**2%**

Grading Scale:

A	92-100%
A-	90-91%
B+	88-89%
B	82-87%
B-	80-81%
C+	78-79%
C	72-77%
C-	70-71%
D+	68-69
D	60-67%
F	< 60%

Important Notes on Grading:

- The maximum total is 108, but will be capped at 100.
- Student must receive 50% or more in the midterm to pass this course.
- If you receive an A for all assignments and exams due on or before June 2 (i.e. all assignments except for June 2 Participation and the Final), you will receive an A and you will not be given a final.
- If you receive a grade other than A for all assignments and exams due on or before June 2, you have the following two options:
  - Opt out the final and June 2 participation quiz and keep the grade.
  - Opt in the final and June 2 participation quiz. Grade of the final exam replaces that of the midterm if it is better. June 2 participation grade replaces the lowest participation grade if it is better.
- Grades for total of all work on or before June 2 will be released by the end of the day on June 4. You should email me by Monday June 7 if you opt in the final. Otherwise I will assume that you opt out the final.

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_cnVtqknOp9ENRMl5yt51_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.

- **Late submissions policy:**
  - **Late homework assignments (HW1 to 3) and Participation Quizzes 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 will be accepted after 3 days.

- **About Class Participation**

  a. For OL-Sync students: Attending Zoom lecture is required.
  For OL-Async students: Viewing of recorded lectures is required.
  b. Weekly video check-ins on flipgrid (see the welcoming announcement on d2l for details).
  c. 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 (Zoom, Pre-Class, and Post-Class, if any). 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
     i. Take notes while attending/viewing the lectures, 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.
     ii. When an "in class" exercise is given, students should work through the exercise before checking solutions.
     iii. Make sure that you get the answers of the in class exercises. Some quiz questions will be on the in class exercises.
  d. Failure to do a. and/or b. above will result in lowering of the participation points irrespective of the participation quiz score.

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 you 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 using Respondus Lockdown Broswer+Zoom):
  - 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 5, at 5**:45pm
    - **Final (Optional) – on Wednesday, June 9, at 5:45pm**
  - **The schedules are for ALL sections. A test section is scheduled at 5:45 pm on Wednesday April 7 (Week 2 at the beginning of the Zoom class meeting) to ensure that all students are ready to take the exam.**
  - **For students enrolled in the OL-Async section** – If you cannot take the exams as scheduled for a valid and documented reason (e.g. schedule conflict with another class), contact me by email, by Friday, April 9. Please understand that the exams will be monitored live and it is difficult for me to schedule multiple sections for it. I appreciate it if you can accommodate and take the exam during the scheduled time.

- 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.

- **Make sure that you read and understand DePaul's academic integrity policy:** https://offices.depaul.edu/academic-affairs/faculty-resources/academic-integrity/Documents/Academic%20Integrity%20Policy_Spring%202016.pdf

  For additional resources concerning academic integrity, 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.**

- **Sharing your work with other students, in or out of this class, is also a violation of academic integrity (called "complicity").** While you are encouraged to help fellow students understand course materials, you should not help them with individual assignments. If you want to help, encourage them to ask questions about what they do not understand in the course materials presented, rather than asking questions directly about the assignment.

- **Under no circumstances should you copy or use simple paraphasing 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.**

- Publicly sharing or posting online any prior or current materials from this course is a violation of DePaul's academic integrity:

  All students are expected to abide by the University's Academic Integrity Policy which prohibits cheating and other misconduct in student coursework. Publicly sharing or posting online any prior or current materials from this course (including exam questions or answers), is considered to be providing unauthorized assistance prohibited by the policy. Both students who share/post and students who access or use such materials are considered to be cheating under the Policy and will be subject to sanctions for violations of Academic Integrity.

- **Respect for Diversity and Inclusion at DePaul University as aligned with our Vincentian Values:** At DePaul, our mission calls us to explore "what must be done" in order to respect the inherent dignity and identity of each human person. We value diversity because it is part of our history, our traditions and our future. We see diversity as an asset and a strength that adds to the richness of classroom learning. In my course, I

strive to include diverse perspectives and teaching pedagogies. I also encourage open dialogue and spaces for students to express their unique identities and perspectives. I am open to having difficult conversations and I will strive to create an inclusive classroom that values all perspectives. If at any time, the classroom experience does not live up to this expectation, please feel free to contact me via email or during office hours.

- **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.

Schedule (Tentative):

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

Week: Date	Topic	Readings	Assignments
1: Mar 31	Class overview; NET 477 Review. High availability FW architecture	Lecture slides	
2: April 7	Respondus Lockdown Browser + Zoom test section. IDS/IPS (I)	**Chapter 17, Santos and Stuppi** **Network Intrusion Detection**, 3rd edition, Northcutt & Novak, Prentice Hall/SAMS – ISBN: 0735712654 (Available on O'Reilly for Higher Education) About Network Taps: • http://en.wikipedia.org/wiki/Network_tap#Companies_making_network_TAPs	**Non-graded, but required, assignments due:** • **If you did not attend Week 1's Zoom lecture and introduce yourself, post a short introduction video on flipgrid;** • **Take the Academic**

		• https://observer.viavisolutions.com/includes/popups/taps/tap-vs-span.php • http://www.networkcomputing.com/networking/span-port-vs-tap-latency-impact/1358909399 ARP poisoning/spoofing tools: http://en.wikipedia.org/wiki/ARP_spoofing https://www.snort.org/documents An example IDS load balancer: https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-ids-servers.html Examples of free host-based IDSs OSSEC https://ossec.github.io/ Patriot NG: http://www.security-projects.com/?Patriot_NG Open Source Tripwire: http://sourceforge.net/projects/tripwire/ (only monitors file changes)	**Integrity Pledge Quiz; and** • **Submit in the submission box "Getting to know more about you")** **Preliminary Lab due** **Week 1 participation and video check-in due**
3: April 14	IDS/IPS (II)	IDS Evasion - http://insecure.org/stf/secnet_ids/secnet_ids.html	**HW #1 due** **Week 2 participation and video check-in due**
4: April 21	Security Information and Event Management (SIEM) Honeypots	A NetworkWorld article on SIEM: https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool.html OSSIM http://www.alienvault.com/open-threat-exchange/projects#ossim-tab Splunk https://www.splunk.com/ Configuring Policy-Based Routing 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	**Lab #1 due** **Week 3 participation and video check-in due**

		Deception Technology Google Hack Database (GHDB): https://www.exploit-db.com/google-hacking-database Google Hack Honeypot (GHH): http://ghh.sourceforge.net/userfaq.php	
5: April 28	Securing Switches	**LAN Switch Security – What Hackers Know About Your Switches** by Eric Vyncke and Christopher Paggen (available on Safari)	**Lab #2 due** **HW #2 due** **Week 4 participation and video check-in due**
6: May 5	**Midterm**		**Week 5 participation and video check-in due**
7: May 12	Securing Routers	**Router Security Strategies: Securing IP Network Traffic Planes** by Gregg Schudel and David J. Smith (available on Safari)	**Lab #3 due** **PT Activity 1 (extra credit)**
8: May 19	TCP/IP Protocol Security DoS Attacks and Defenses	A look back at Security Problems in the TCP/IP Protocol Suite The real cause of large DDoS - IP Spoofing	**PT Activity 2 (extra credit) due** **Week 7 participation and video check-in due**
9: May 26	BGP Security	A survey of BGP Security https://www.researchgate.net/publication/224092573_A_Survey_of_BGP_Security_Issues_and_Solutions MANRS (Mutually Agreed Norms for Routing Security) https://www.manrs.org/	**Lab #4 due** **Week 8 participation and video check-in due**
10: June 2	DNS Security	DNS Cache Poisoning http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html	**PT Activity 3 due (extra credit)**

	Course Wrap-up and Final Review	DNSSEC resources: http://www.internetsociety.org/deploy360/dnssec/?gclid=CNfAyejdzcsCFYGFaQod6j4HeQ	**HW #3 due** **Week 9 participation and video check-in due**
11: June 9	**Final (Optional)**		**Week 10 participation and video check-in (optional) 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.

Respect for Diversity and Inclusion at DePaul University as aligned with our Vincentian Values

At DePaul, our mission calls us to explore "what must be done" in order to respect the inherent dignity and identity of each human person. We value diversity because it is part of our history,

our traditions and our future. We see diversity as an asset and a strength that adds to the richness of classroom learning. In my course, I strive to include diverse authors, perspectives and teaching pedagogies. I also encourage open dialogue and spaces for students to express their unique identities and perspectives. I am open to having difficult conversations and I will strive to create an inclusive classroom that values all perspectives. If at any time, the classroom experience does not live up to this expectation, please feel free to contact me via email or during office hours.

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

* Last updated on 3/27/2021

Appendix: Respondus Lockdown Browser + Zoom

We will be using this tool for the online exam. See the syllabus and view the recordings for the first lecture so that you understand what needs to be done to take the exam.

If you have not used Respondus Lockdown Browser before, follow this link to install it on your computer:
https://download.respondus.com/lockdown/download.php?id=362112432

Additional information:

- A Zoom link other than the one we use for class will be posted the day before an exam.
- This will not work on a tablet. You must use a laptop or desktop for the exam.
- Once all students are admitted into the Zoom meeting, a start code will be provided so that you can start taking the exam (as a quiz in d2l).
- Once you start the quiz, Zoom will be running in the background and you will not be able to access Zoom again until after you submit your quiz and exit the lockdown browser.

At the beginning of Week 2's Zoom lecture, we will do a practice quiz to make sure that it is working for everyone.