Department of Information Sciences and Technology

Volgenau School of Engineering

IT 467 Network Defense
Fall 2017

Common Syllabus

revised 8/10/2017

This syllabus contains information common to all sections of IT 467 for the Fall 2017 semester. Information specific to each section will be made available to registered students via the Blackboard course management system.

University Policies

The University Catalog is the central resource for university policies affecting student, faculty, and staff conduct in university affairs. Unless explicitly noted, any conflict between the policies in the University Catalog and the content of this document is unintentional. Please notify the author to resolve any such conflicts.

Please note that the Academic Year runs from the Fall semester of one calendar year through the Spring and Summer semesters of the following calendar year. Please be sure to select the correct archived Catalog if appropriate.

Scheduled Sections

Section	Instructor	Campus	Day	Time
001	Prof. Lyons	Science and Technology	Wednesdays	7:20–10:00 p.m.

Course Description

From the University Catalog:

> **IT 467:** *Network Defense.* 3 credits.
>
> Practices and procedures for defending business-class, heterogeneous networks against threats (including system failure, environmental events, human error) and attacks (including intrusion, malicious software, denial of service). Through practical lab sessions, students receive real-world experience designing networks, installing and configuring system components, detecting and recovering from problems and attacks, and gathering data to support prosecution of offenders and refinement of countermeasures. Offered by Info Sciences & Technology. Limited to two attempts.

Registration Restrictions:

Required Prerequisites: IT 366[C] and IT 223[B].
[C] Requires minimum grade of C.
[B] Requires minimum grade of B.

Enrollment is limited to students with a major, minor, or concentration in Applied Information Technology, Applied Science, Individualized Study, Information Technology or Infmtn Tchngy Entrepreneurship.

Students with the terminated from VSE major attribute may **not** enroll.

Schedule Type: Lecture

Prerequisites

The required grades must be achieved in each prerequisite course **before** a student is qualified to take this course. The prerequisite courses must be completed prior to, not concurrently with, this course.

This requirement will be **strictly enforced**. Any student enrolled in the course who has not meet the prerequisite requirements (or received a waiver) by the start of the semester will be dropped from the course and the student will be responsible for any consequences of being dropped.

Rationale

This course allows students substantial hands-on experience in network defense, complementing the study of network security theory and practice in IT 366 Network Security I and continued in IT 466 Network Security II. It is intended to satisfy student and employer demands for real-world practical experience that can be immediately applied in the workplace.

Lab work will be performed in small teams, each of which will be given a variety of servers and workstations running typical business software applications. Each team will be challenged to design and implement a network security infrastructure, then test it against real-world threats and attacks. Students must consider all possible threat types, including system failure, natural events, human error, and malicious attacks, any of which may originate outside the network or within it.

Students will learn a holistic approach to network security, from initial definition of requirements through design, implementation and testing of security practices and technologies, to on-going operation, maintenance and support activities. A protect/detect/react paradigm will be used to anticipate problems, attempt to defend against them, determine when defensive measures have failed, and take appropriate remedial action, including recovery and re-design. Students will learn how to collect and analyze data to enable early detection of problems, define requirements for system changes, notify support agencies (*e.g.* CERTs), and .support law enforcement efforts to apprehend and prosecute criminal offenders.

The content is relevant to students currently or expecting to be working in information security in business, government (especially homeland security), and law enforcement, especially in network security, vulnerability assessment, and penetration testing. Target audiences include George Mason University students and employees of businesses and agencies in the region.

Course Applicability

IT 467 is an option in the Information Security (INFS) concentration of the Bachelor of Science in Information Technology, and a Technical Focus Course in the Information Technology Minor and the Information Technology Undergraduate Certificate.

Objectives

On successful completion of this course, students will:

– Examine and document the network architecture of an information system.

– Identify potential flaws in a network design and recommend and justify changes to it.

– Create, configure, and operate a variety of computing platforms in a virtualized environment.

– Demonstrate real-world attacks against typical business platforms and applications.

– Implement defensive procedures to address potential vulnerabilities and attacks.

– Demonstrate the level of effectiveness of defensive procedures against real-world attacks.

Faculty and Staff

Course Coordinator:
Michael X. Lyons

Instructors:
See **Scheduled Sections** above

Teaching Assistants:
To be assigned – see Blackboard

Administrative support:
Department of Information Sciences and Technology
Fairfax campus
5400 Nguyen Engineering Building
Email: bsit@gmu.edu
Phone: 703-993-3565

References

Textbooks

There are no required textbooks for this course.
The Instructor will recommend appropriate references throughout the semester.

Grading

Grades will be awarded in accordance with the Mason Grading System for undergraduate students. See the University Catalog, Academic Policies, AP.3.1 Undergraduate Grading for more information.

The grading scale for this course is:

97 – 100%	A+	Passing
93 – 96%	A	Passing
90 – 92%	A-	Passing
87 – 89%	B+	Passing
83 – 86%	B	Passing
80 – 82%	B-	Passing
77 – 79%	C+	Passing
73 – 76%	C	Passing
70 – 72%	C-	*Passing**
60 – 69%	D	*Passing**
0 – 59%	F	**Failing**

* Grades of "C-" and "D" are considered passing grades for undergraduate courses. However:

- As of Catalog Year 2014-15 a minimum grade of "C" is required in all Concentration courses in the IT major. See the University Catalog for minimum grade requirements for other programs.

Raw scores may be adjusted by the Instructor to calculate final grades.

Final grades will be determined based on the following components:

Assignments	50%
Mid-term exam	25%
Final exam	25%

These components are outlined in the following sections.

Assignments

Individual and group work will be assigned in class several times during the semester. Each assignment will count towards the final grade - there are no "optional" assignments. Each assignment is to be prepared and submitted as specified by the Instructor.

Mid-term exam

The mid-term exam will be conducted during the 5th scheduled class session.

The mid-term exam will be based on topics addressed in Lectures 1-5, and will be "closed book" - no reference materials other than those provided with the exam paper will be permitted. Mid-term exams will be returned to students.

Final exam

The final exam will be held during the scheduled final exam session (see Fall 2017 Final Exams).

Please note that exams may be re-scheduled to compensate for disruptions in the semester schedule and ***students are required to be available throughout the exam period including the scheduled Make-up Day***.

The final exam will be based on topics addressed throughout the entire course and will be "closed book" - no reference materials other than those provided with the exam paper will be permitted. Final exams will be retained by the Department of Information Sciences and Technology and will not be returned to students.

Students are expected to submit work as scheduled by the Instructor. Any assignment submitted after the due date-time but within 24 hours of it will be graded with a penalty of 25% of the available credit. Any assignment submitted more than 24 hours late will not be graded. Exceptions to the submission time requirement may be made at the sole discretion of the Instructor.

Any student with an unexcused absence (including absence from part of a classroom session due to late arrival or early departure) will receive no credit for any assessment activity missed during that absence. A student arriving after an assessment activity has begun will not receive additional time to complete the activity.

A student with an exam conflict (or other circumstance that would justify rescheduling an exam under Mason policy), must notify the Instructor **no later than 2 weeks prior to the scheduled exam**.

Any student arriving more than 15 minutes late for an exam may be prohibited from taking the exam at the sole discretion of the Instructor.

Each student is required to present a current Mason ID in order to take an exam or other in-person assessment. No other form of identification is accepted. See the Mason ID Web page website for information on obtaining a card.

Mid-term and final grades will be posted to PatriotWeb, which is the only mechanism for students to obtain those grades. A student with a "hold" on his/her PatriotWeb account will be unable to access grades until the hold has been removed by the Registrar.

Schedule

Lecture	Content
1	Introductions, Logistics, Overview Information system architecture; Network partitioning
2	Introduction to virtualization
3	Physical and infrastructure security Reconnaissance, footprinting
4	Firewalls Access control, user authentication Intrusion detection and prevention, logging and auditing, incident reporting
5	Platform security Review for mid-term exam
6	**Mid-term exam** Team work
7	Malicious software – Trojan horses, viruses, worms, bots
8	Malicious software – buffer overflows, root kits
9	Code injection attacks
10	Denial of service attacks
11	Protocols and standards IP Security, SSL/TLS, S/MIME
12	Authentication applications Kerberos, X.509, federated identity management
13	Guest lecture
14	Review for final exam
-	**Final exam**

This schedule is subject to revision before and throughout the course.
Registered students should see Blackboard for the latest class schedule.

If a class is cancelled due to closure of a University campus or similar circumstance:

- The Provost may schedule a Make-Up Day, in which case the cancelled class will be held on that day, at the usual class time and in the usual classroom unless otherwise advised. Please note that the Make-Up Day may be on a different day of the week from the usual class day.
- If the Provost does not schedule a Make-Up Day the Instructor will schedule an *ad hoc* make-up session. The make-up session may be online – students will need Internet access and a compatible browser in order to participate in real time, but the session will be recorded for later viewing.

Important Dates

Please see the Fall 2017 Calendar for important dates, including the last days to add and drop courses.

Religious Holidays

A list of religious holidays is published by University Life. Any student whose religious observance conflicts with a scheduled course activity must contact the Instructor ***at least 2 weeks in advance*** of the conflict date in order to make alternative arrangements.

Attendance Policy

Students are expected to attend every class, to complete any required preparatory work (including assigned reading – see **Schedule** above) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor as soon as possible if they miss any class without prior notice. Any student who expects to miss more than one class session is **strongly advised** to drop the course and take it in a later semester when he/she can attend every class.

Mason policy AP.3.10 requires students to take exams at the scheduled time and place, unless prior approval is granted by the student's academic dean or director. An unexcused absence from an exam will result in a score of zero (0) for that exam. Please note that exams may be re-scheduled by the Registrar to compensate for disruptions in the semester schedule and ***students are required to be available throughout the exam period including the scheduled Make-up Day***.

Classroom conduct

Students are expected to conduct themselves in a manner that is conducive to learning, as directed by the Instructor. Any student who negatively impacts the opportunity for other students to learn may be asked to leave the classroom.

Electronic devices are potential distractions in the classroom environment. All electronic devices must be turned off or set to "silent" mode at all times unless the Instructors directs otherwise. In order to maximize student engagement the Instructor may prohibit use of such devices.

Communications

Registered students will be given access to a Blackboard section for this course. Blackboard will used as the primary mechanism (outside of lectures) to disseminate course information, including announcements, lecture slides, homework and other assignments, and scores for homework and exams. Some announcements may be sent via Blackboard to students' Mason email accounts.

Communication with the Instructor on issues relating to the individual student only should be conducted using Mason email, via telephone, or in person - ***not*** in the public "Discussions" forums on Blackboard. To protect student privacy any communication related in any way to a student's status must be conducted using secure Mason systems – if you use email to communicate with the Instructor you ***MUST*** send messages from your Mason email account. Students must activate and monitor their Mason email accounts to receive important information from the University, including messages related to this class.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided in Blackboard as a courtesy to students *provided acceptable attendance is maintained*.

All course materials (lecture slides, assignment specifications, *etc*) are published on Blackboard in Adobe® Portable Document Format (PDF). This allows users of most computing platforms to view and print these files. Microsoft® Word (or a compatible word processing application) is required for preparing assignments – it is available on computers in the Mason open labs.

Online sections will use several tools through the Blackboard course management system. Students are responsible for obtaining Internet access and a compatible platform. Appropriate computers are available on campus in open labs.

Privacy

Instructors respect and protect the privacy of information related to individual students.

As described above, issues relating to an individual student will be discussed via email, telephone or in person. Instructors will not discuss issues relating to an individual student with other students (or anyone without a need to know) without prior permission of the student.

Homework, quizzes, mid-term exams and other assessable work will be returned to individual students directly by the Instructor (or by a faculty member, staff member, or Teaching Assistant designated by the Instructor, or via another secure method). Under no circumstances will a student's graded work be returned to another student.

Instructors, staff, and Teaching Assistants will take care to protect the privacy of each student's scores and grades.

Disability Accommodations

Disability Services works with disabled students to arrange for appropriate accommodations to ensure equal access to university services. Any student with a disability of any kind is strongly encouraged to register with Disability Services as soon as possible and take advantage of the services offered.

Accommodations for disabled students ***must*** be made in advance – Disability Services cannot assist students retroactively. Any student who needs accommodation should contact the Instructor no later than the first class.

Campus Notifications

Students are encouraged to subscribe to the Mason Alert system to receive notifications of campus emergencies, closings, and other situations that could affect class activities.

Each classroom has a poster explaining actions to be taken in different types of crisis. Further information on emergency procedures is available at the Emergency Management Web site. In the event of a possible emergency, students are encouraged to dial 911.

Other Resources

Mason provides many useful resources for students.
The following resources may be particularly useful:

- The Writing Center
- The Academic Advising Center
- The University Libraries
- Counseling and Psychological Services
- University Career Services

See `http://www.gmu.edu/resources/students/`
for a complete listing of Mason resources for students.

Academic Integrity

All members of the Mason community are expected to uphold the principles of scholarly ethics.

The IT major bas been designed to achieve several specific outcomes. One of those outcomes is: "*An understanding of professional, ethical, legal, security, and social issues and responsibilities.*"

Graduating students are bound by the ethical requirements of the professional communities they join. The ethics requirements for some of the communities relevant to IT graduates are available via the following links:

- ACM Code of Ethics and Professional Conduct
- IEEE Code of Ethics
- EC-Council Code of Ethics

On admission to Mason, students agree to comply with the requirements of the Mason Honor Code and System. The Honor Code will be **strictly enforced** in this course. Honor Code cases are heard by a panel of students – students who meet the requirements are encouraged to nominate themselves to serve on the Honor Committee.

Any use of the words or ideas of another person(s), without explicit attribution that clearly identifies the material used and its source in an appropriate manner, is **plagiarism** and will not be tolerated. The Instructor reserves the right to use manual and/or automated means (including such services as SafeAssign) to detect plagiarism in any work submitted by students for this course, and to direct Teaching Assistants and/or other faculty and/or staff members to do likewise in support of this course.

For this course, the following requirements are specified:

- All assessable work is to be prepared by the individual student, unless the Instructor explicitly directs otherwise.
- All work must be newly created by the individual student for this course for this semester. Any usage of work developed for another course, or for this course in a prior semester, is strictly prohibited without prior approval from the Instructor.

Students may seek assistance with assigned work (and are encouraged to do so if they feel the need), ***provided***:

- The directions for the assigned work do not prohibit such assistance.
- Such assistance is ***explicitly acknowledged*** in the submitted work, clearly identifying the person(s) giving assistance and the nature of the assistance given.
- Any work to be submitted is prepared entirely and exclusively by the student submitting it. Students are expressly prohibited from sharing any assessable work for this course in any manner with other students (except students assigned as Teaching Assistants or Undergraduate Peer Mentors to this course and the student's section), unless all students involved have had their work graded and returned by the Instructor, or the Instructor has explicitly approved such sharing.

Another aspect of academic integrity is the free exchange of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. Please see the Mason Diversity Statement for more information on this topic.

Students are encouraged to ask for clarification of any issues related to academic integrity and to seek guidance from the Instructor, other faculty members, academic advisors, or the Office for Academic Integrity.

