



DFORS 780 (Exploring the Darknet) 2021 Fall

Meeting Times: Wednesdays, 4:30 – 7:10 PM

Meeting Dates: August 25 - December 1, 2021

Meeting Location: Nguyen Engineering Building, Room 4457

Instructor: Prof. David Vargas, MS, CISSP, CISM, CEH

Contact Info: dvargas7@gmu.edu

Office Hours: As needed (to help students succeed, the instructor can make himself available before class, after class, via email, and/or via phone)

Course Description: This course is an introduction to a misunderstood part of the Internet known as the Darknet. While often considered a safe-haven for those committing cybercrime, it is also a place where dissidents and other well-meaning individuals can relay their message anonymously. Because of how the Darknet is used by cybercriminals and nation-states for malicious purposes, understanding its operation, protocols and architecture is crucial for those working in security.

Course Objectives: At the conclusion of this course, students will:

- Have a complete understanding of the Darknet and how it differs from the Surface Web
- Be able to describe and work with the individual components and protocols that make up the Darknet
- Understand how the TorBrowser anonymizes web surfing on the Darknet
- Know exactly how cybercriminals and nation-states use the Darknet for malicious purposes
- Be able to describe how law enforcement tries to deanonymize criminal activity on the Darknet

Honor Code: The Mason Honor Code is in effect <http://oai.gmu.edu/honor-code/masons-honor-code/>

- Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

Mason Calendar: https://registrar.gmu.edu/calendars/fall_2021/

Prerequisites: Knowledge of local and wide area networking

Schedule:

Week	Date	Content	Readings and Other Assignments	In-Class Labs and Exercises
1	Aug 25, 2021	Introduction <ul style="list-style-type: none"> Syllabus Review Student and Faculty Introductions Introduction to the Darknet 	-Supporting Materials	NA
2	Sep 1, 2021	Crimes on the Darknet <ul style="list-style-type: none"> Drugs Child Exploitation Hitmen Etc Nation-States as Cybercriminals <ul style="list-style-type: none"> North Korea China Foundation Technologies <ul style="list-style-type: none"> Virtualization for the Darknet Introduction to VirtualBox 	-Supporting Materials -Case Study: Playpen -Homework: Dangers of the Dark Web: Murder for Hire (https://art19.com/shows/crime-stories-with-nancy-grace/episodes/68c869e8-a715-4496-a9ae-6fa3d2ac3a3d/embed)	Labs: -Create Power Off and Delete VMs in VirtualBox -Install Kali Linux -Navigate the Kali GUI
3	Sep 8, 2021	Foundation Technologies <ul style="list-style-type: none"> VM Snapshots Virtual Networking 	-Supporting Materials	Labs: -Create Snapshots in VirtualBox -Configure Virtual Networking in VirtualBox for Windows

4	Sep 15, 2021	Darknet <ul style="list-style-type: none"> • TorBrowser 	-Supporting Materials	Labs: -Enter the Darknet with TorBrowser -Configure Tor Browser Weekend: Quiz #1 (1-4 Labs)
5	Sep 22, 2021	Darknet <ul style="list-style-type: none"> • TorBrowser (cont) 	-Supporting Materials	Review: Quiz #1 Labs: -Introduction to Cookies for Cyber -Introduction to Browser Fingerprinting
6	Sep 29, 2021	Darknet <ul style="list-style-type: none"> • .onion Sites • Darknet Search 	-Supporting Materials	Labs: -Visit Darknet Sites -Search the Darknet
7	Oct 6, 2021	Darknet <ul style="list-style-type: none"> • Tor Network Architecture • Tor Metrics • Tor Traffic <ul style="list-style-type: none"> ○ Introduction to Wired Packet Capture ○ Introduction to Wireshark 	-Supporting Materials	Labs: -Wireshark Fundamentals -Work with Capture Files in Wireshark Weekend: Quiz #2 (5-7 Labs)
8	Oct 13, 2021	Midterm Exam (Sessions 1-7)		
9	Oct 20,	Review: Midterm Exam Darknet	-Supporting Materials	Review: Quiz #2

	2021	<ul style="list-style-type: none"> • Darknet Markets <ul style="list-style-type: none"> ○ Arrests and Takedowns ○ Cyber Bunker (Germany) <p>Underling Technologies</p> <ul style="list-style-type: none"> • TCP/IP • The Internet 	Case Study: Silk Road	Labs: -None
10	Oct 27, 2021	<p>Underlying Technologies</p> <ul style="list-style-type: none"> • Encryption <ul style="list-style-type: none"> ○ Going Dark (Law Enforcement vs. Industry) • Hashing 	<p>-Supporting Materials</p> <p>Homework: Carnegie Foundation’s “Moving the Encryption Policy Conversation Forward” (https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573)</p>	<p>Labs:</p> <ul style="list-style-type: none"> -Create Virtual Encrypted Disks with VeraCrypt -Homework: Encrypt Files and Folders with GPG on Linux -Introduction to Hashing with HashCalc on Windows -Introduction to Hashing on Linux <p>Weekend: Quiz #3 (9-10 Labs)</p>
11	Nov 3, 2021	<p>Underlying Technologies</p> <ul style="list-style-type: none"> • Digital Certificates • Digital Signatures • Transport Layer Security (TLS) 	-Supporting Materials	<p>Review: Quiz #3</p> <p>Labs:</p> <ul style="list-style-type: none"> -View Digital Certificates in Web Browsers -Introduction to Sysinternals Sigcheck for Cyber

12	Nov 10, 2021	Underlying Technology <ul style="list-style-type: none"> • Cryptocurrencies (Bitcoin, Monero, etc) • Blockchain • Cryptocurrency Scams <ul style="list-style-type: none"> ○ Onecoin and Dr. Ruja • Cryptomining Malware 	-Supporting Materials -Homework: The Blockchain Bandit: How \$54 million in Ethereum was Stolen (https://www.youtube.com/watch?v=HX8-BCfYBmU) -Homework: Missing Cryptoqueen Podcast - Onecoin (https://www.bbc.co.uk/programmes/p07nkd84/episodes/downloads)	Labs: -None
13	Nov 17, 2021	Tor Alternatives <ul style="list-style-type: none"> • Personal VPNs • DNS over HTTPS (DoH/DNS over TLS (DOT)) • I2P, Freenet 	-Supporting Materials	Labs: -Introduction to Personal VPNs -Introduction to Personal VPN WireGuard -Epic Privacy Browser Weekend: Quiz #4 (11-13 Labs)
14	Nov 24, 2021	No Class – Thanksgiving Holiday		
15	Dec 1, 2021	Final Exam (Sessions 9-13)		

**The instructor may alter the contents of this course at any time to customize the topics to the class or to integrate recent developments in the subject matter. Changes will be announced in class and/or on Blackboard as soon as possible.*

Evaluation and Grading

Assignment	Weight
Four (4) Quizzes	60%
Mid-Term Examination	20%
Final Examination	20%
Total	100%

Midterm and Final Exams: Are closed-book, closed-notes and will cover all topics covered to date. There will be two (2) exams. Exam questions are largely derived from lectures and textbook chapters. Exams will be administered on Blackboard. Exams cannot be taken after they are administered. To be fair to all students, and to protect the integrity of the exams, exceptions cannot be made.

Quizzes: Because in the cybersecurity field, it is important to both know and do, this course will include hands-on quizzes. Quiz questions are largely derived from the labs and the discussions surrounding the labs. Quizzes will be administered on Blackboard. Quizzes cannot be taken after they are administered. To be fair to all students, and to protect the integrity of the exams, exceptions cannot be made.

Online Lectures: In certain situations, we may have class online via Blackboard Collaborate. Students will be contacted by email ahead of time should a class be held online. Online classes will be recorded and saved for later review.

- Accessing Online lectures:
 - Follow instructions to login into Blackboard
 - Click on Tools
 - Click on Blackboard Collaborate Ultra
 - You should see the current session listed
 - Previously recorded sessions are accessed via the Previously Recorded Tab

Course Material: All course material will be available on Mason Blackboard.

- Getting on Blackboard:
 - Go to: <https://mymasonportal.gmu.edu/webapps/portal/frameset.jsp>
 - Login with your Mason Credentials
 - Click on the Courses tab
 - Click on the CFRS-780

Required Hardware: A USB drive is required. It will be used to save one's software and VMs (the lab's hard drives are wiped nightly).

Lab Computers: This course uses GMU lab computers. Please make sure that your computer is working properly prior to the start of class. If your machine is not working, please let the instructor know.

Required Readings and Reference Materials: All materials will be provided by the instructor via Blackboard.

Student Welcome: This link provides up-to-date information on IT services:
<http://labs.vse.gmu.edu/uploads/FacultyFAQ/StudentWelcome.pdf>

Disability Services: <http://itservices.gmu.edu/downloads/index.cfm>.

- Students with disabilities who seek accommodations in a course must be registered with the Mason Office of Disability Services (ODS) and inform the instructor, in writing, at the beginning of the semester. See <http://www2.gmu.edu/dpt/unilife/ods/> or call 703-993-2474 to access the ODS.

Note:

- ALL STUDENTS MUST HAVE GMU CREDENTIALS (EMAIL ACCOUNT) AND HAVE ACCESS TO <https://mymasonportal.gmu.edu> !!
- All Email Correspondence Will Take Place From Your GMU Account to dvargas7@gmu.edu!!!
- Students are responsible for all of the material in the course