CMSC 414: Computer and Network Security
Spring 2022 Course Syllabus

Instructor: Dr. Irfan Ahmed
Office Location: ERB 2323
Office hours: Tuesday and Thursday between 3:00 pm and 4:00 pm
or by appointment.
Email: iahmed3@vcu.edu

Overview (Catalog Course Description):
Semester course; 3 lecture hours. 3 credits. This course covers a wide range of computer network attacks and defenses.

Course Prerequisites:
CMSC 312 - Introduction to Operating Systems

Class Meeting:
Room 0301 in Engineering Building West

Textbook:
- *Network Security Essentials: Applications and Standards* by William Stallings, Pearson; 6th edition, 2016
- *Computer Networking: A Top-Down Approach* by James Kurose and Keith Ross, Pearson; 7th edition, May 2016

Reference Books:
- *Penetration Testing: A Hands-on Introduction to Hacking* by Georgia Weidman, 2014
- *Black Hat Python: Python Programming for Hackers and Pentesters* by Justin Seitz; No Starch Press; 1st edition; Dec, 2014
- *Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation* by James Forshaw; 1st Edition, Dec 2017
- *Hacking Exposed 7: Network Security Secrets and Solutions* by Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Education; 7 edition, 2012

Grading:

Midterm Examination	15%
Final Examination	15%
Assignments	50%
Project	20%

Grading Scale:
The following grading scale is used. I never curve. Grading in college courses is objective and based directly on your performance. Please don't ask me to change your grade on an assignment unless you clearly deserve it and can demonstrate that this is the case.

A	**90-100**	**B**	**80-89**	**C**	**70-79**
D	**60-69**	**F**	**0-59**		

Tests:
There will be one midterm and one final. The final examination is based on the material covered after the midterm. Any missed test will receive a grade of zero unless arrangements are made with me.

Midterm Exam Date: Thursday, March 17
Final Exam Date: Tuesday, May 10

Assignments: There will be significant laboratory/programming assignments in this course. You should consider the due date for each assignment to be a hard deadline. When the due date arrives, turn in what you have. I do give partial credit, but **late submissions are not accepted.** Submission procedures will be discussed in class.

Project: You will develop a security project during the semester. The project should involve the ***demonstration*** of a cyberattack, and/or ***development*** of a working prototype of a security solution (that can be borrowed from an existing popular tool, or a research paper, or it can be your own idea).

You will have to perform the following steps: register a team, submit a project proposal, and then a progress report and finally, project deliverables (presentation slides and demo video). You gain allocated marks for each completed step. Details are as follows:

Team Registration: ***(One Mark)***
You will have to register your project and team members. The excel sheet is available at Google Docs at [ ].
(Copy-paste the link on your browser if the link does not work)

Proposal: ***(Four Marks)***
Initially you will submit a ***2-page proposal*** for the project that I will review and approve.

The proposal ***must*** have the following sections:

- Objective or main idea of the project
- List of tasks along with their description, and execution and completion timeline
- Evaluation approach of the prototype to verify that your attack or solution works
- Name and student IDs of group members
- Role and work scope of each group member

You can work on the project in a team of up to three members.
Progress Report: ***(Three Marks)***

- 50% work must be completed by the due date of this report.

- It should contain the following:
    - Project Objectives
    - The approach that you are working on
    - List of tasks with their descriptions
    - what tasks have been completed and what are left to be done.

Project Deliverables: I expect two deliverables:
1) a detailed presentation slides in pdf format ***(Six Marks)***
2) a demo video ***(Six Marks)***
The slides should contain
- Sufficient background information
- Project Objectives
- Details of the approach that you want to implement
- List of tasks with their descriptions
- Implementation Details
- Evaluation Results

Important Dates:
Team Registration Deadline: February 3, Thursday
Proposal Submission Deadline: March 1, Tuesday
Progress Report Deadline: April 5, Tuesday
Project Submission Deadline: April 25, Monady

Class Materials: The lecture slides will be available via *Canvas*. Be sure to check the *Canvas* site frequently, http://canvas.vcu.edu/.

Major Topics Include:
- Computer Networks and Internet Overview
- Network TCP/IP Stack and Attacks
- Firewall, and Network Intrusion Detection and Prevention System
- Cryptographic Tools
- Network Penetration Testing Primer

Tentative Lecture Schedule:

Date	Slide set	Topics
Tues, Jan 18	Overview of Computer Security	- CIA Triad - Computer Security Challenges and Strategy
Thu, Jan 20	Computer Networks and the Internet	- Internet structure - Network core
Tues, Jan 25	Computer Networks and the Internet	- Internet protocol stack
Thu, Jan 27	Application Layer Attacks	- Socket programming in Python - Wireshark to capture and analyze packet

	Assignment 1	- **Network Application Development and Wireshark Analysis**
Tues, Feb 1	Application Layer Attacks	- Python Programming for Hackers and Pentesters
Thu, Feb 3	Application Layer Attacks	- HTTP - Slowloris - Shellshock
Tues, Feb 8	Application Layer Attacks	- DNS: domain name system - Source Address Spoofing - Reflection & Amplification Attacks
Thu, Feb 10	Application Layer Attacks	- Botnet and Zeus - Rootkits (FU and *Basic_6*)
	Assignment 2	- **Bot Infection Analysis**
Tues, Feb 15	Application Layer Attacks	- Industrial Control Systems - Modbus Protocol and Vulnerabilities
Thu, Feb 17	Application Layer Attacks	- Subverting PLC Password Protection - Control Logic Injection Attacks - Real-world ICS Attacks
Tues, Feb 22	Transport Layer Attacks	- Multiplexing/demultiplexing - UDP: User Datagram Protocol
	Assignment 3	- **Network Data Breach Investigation**
Thu, Feb 24	Transport Layer Attacks	- TCP: Transmission Control Protocol - Port Scanning Attacks - TCP Reset Attack
Tues, Mar 1	Transport Layer Attacks	- SYN Spoofing - TCP Session Hijacking Attack
Thu, Mar 3	Transport Layer Attacks	- TCP Sequence Prediction Attack - Tiny Fragment Attack
Mar 8	**Spring Break**	
Mar 10	**Spring Break**	
Tues, Mar 15	**Review before Midterm**	
Thu, Mar 17	**Midterm Exam**	
Tues, Mar 22	Network Layer Attacks	- *Forwarding and routing* - IP fragmentation - Teardrop Attack
Thu, Mar 24	Network Layer Attacks	- DHCP: Dynamic Host Configuration Protocol - NAT: network address translation - ICMP: internet control message protocol - Ping of Death Attack - Smurf Attack
Tues, Mar 29	Link Layer Attacks	- ARP: address resolution protocol - ARP Spoofing and Ettercap
Thu, Mar 31	Link Layer Attacks	- Ethernet switch - Ethernet CSMA/CD

		- MAC Flooding
Tues, April 5	Firewall and Intrusion Detection and Prevention System	- Intrusion Detection Systems - Host and Network-Based IDS
	Assignment 4	- **Snort Rules**
Thu, April 7	Firewall and Intrusion Detection and Prevention System	- Honeypot - Snort - Firewall
Tues, April 12	Cryptographic Tools	- Symmetric Encryption - Message Authentication
Thu, April 14	Cryptographic Tools	- Kerberos
	Assignment 5	- **Public Key Authentication using SSH Server**
Tues, April 19	Cryptographic Tools	- Public Key Encryption - Public Key Certificate - Digital signature
Thu, April 21	Network Penetration Testing Primer	- Information Gathering - Finding Vulnerabilities
Tues, April 26	Network Penetration Testing Primer	- Attacks and Exploitation
April 28 and May 3	Project Demos of Selected Class Projects	
May 5	**Review before Final Exam**	
May 10	**Final Exam**	

Learning objectives/outcomes

At the end of the course, students will be able to understand network security concepts, and different cyberattacks and their countermeasures. The course will also prepare the students for advance network security courses at graduate level.

Technology Support

Engineering & VCU Resources:

- **Personal Computer Requirement**: For our current system requirements and recommendations, see: https://egr.vcu.edu/admissions/accepted/computer-recommendations/
- **Remote Access to Public Lab computers**: To provide remote access, we use the Citrix App2Go environment to provide full and exclusive control over "the next available" computer in the lab. See this link for more details: https://wiki.vcu.edu/x/Oa0tBg

- **VCU provides a lot of software available for students to download to their personal computers.** For a list of software and the specifics for each, see: https://ts.vcu.edu/software-center/. In particular, Microsoft Office is available free to students.
- **VCU is transitioning to Canvas.** See the Canvas Student Guide at this link: https://community.canvaslms.com/t5/Student-Guide/tkb-p/student
- **For IT help in the College of Engineering**, see our Wikipedia for "student" help at: https://wiki.vcu.edu/display/EGRITHELP
- **VCU's Technology Services (TS) provides support for "central IT" services**. If you have a technical issue with any of the following services, please submit a ticket with VCU Technology Services at https://itsupport.vcu.edu/ or call (804) 828-2227. VCU TS maintains and supports these services and will be able to provide assistance to you.
    - VCU Cisco VPN
    - 2Factor or Dual Authentication (DUO)
    - Blackboard/Canvas
    - Gmail or other Google Apps
    - Zoom videoconferencing
    - VCU App2Go (Application server)
    - Resetting VCU password
- **For IT issues related to College of Engineering teaching and research, email egrfixit@vcu.edu**
- **For loaner Chromebooks for emergency purposes:** See this link for more details: https://vcutsmpc.getconnect2.com/