Fall 2019

IT 230-101: Computer Systems Security

Arnold Felberbaum

Course Syllabus

Jump to Today

IT230 fall 2019 – Tuesday Session

Computer Systems Security

General Information

Course Description

IT 230 introduces the applied topic of Computer Security. Students will learn ways of preventing, identifying, understanding, and recovering from attacks against computer systems. It also presents the evolution of computer security, the main threats, attacks and mechanisms, applied computer operation and security protocols, main data transmission and storage protection methods, cryptography, network systems availability, recovery and business continuation procedures. The prerequisite is IT120, Introduction to Network Technology.

Upon completion of this course, students will:

- Have a sound understanding of computer system vulnerabilities and threats, and ways to mitigate them to protect computers against attacks
- Design, develop and implement a computer information security strategy

The textbook addresses all of the objectives of the CompTIA Security+ Certification Exam. The purpose of the course is not to prepare you for the exam, and you are not required to take it. However, you may be able to pass the exam with some extra preparation.

All students are **not permitted** to use their smartphone during class. Electronic distractions will interfere with your ability to participate in class and will impact your class participation score. I will provide periodic breaks during class that will allow you time to "catch up" on your digital interactions. Of course, from time to time, you may have that occasional call regarding a personal or work situation that needs your immediate attention. You may accept these calls and leave the classroom.

Instructor

Arnold Felberbaum

Guttenberg Information Technologies Center (GITC)

Phone: 973-632-8866

Email: afelberb@njit.edu

Office Hours: Class Day 4:00 pm – 6:00 pm, and by appointment

Resources

Textbook: CompTIA Security+ SYS-501 Cert Guide Academic Edition, Copyright 2018 by Pearson Education, Inc.

The class web page is on **Canvas** where Notes, assignments, tests, and solutions will be posted on the web page.

Grading

Your term grade is based on exams, quizzes, homework, and a lab submissions and participation.

Midterm	15%	One 150-point exam
Final	15%	One 150-point exam
Quizzes	15%	2 quizzes, each worth 75 points
Homework	15%	10 homework assignments at 10 points each
Participation	10%	Based on engagement in class (7.5 points based on 13 classes)
Palo Alto Lab points	30%	20 Labs to be completed each worth 15 pts for total of 300

Grades are assigned based on the sum of the points you earn (1000 total points).

A:	Greater than or equal to 911 points
B+	860 – 910 points
B:	800 – 859 points
C+	750 – 799 points
C	700 – 749 points

D 600 – 699 points

F: 0 - 599 points

For example, you may earn an A if you have 900 points and have good class participation. You cannot earn an A without reasonable class participation.

Grades are based solely on the points you earn and are not negotiable.

Exams and Quizzes

The midterm will be during a regular class period. The final exam will be during finals week. The final is not cumulative and covers the material from the midterm until the end of the course. Quizzes will be given during class and will last about 30-45 minutes. The purpose of the quizzes is for you to assess your readiness for the midterm and final. Make-up exams and quizzes will not be given unless there is a reason beyond your control.

Exams and quizzes will be closed book and must be taken in the classroom. I will allow one single-sided sheet of paper with notes. Calculators are permitted, and you may not use your phone or any networked computing device as a calculator.

Tests and Quizzes must be completed in the classroom. When you are done with tests, you may leave. However, you need to sign out and time-stamp your departure. When you are done with Quizzes, you may take a break and must return to class and attendance will be taken at the end of class.

<u>If you do not sign out, you will receive a grade of 50%.</u>

Guidelines for labs

Palo Alto Labs are to be completed according to the delivery dates specified. Each lab takes approximately 30 minutes each. You will need to submit the following document for each lab:

1. A full-screen print of at least three of the steps between the start and end of the lab. The screen print must include:
    1. The session id number (you will need that to name the file)
    2. The time left in the session
    3. The date and time of your PC (Windows – lower right, MAC – upper right) must be included
2. Must paste the screen copies in a word document
3. The file name is: Session ID Your last and first name lab #. Example: 123456789 Felberbaum Arnold Lab 1
4. Do not convert to a PDF.

Class Preparation and Participation

Powerpoint notes and other resources will be available on the class page before each class. I expect you to do the assigned reading and review the notes before you come to class. You will get more out of the class if you have spent some time thinking about the material in advance. This course covers a lot of material quickly. There are 10 questions 15-minute homework assignment due by the following class. Don't let yourself get behind!

Attendance and participation is highly correlated with good performance in the class, so I will record attendance for every class and can affect your grade as follow (two warnings during class regarding smartphone use will result in no class participation for that class):

- Miss 0 - 2 classes — no participation penalty
- Miss 3 - 8 classes — Up to a 75% participation penalty
- Miss > 8 classes — You cannot receive an A

Absences may be excused for athletics, religious holidays, illness, military obligation, or family emergencies if you contact me before the missed class. Leaving class early can have an impact on your ability to participate during class. If you need to leave early, please advise the professor.

I expect you to be an active participant in each class.

Homework

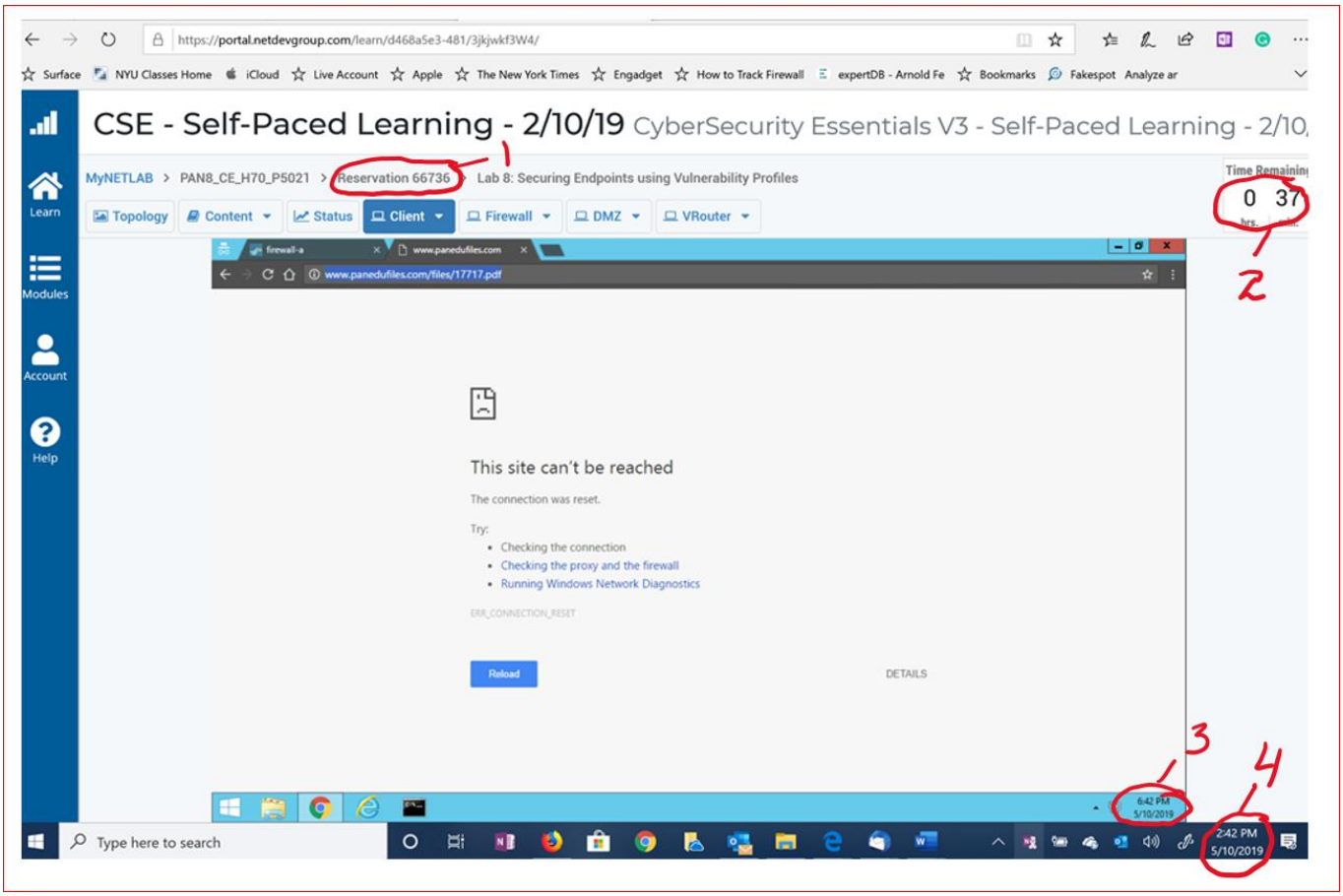
Homework is due regularly. Homework problems will be online through Canvas. Solutions will be provided on the class Canvas page.

Unless otherwise specified, homework is due at the beginning of class on the due date. It is automatically graded unless a question requires a detailed answer. Late homework will be accepted with a penalty unless there is a reason beyond your control. Homework is a large component of your semester grade.

Lab Submissions

All Labs are to be submitted according to the schedule posted on Canvas. Lab submissions consist of several pieces of information, as follows:

Sample:



1 – Reservation Number, 2 – Session time remaining, 3 – Lab Time, 4 Your computer time

#	Date	Chapters	Deliverables	Subject
1	September 3	1 & 2		**Class Orientation** · Homework · PaloAlto – Logon and Validate · Use of Respondus **Introduction to Security** • Security 101 • Think like a hacker • Threat actor types and attributes **Computer Systems Security Part I** • Malicious software types • Delivery of malware • Preventing and troubleshooting malware
2	September 10	3 & 4	Respondus Verification Quiz CSG Lab 1 CSG Lab 2 CSG Lab 3	**Computer Systems Security Part II** • Implementing security applications • Securing computer hardware and peripherals • Securing mobile devices **OS Hardening and Virtualization** • Hardening operating systems • Virtualization technology

3	September 17	5 & 6	CSG Lab 4 CSG Lab 5	**Application Security** · Securing the browser · Securing other applications · Secure programming **Network Design Elements** · Network design · Cloud security and server defense
4	September 24	7 & 8	CSG Lab 6 CSG Lab 7	**Networking Protocols and Threats** • Ports and protocols • Malicious attacks **Network Perimeter Security** • Firewalls and network security • NIDS versus NIPS
5	October 1	9	CSG Lab 8 CSG Lab 9	**Securing Network Media and Devices** • Securing wired networks and devices • Securing wireless networks
6	October 8	**Quiz** – Preliminary to Mid-Term Review of Chapters 1-9 for Midterm and Study Guide		
7	October 15	**Mid Term Exam**		

8	October 22	10 & 11	CSE Lab 1 CSE Lab 2	**Physical Security and Authentication Models** · Physical security · Authentication models and components **Access Control Methods and Models** · Access control models defined · Rights, permissions, and policies
9	October 29 Guest Lecturer	12 &13	CSE Lab 3 CSE Lab 4	**Vulnerability and Risk Assessment** • Conducting risk assessments • Assessing vulnerability with security tools **Monitoring and Auditing** • Monitoring methodologies • Using tools to monitor systems and networks • Conducting audits
10	November 5	14 & 15	CSE Lab 5 CSE Lab 6 CSE Lab 7	**Encryption and Hashing Concepts** • Cryptography concepts • Encryption algorithms • Hashing basics **PKI and Encryption Protocols** • Public key infrastructure • Security protocols

11	November 12	16 & 17	CSE Lab 8 CSE Lab 9 CSE Lab 10	**Redundancy and Disaster Recovery** • Redundancy planning • Disaster recovery planning and procedures **Social Engineering, User Education, and Facilities Security** • Social engineering • User education • Facilities security
12	November 19	17 &18	CSG Lab 10 CSG Lab 11	**Social Engineering, User Education, and Facilities Security** • Social engineering • User education • Facilities security) **Policies and Procedures** • Legislative and organizational policies • Incident response procedures • IT security frameworks
13	December 3	**Quiz** – Preliminary to Final Review of Chapters 10-18 for Midterm and Study Guide		
14	December 17	**Final Exam**		

Course Summary:

Date	Details
Tue Sep 10, 2019	Assignment Homework Chapter 1 due by 6pm
	Assignment Homework Chapter 2 due by 6pm
Mon Sep 16, 2019	Assignment NOVA Cybersecurity Lab due by 11:59pm
Tue Sep 17, 2019	Assignment Respondus Test Quiz- Requires Respondus LockDown Browser due by 11:59pm
Wed Sep 18, 2019	Assignment CSE Lab 1 due by 11pm
	Assignment CSE Lab 2 due by 11pm
	Assignment CSE Lab 3 due by 11pm
	Assignment Homework Chapter 10
	Assignment Homework Chapter 11
	Assignment Homework Chapter 12
	Assignment Homework Chapter 13
	Assignment Homework Chapter 14
	Assignment Homework Chapter 15
	Assignment Homework Chapter 16
	Assignment Homework Chapter 17
	Assignment Homework Chapter 18
	Assignment Homework Chapter 3
	Assignment Homework Chapter 4
	Assignment Homework Chapter 5
	Assignment Homework Chapter 6
	Assignment Homework Chapter 7
	Assignment Homework Chapter 8
	Assignment Homework Chapter 9
	Assignment Least Privilege
	Assignment Roll Call Attendance
	Assignment sample document upload
	Assignment This is just an assignment thing

Course Syllabus

Jump to Today

IT230 fall 2019 – Thursday Session

Computer Systems Security

General Information

Course Description

IT 230 introduces the applied topic of Computer Security. Students will learn ways of preventing, identifying, understanding, and recovering from attacks against computer systems. It also presents the evolution of computer security, the main threats, attacks and mechanisms, applied computer operation and security protocols, main data transmission and storage protection methods, cryptography, network systems availability, recovery and business continuation procedures. The prerequisite is IT120, Introduction to Network Technology.

Upon completion of this course, students will:

- Have a sound understanding of computer system vulnerabilities and threats, and ways to mitigate them to protect computers against attacks
- Design, develop and implement a computer information security strategy

The textbook addresses all of the objectives of the CompTIA Security+ Certification Exam. The purpose of the course is not to prepare you for the exam, and you are not required to take it. However, you may be able to pass the exam with some extra preparation.

All students are **not permitted** to use their smartphone during class. Electronic distractions will interfere with your ability to participate in class and will impact your class participation score. I will provide periodic breaks during class that will allow you time to "catch up" on your digital interactions. Of course, from time to time, you may have that occasional call regarding a personal or work situation that needs your immediate attention. You may accept these calls and leave the classroom.

Instructor

Arnold Felberbaum

Guttenberg Information Technologies Center (GITC)

Phone: 973-632-8866

Email: afelberb@njit.edu

Office Hours: Class Day 4:00 pm – 6:00 pm, and by appointment

Resources

Textbook: CompTIA Security+ SYS-501 Cert Guide Academic Edition, Copyright 2018 by Pearson Education, Inc.

The class web page is on **Canvas** where Notes, assignments, tests, and solutions will be posted on the web page.

Grading

Your term grade is based on exams, quizzes, homework, and a lab submissions and participation.

Midterm	15%	One 150-point exam
Final	15%	One 150-point exam
Quizzes	15%	2 quizzes, each worth 75 points
Homework	15%	10 homework assignments at 10 points each
Participation	10%	Based on engagement in class (7.5 points based on 13 classes)
Palo Alto Lab	30%	20 Labs to be completed. Each worth 15 points

Grades are assigned based on the sum of the points you earn (1000 total points).

A:	Greater than or equal to 911 points
B+	860 – 910 points
B:	800 – 859 points
C+	750 – 799 points

C 700 – 749 points

D 600 – 699 points

F: 0 - 599 points

For example, you may earn an A if you have 900 points and have good class participation. You cannot earn an A without reasonable class participation.

Grades are based solely on the points you earn and are not negotiable.

Exams and Quizzes

The midterm will be during a regular class period. The final exam will be during finals week. The final is not cumulative and covers the material from the midterm until the end of the course. Quizzes will be given during class and will last about 30-45 minutes. The purpose of the quizzes is for you to assess your readiness for the midterm and final. Make-up exams and quizzes will not be given unless there is a reason beyond your control.

Exams and quizzes will be closed book and must be taken in the classroom. I will allow one single-sided sheet of paper with notes. Calculators are permitted, and you may not use your phone or any networked computing device as a calculator.

Tests and Quizzes must be completed in the classroom. When you are done with tests, you may leave. However, you need to sign out and time-stamp your departure. When you are done with Quizzes, you may take a break and must return to class and attendance will be taken at the end of class.

<u>If you do not sign out, you will receive a grade of 50%.</u>

Guidelines for labs

Palo Alto Labs are to be completed according to the delivery dates specified. Each lab takes approximately 30 minutes each. You will need to submit the following document for each lab:

1. A full-screen print of at least three of the steps between the start and end of the lab. The screen print must include:
    1. The session id number (you will need that to name the file)
    2. The time left in the session
    3. The date and time of your PC (Windows – lower right, MAC – upper right) must be included
2. Must paste the screen copies in a word document
3. The file name is: Session ID Your last and first name lab #. Example: 123456789 Felberbaum Arnold Lab 1

4. Do not convert to a PDF.

Class Preparation and Participation

Powerpoint notes and other resources will be available on the class page before each class. I expect you to do the assigned reading and review the notes before you come to class. You will get more out of the class if you have spent some time thinking about the material in advance. This course covers a lot of material quickly. There are 10 questions 15-minute homework assignment due by the following class. Don't let yourself get behind!

Attendance and participation is highly correlated with good performance in the class, so I will record attendance for every class and can affect your grade as follow (two warnings during class regarding smartphone use will result in no class participation for that class):

- Miss 0 - 2 classes no participation penalty
- Miss 3 - 8 classes Up to a 75% participation penalty
- Miss > 8 classes You cannot receive an A

Absences may be excused for athletics, religious holidays, illness, military obligation, or family emergencies if you contact me before the missed class. Leaving class early can have an impact on your ability to participate during class. If you need to leave early, please advise the professor.

I expect you to be an active participant in each class.

Homework

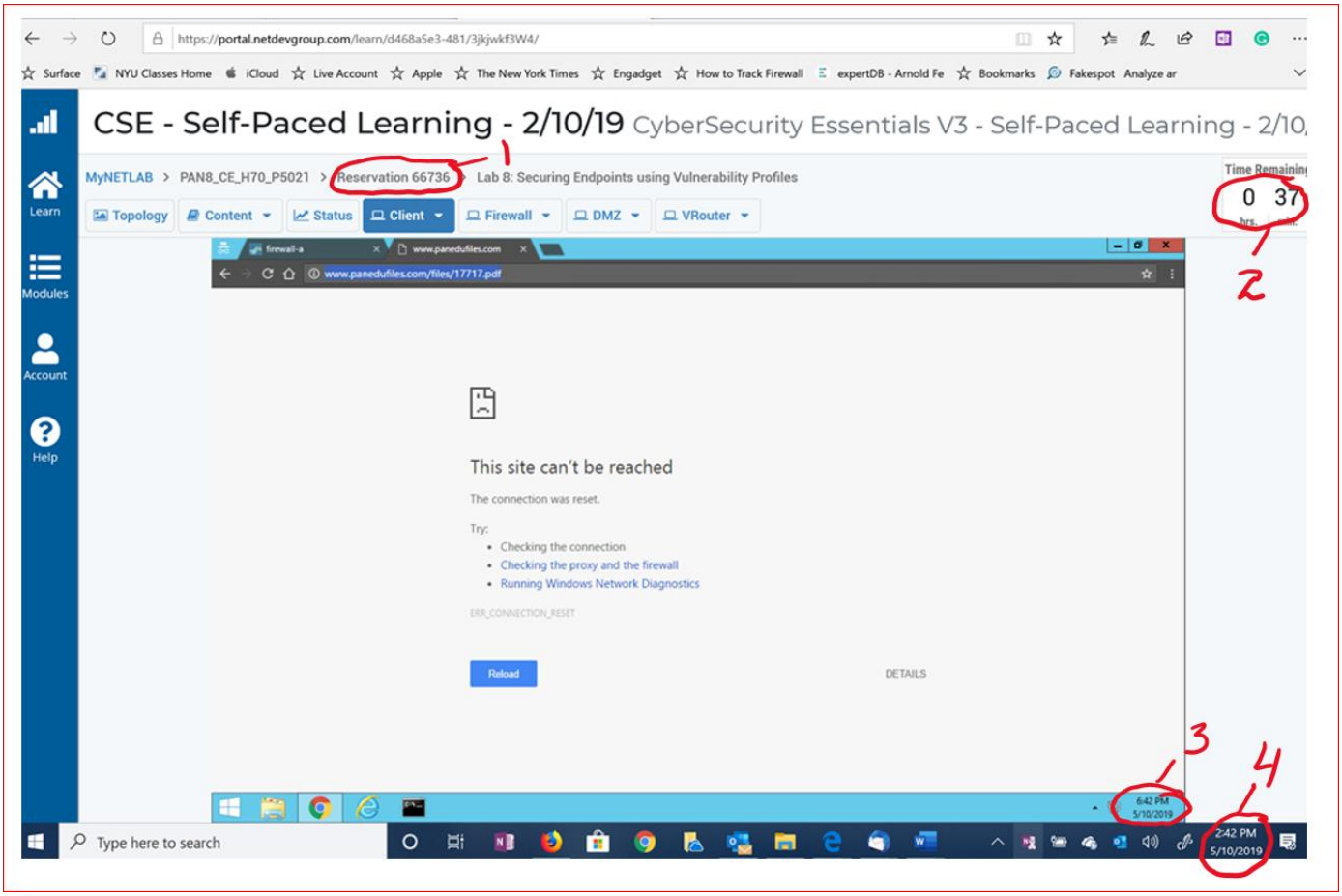
Homework is due regularly. Homework problems will be online through Canvas. Solutions will be provided on the class Canvas page.

Unless otherwise specified, homework is due at the beginning of class on the due date. It is automatically graded unless a question requires a detailed answer. Late homework will be accepted with a penalty unless there is a reason beyond your control. Homework is a large component of your semester grade.

Lab Submissions

All Labs are to be submitted according to the schedule posted on Canvas. Lab submissions consist of several pieces of information, as follows:

Sample:



1 – Reservation Number, 2 – Session time remaining, 3 – Lab Time, 4 Your computer time

#	Date	Chapters	Deliverables	Subject
1	September 5	1 & 2		**Class Orientation** · Homework · PaloAlto – Logon and Validate · Use of Respondus **Introduction to Security** • Security 101 • Think like a hacker • Threat actor types and attributes **Computer Systems Security Part I** • Malicious software types • Delivery of malware • Preventing and troubleshooting malware
2	September 12	3 & 4	Respondus Verification Quiz CSG Lab 1 CSG Lab 2 CSG Lab 3	**Computer Systems Security Part II** • Implementing security applications • Securing computer hardware and peripherals • Securing mobile devices **OS Hardening and Virtualization** • Hardening operating systems • Virtualization technology

3	September 19	5 & 6	CSG Lab 4 CSG Lab 5	**Application Security** · Securing the browser · Securing other applications · Secure programming **Network Design Elements** · Network design · Cloud security and server defense
4	September 26	7 & 8	CSG Lab 6 CSG Lab 7	**Networking Protocols and Threats** • Ports and protocols • Malicious attacks **Network Perimeter Security** • Firewalls and network security • NIDS versus NIPS
5	October 3	9	CSG Lab 8 CSG Lab 9	**Securing Network Media and Devices** • Securing wired networks and devices • Securing wireless networks
6	October 10	**Quiz** – Preliminary to Mid-Term Review of Chapters 1-9 for Midterm and Study Guide		
7	October 17	**Mid Term Exam**		

8	October 24	10 & 11	CSE Lab 1 CSE Lab 2	**Physical Security and Authentication Models** · Physical security · Authentication models and components **Access Control Methods and Models** · Access control models defined · Rights, permissions, and policies
9	October 31 Guest Lecturer	12 &13	CSE Lab 3 CSE Lab 4	**Vulnerability and Risk Assessment** • Conducting risk assessments • Assessing vulnerability with security tools **Monitoring and Auditing** • Monitoring methodologies • Using tools to monitor systems and networks • Conducting audits
10	November 7	14 & 15	CSE Lab 5 CSE Lab 6 CSE Lab 7	**Encryption and Hashing Concepts** • Cryptography concepts • Encryption algorithms • Hashing basics **PKI and Encryption Protocols** • Public key infrastructure • Security protocols

11	November 14	16 & 17	CSE Lab 8 CSE Lab 9 CSE Lab 10	**Redundancy and Disaster Recovery** • Redundancy planning • Disaster recovery planning and procedures **Social Engineering, User Education, and Facilities Security** • Social engineering • User education • Facilities security
12	November 21	17 &18	CSG Lab 10 CSG Lab 11	**Social Engineering, User Education, and Facilities Security** • Social engineering • User education • Facilities security) **Policies and Procedures** • Legislative and organizational policies • Incident response procedures • IT security frameworks
13	December 5	**Quiz** – Preliminary to Final Review of Chapters 10-18 for Midterm and Study Guide		
14	December 19	**Final Exam**		

Course Summary:

Date	Details
Thu Sep 12, 2019	Assignment Homework Chapter 1 due by 6pm

Date	Details	
	Assignment Homework Chapter 2 due by 6pm	
Mon Sep 16, 2019	Assignment NOVA Cybersecurity Lab due by 11:59pm	
Tue Sep 17, 2019	Assignment Respondus Test Quiz- Requires Respondus LockDown Browser	due by 11:59pm
Fri Sep 20, 2019	Assignment CSE Lab 1 due by 11pm	
	Assignment CSE Lab 2 due by 11pm	
	Assignment CSE Lab 3 due by 11pm	
	Assignment Homework Chapter 10	
	Assignment Homework Chapter 11	
	Assignment Homework Chapter 12	
	Assignment Homework Chapter 13	
	Assignment Homework Chapter 14	
	Assignment Homework Chapter 15	
	Assignment Homework Chapter 16	
	Assignment Homework Chapter 17	
	Assignment Homework Chapter 18	
	Assignment Homework Chapter 3	
	Assignment Homework Chapter 4	
	Assignment Homework Chapter 5	
	Assignment Homework Chapter 6	
	Assignment Homework Chapter 7	
	Assignment Homework Chapter 8	
	Assignment Homework Chapter 9	
	Assignment Least Privilege	
	Assignment Roll Call Attendance	