**MET CS 690**

**Network Security**

**Instructor**

Edward Matthews, DB Security, DB Concepts, Python
Part time instructor, Computer Science Department Metropolitan College Boston University

**Office hours:** By prior arrangement.

**E-mail:** ematth01@bu.edu; matthews44@gmail.com

## **Course Description**

This course covers advanced network security issues and solutions. The course starts with consideration of why network security is necessary, network vulnerabilities and the types of attacks networks need to defend against. Discussion of basic security concepts, security services, and the role played by encryption and hash algorithms. Along with issues and approaches for key management follow. Particular focus and emphasis are then covered regarding to network security capabilities and mechanisms (Access Control on wired and wireless networks), IPsec, Firewalls, Deep Packet Inspection and network flow monitoring. A discussion of network application security (Email, Web, P2P, etc.) is presented followed by consideration of network utility (DNS, NTP, etc.) and management protocols (SNMP, RMON, etc.), management tools (Syslog, vulnerability scanning, penetration texting, etc.). Followed by a review of necessary operational security processes and activities. Discussion of remote access issues, such as dial-up servers, modems, VPN gateways and clients are included, as with the basic security concepts of cloud security.

**Learning Outcomes**

Upon successful completion of this course, each student should be able to

1. Explain the key concepts and actions taken to protect, monitor, analyze, detect and respond to unauthorized access to computer networks.
2. Assess the key concepts of network defense tools, their application, importance, and configuration to allow a company to successfully evaluate and implement them to alleviate vulnerabilities and defend against attacks.
3. Identify applicable security policies and procedures to properly secure and protect a network.
4. Evaluate network operational procedures and their implementation and impact to network security.
5. Identify different types of network defense mechanisms and design, and their applications. Understand the concept of VPNs and their implementations, as well as their advantages and limitations. Understand the security concepts of firewalls and other network security mechanisms.
6. Explain the fundamental concepts of Network / Cyber defense discipline using industry-wide vocabulary and common acronyms.
7. Describe the importance and interactions of people, processes, and systems to successful implementation of network security.
8. Explain different types of network attacks and apply their mitigation mechanisms.
9. Explain the importance of network defense tools, and be able to detail a risk assessment inclusive of detection and remediation.

**Prerequisites**

* MET CS535 or MET CS625 Data Communications and Computer Networks;
* Familiarity with the OSI and TCP/IP protocol stacks.
* Familiarity with binary numbers, prime numbers. Base conversion between binary, hexadecimal, and decimal numbering systems.
* Familiarity with computer programming concepts.

**Required Course Book**

**Computer & Internet Security – A Hands-on Approach**, Wenliang Du, 2nd Edition, Independently published, May 2019, ISBN 978-1-7330039-3-3

**Introduction to Network Security – Theory and Practice,** Jie Wang, Zackary Kissel**,** 2nd Edition, John Wiley and Sons, 2015, ISBN 978-1-1189-3948-2

(Students have access to this through the BU Library and can download the eCopy of the text. )

**Courseware**

This course uses Online Campus (Blackboard). Once the course starts all students must use the Online Campus Dashboard internal messages service.

Use Online campus:

* for reading assignments beyond textbook assigned reading,
* Submitting homework assignments,
* Submitting lab exercises,
* Taking on-line quizzes,
* Participating in discussion threads
* Taking the on-line final examination and practice final exam
* All course related email correspondence.

**Class Policies**

1. Assignment, Lab Exercise and Discussion Completion & Late Work
* Homework assignments are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable to submit an assignment by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.
* Lab exercises: are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. If a student will be unable to submit a Lab exercise by its due date, the student must contact the Instructor or Facilitator **in advance** to avoid a grade of zero (0) on the submitted material.
* Student postings to discussion topic after the listed closing dates will not be counted when calculating a student’s discussion grades.
1. Academic Conduct Code – Cheating and plagiarism will not be tolerated in any Metropolitan College course. Such activities/behavior will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

<http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html>.

Such activities/behavior includes copying (even with modifications) of another student’s work or letting your work to be copied. Your participation in interactions with the instructor and your classmates is encouraged, but the work you submit must be your own. Collaboration is not permitted.

**Assignments**

* All homework assignments are identified within the Online campus Class specific site.
* File names for assignment documents should be:

 CS690-HW<number>-<student last name>.doc

 An example assignment document file name is:

 CS690-HW5-Matthews.doc

Student submissions which fail to follow this direction will have 5 points deducted!

* Student assignment submissions must be no more than 4 pages in length, be single spaced**,** use 12 point Times Roman type font and 1” margins on all sides. Student submissions which fail to follow this direction will have points deducted!
* Include the file name in the header and a page number in the footer of you assignment submission document. Student submissions which fail to follow this direction will have points deducted!
* Title cover pages are not required and should not be used;
* Assignment submission documents MUST be in Word 2016 or greater file formats that are NOT encoded in XML;
* Quoted material and citations must follow the American Psychological Association (APA) format with a reference section at the end of a student’s submitted work. Please refer to the <http://www.apastyle.org/> web site for guidance on following the APA style guide.
* Students are required to comply with the directions contained within the document
 **APA Criteria for Course.pdf**
whenever the work of others is used as part of a student’s assignment submission. Failure to do so will result in points being deducted for the assignment grade.
* Wikipedia is a useful starting point for finding information about a subject BUT NOT an acceptable direct reference source. One should only reference or quote from primary (source) documents.

Lab Exercises

* Lab exercises are identified within the Assignment description document for each course module. Labs #2 & #3 are SEED labs which require an Ubuntu virtual machine be setup with the lab environment. Please visit the SEED lab site for more detail - https://seedsecuritylabs.org/.
* File names for lab exercise documents should be:

 CS690-LAB<number>-<student last name>.doc

 An example lab exercise document file name is:

 CS690-LAB5-Heister.doc

Student submissions which fail to follow this direction will have 5 points deducted!

* Students should enter their lab exercise answers direct within each lab exercise document and then submit the completed document appropriately renamed as stated above;
* Lab exercise submission documents MUST be in Word 2016 or greater file formats that are NOT encoded in XML.

Discussion Threads (online class only)

* Each course module includes a discussion topic that students are required to participate in. Student discussion postings will be graded as per the “Discussion Grading Rubric” under the Online Campus “ Syllabus and Course Information” area.

In Class Presentation (on campus class only)

* Students will sign up to give a 5-10 minute presentation about an advanced topic or a news item. To be discussed further in class.

Examinations

* Students are required to take six on-line quizzes (one per module) while the course is running. Students will be allowed 75 minutes to complete each quiz. A student may take each of these quizzes in the window that they are available via Online Campus If a student cannot complete a quiz during the week each quiz is available, the student must make prior arrangements with the instructor.
* Students are required to take a proctored final exam that will last 3 hours. This exam is open book and open notes.
* A practice final exam will be available on Online Campus which can be taken as many times as a student wishes.
* If any work is to be completed beyond the scheduled dates of this course the student must negotiate a Boston University "Contract for an Incomplete Grade" with the professor prior to the end of the class.

**Grading Criteria**

Students will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

Grades will be based on:

* homework assignments (25%)
* quizzes (20%)
* lab exercises (15%)
* discussion thread/class participation (10%)
* proctored final exam (30%)

Grade ranges are as follows:

* + 94 <= is an A
	+ 90 <= and < 94 is an A-
	+ 87 <= and < 90 is a B+
	+ 84 <= and < 87 is a B
	+ 80 <= and < 84 is a B-
	+ 77 <= and < 80 is a C+
	+ 74 <= and < 77 is a C
	+ 70 <= and < 74 is a C-
	+ 60 <= and < 70 is an F

**Course Outline**

**Module 1**

**Lecture 1** Why network security is needed, The different ways security is commonly discussed, Process of information security governance, The concept of defense in depth.

**Lecture 2** – Foundation concepts: security services and controls Access control concepts, Asset inventory, classification concepts, vulnerabilities, threats and risks.

Assignments: Assignment 1, Quiz 1, Discussion 1

**Module 2**

**Lecture 3 –** Concept of encryption, Forms of symmetric and asymmetric encryption, cryptographically secure hash algorithms,

**Lecture 4 –** The need for encryption key management, key distribution approaches including Diffie-Hellman key negotiation, and Public Key Infrastructures.

**Assignments**: Assignment 2, Lab 1, Quiz 2, Discussion 2

**Module 3**

**Lecture 5 -** Role of Cryptography in Security to provide authentication, confidentiality and data integrity, Authentication Systems: Single Sign-on and XML, Kerberos and Shibboleth Based Authentication.

**Lecture 6 –** Traditional networking architectures, Types of networks (LANs, MANs, WANs), Network physical layer and data link layer attacks and defensive mechanisms available (IEEE 802.1ae, 802.1x).

**Assignments**: Assignment 3, Lab 2, Quiz 3, Discussion 3

**Module 4**

**Lecture 7 –** The Insecurity of ARP, IP and other network layer protocols covering vulnerabilities and protocol internal security mechanism. Network layer attacks and defensive mechanisms available (IP security, packet filtering firewalls).

**Lecture 8 –** Transport layer protocols, vulnerabilities, attacks and defensive mechanisms available (TLS-DTLS-SSL, SSH).

**Assignments:** Assignment 4, Lab 3, Quiz 4, Discussion 4

**Module 5 –**

**Lecture 9 –** Multi-protocols layer attacks and defensive mechanisms (Application gateway firewalls, Deep pack inspection, network flow monitoring, Honey Pots).

**Lecture 10 –** Cloud Security.Web and Electronic mail vulnerabilities, attacks and defensive mechanisms (digest authentication, TLS, PGP-GPG).

**Assignments:** Assignment 5, Quiz 5, Discussion 5

**Module 6**

**Lecture 11 –** Mobile Security, Peer-to-peer, Instant Messaging, Domain Name System, Network Time vulnerabilities, attacks and defensive mechanisms (Session Boarder Controls, DNS SEC, malware scanning).

**Lecture 12 –** Security in management protocols**,** Network Security management tools (Syslog and log management, vulnerability scanning, Security Event and Information Management, Penetration Testing), Network Operations Security (OpSec) and OpSec compliance.

**Lecture 13 –** Course review.

**Assignments:** Assignment 6, Quiz 6, Discussion 6

**Non-required textbooks and references good for further study**

*The following books are* **NOT** *required for this course. However you will find each to be valuable resources to anyone involved in the Information Security area.*

1. **Practical UNIX & Internet Security**, 2nd Edition, ,Simson Garfinkel and Gene Spafford: O'Reilly, 1996
*This book is a classic for its very detailed treatment of general networking security and hardening of unix typs operating systems and is still relevant today.*
2. **Hacking Expose Network Security Secrets & Solutions**, 2nd Edition, Joel Scambray, Stuart McClure, and George Kurtz, McGraw-Hill, 2001
*This book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.*
3. **Security Engineering; A Guide to Building Dependable Distributed Systems**, Ross Anderson, Wiley, 2001
*This book is an interesting collection of discussions on security engineering and associated challenges.*
4. **Computer Related Risks,** Peter G. Neumann, Addison-Wesley, 1995
*This book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.*
5. **Applied Cryptography**, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996
*This book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.*
6. **Computer Security**, Dieter Gollmann, 2nd ed, John Wiley, 2006
*This book provides depth coverage of computer security and is highly recommended.*
7. **Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance**, Stuart Jacobs, IEEE Press Series on Information and Communication Networks Security, Wiley-IEEE Press; 1 edition, ISBN-10: 0470565128, ISBN-13: 978-0470565124
*The above book covers the subject area of information security from an engineering perspective*