

SYLLABUS

NET 577

Network Security II

Spring 2024

April 3, 2024

Instructor: Dale Buchholz
Class Time: Wednesday 5:45-9:00 pm
Location: Loop Campus – Lewis 1007
Office Hours: Wednesday 4:00-5:30 pm or by appointment (Zoom)
Phone: 312-362-6819
Office: CDM 617
E-mail: dbuchhol@depaul.edu
Prerequisite: NET 477 Network Security
References: *CCNA SECURITY 210-260: Official Cert Guide*, Santos, Omar; Stuppi, John, Cisco Press, 2015, ISBN 0-13-407785-7
(not required)

CCNA SECURITY 640-554: Live Lessons, Barker, Keith, Pearson IT Certification, 2012, ISBN 0-13-325900-5

LAN Switch Security: What Hackers Know About Your Switches by Eric Vyncke and Christopher Paggen, Cisco Press, 2007, ISBN 1587052569

Router Security Strategies: Securing IP Network Traffic Planes by Gregg Schudel and David J. Smith, Cisco Press, 2007, ISBN 1587053365

Course Summary:

This course is an advanced class in network security. Topics include Intrusion Detection and Prevention Systems; Security Engineering processes; Advanced firewall considerations; Honeypots; Incident response; Forensics; Enterprise security policy development and complex enterprise security infrastructure design and integration.

Learning Outcomes:

- 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, and countermeasures.
- Explain DDoS attacks and countermeasures.

- Explain weaknesses in protocols such as BGP and DNS.
- Explain how BGP-SEC and DNS-SEC provide security for these protocols.

Course Prerequisites:

- You must have taken NET 463 and NET 477. Other graduate networking courses at the 500 level will be beneficial.
- You have good knowledge of fundamental network concepts, such as layer 2 and layer 3 services, operations and
- You have a good understanding of TCP/IP protocols, including OSPF, BGP, DNS, DHCP, TCP, TLS and QoS.
- You have practical experience with configuration of switches, routers and network services using Packet Tracer, CML or GNS3.

Coursework:

Since NET 577 is an advanced graduate class, some students may be interested in more of a research curriculum, i.e., read trade journals, industry technical papers and/or research papers to gain a deeper understanding of industry and technical trends. Other students may be interested in more practical hands-on labs and the application of technology learned in the course. And still others may prefer a mixture of both.

In order to allow students to somewhat customize their assignment workload, the following is required:

All students are required to complete and submit the General Knowledge Exam (100 pts). This will be due late in the quarter (week 9).

All students are required to submit 200 points worth of assignments chosen from the following:

- a) 2 Research Papers (100 pts each)—one due Week 6; one due Week 11 (last class)
- b) 6 Labs (50 pts each) – CML, Packet Tracer and Snort

The total number of points submitted for the class is 300. Students may choose any combination of assignments that total to 200 points. For example:

All research program: first paper (due Week 6) plus General Knowledge Exam (due Week 9) plus second paper (due Week 11).

All labs program: 4 labs from the set of {4 CML, 1 PT and 1 Snort} (due Weeks 3, 5, 7 and 11) plus General Knowledge Exam (due Week 9)

Mixed program: 2 labs (due Weeks 3 and 5), 1 paper (due Week 11) and the General Knowledge Exam (due Week 9). This is an example. Other plans are possible. The key requirement is 200 points and a realistic schedule for submission. That is, work must be submitted periodically throughout the quarter and cannot be all submitted at or near the end of the quarter.

Further details on each assignment will be distributed by April 7. Students will be required to submit a plan for their 200 points by Sunday, April 14. This can be adjusted during the quarter if need be but must be approved by the instructor.

Research papers, labs and the General Knowledge Exam must be completed individually. Class attendance (sync or async) is strongly recommended since lectures may cover topics outside the text. All class sessions will be recorded for asynchronous viewing.

Grades:

Final grades will be calculated as follows: points earned divided by possible points yields a total course percentage between 0% and 100%. Final letter grades will be assigned as:

Percent	Grade	Percent	Grade
93-100	A	77-79	C+
90-92	A-	73-76	C
87-89	B+	70-72	C-
83-86	B	60-69	D
80-82	B-	< 60	F

Late Assignments:

All homework and labs are due on Sunday by 11:59 pm. Late submissions will be penalized as follows: 10% deduction per day late up to 1 week. No credit after 1 week late. D2L will be closed for submission after 1 week. Any penalty may be waived with permission of the instructor. You must notify the instructor via email before the due date in order to get an extension of the due date. You must provide a reason in your email.

Class Schedule:

Class dates, topics, readings, and assignments are shown in the Class Schedule below.

Class Schedule

NET 577 — Spring 2024

(April 3, 2024)

<i>Date</i>	<i>Topics</i>	<i>Readings</i>	<i>Assignments</i>
Week 1 April 3	Course Overview Review NET 477 Firewall Architectures	CCNA Security	Attendance Assignment (HW0) due April 7
Week 2 April 10	Intrusion Detection (ID) Intrusion Prevention (IP)		Preliminary Program (HW1) due April 14
Week 3 April 17	More ID / IP		1 st Lab due April 21

Week 4 April 24	Security Information and Event Mgmt (SIEM) Honeypots		
Week 5 May 1	Securing Switches	LAN Switch Security	2 nd Lab due May 5
Week 6 May 8	Securing Routers	Router Security Strategies	Research Paper due May 12
Week 7 May 15	BGP Security		3 rd Lab due May 19
Week 8 May 22	DNS Security General Knowledge Exam out Friday, May 24		
Week 9 May 29	IP Network Slicing	Handout	General Knowledge Exam due June 2
Week 10 June 5	Secure Access Service Edge (SASE)	Handout	
Week 11 June 12	Last class (no class)		4 th Lab or Research Paper due on June 12

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.

Online Course Evaluations

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 three weeks. Students do not receive reminders once they complete the evaluation. Please see <https://resources.depaul.edu/teaching-commons/teaching/Pages/online-teaching-evaluations.aspx> for additional information.

Academic Integrity and Plagiarism

This course will be subject to the university's academic integrity policy. More information can be found at <https://resources.depaul.edu/teaching-commons/teaching/academic-integrity/Pages/default.aspx>.

Academic Policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the [University Academic Calendar](#). Information on enrollment, withdrawal, grading and incompletes can be found at: <http://www.cdm.depaul.edu/Current%20Students/Pages/PoliciesandProcedures.aspx>

Incomplete Grades

An incomplete grade is a special, temporary grade that may be assigned by an instructor when unforeseeable circumstances prevent a student from completing course requirements by the end of the term and when otherwise the student had a record of satisfactory progress in the course. All incomplete requests must be approved by the instructor of the course and a CDM Associate Dean. Only exceptions cases will receive such approval. Information about the Incomplete Grades policy can be found at:

<http://www.cdm.depaul.edu/Current%20Students/Pages/Grading-Policies.aspx>

Students with Disabilities

Students seeking disability-related accommodations are required to register with DePaul's Center for Students with Disabilities (CSD) enabling them to access accommodations and support services to assist with their success. There are two office locations:

- Loop Campus (312) 362-8002
- Lincoln Park Campus (773) 325-1677
- Email: csd@depaul.edu

Students who register with the Center for Students with Disabilities are also invited to contact Dr. Gregory Moorhead, Director of the Center, privately to discuss how he may assist in facilitating the accommodations to be used in a course. This is best done early in the term. The conversation will remain confidential to the extent possible. Please see <https://offices.depaul.edu/student-affairs/about/departments/Pages/csd.aspx> for Services and Contact Information.