DFOR 780 (Darknet Technologies)
2022 Fall

Meeting Times: Wednesdays, 4:30 – 7:10 PM
Meeting Dates: August 24 – November 30, 2022
Meeting Location: Nguyen Engineering Building, Room 5358

Instructor: Prof. David Vargas, MS, CISSP, CISM, CEH
Contact Info: dvargas7@gmu.edu
Office Hours: As needed (**t**o 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. The beginning of the course will focus on the Darknet itself while the remainder will focus on its underlying technologies.

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 Tor Browser 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_2022/

Prerequisites: Knowledge of local and wide area networking
Schedule:

Week	Date	Content	Readings and Other Assignments	In-Class Labs and Exercises
1	Aug 24, 2022	**Introduction** • Syllabus Review • Student and Faculty Introductions • Introduction to the Darknet	**-Supporting Materials** **-Homework:** Vice Cyber Podcast - "Drugs Cannabis and identity Theft - The Truth Behind the Dark Web" (Uploaded onto BB)	NA
2	Aug 31, 2022	**Crimes on the Darknet** • Drugs • Child Exploitation • Hitmen • Etc. **The Nation-State as Cybercriminals** **Foundation Technology (Accessing the Darknet Safely)** • Virtualization for the Darknet • Introduction to Oracle VirtualBox	**-Supporting Materials** **-Case Study:** Playpen **-Homework:** + 2022 FBI Internet Crime Report 2022 +Dangers of the Dark Web: Murder for Hire (https://art19.com/shows/crime-stories-with-nancy-grace/episodes/68c869e8-a715-4496-a9ae-6fa3d2ac3a3d/embed) **-Suggested:** +The Lazarus Hei$t (https://www.bbc.co.uk/programmes/w13xtvg9/episodes/downloads)	**Labs:** -Install VirtualBox on Windows -Create Power Off and Delete VMs in VirtualBox for Windows -Install Kali Linux in VirtualBox -Create Snapshots in VirtualBox
3	Sep 7, 2022	**Foundation Technology** • Virtual Networking in VirtualBox **Darknet** • Tor Browser	**-Supporting Materials**	**Labs:** -Configure Virtual Networking in VirtualBox for Windows -Navigate the Kali GUI -Enter the Darknet with Tor Browser on Windows

4	Sep 14, 2022	**Darknet** • Tor Browser (cont) ○ Review: HTTP Cookies ○ Fingerprinting ○ Anti-Fingerprinting ○ Anti-Detection Browsers	**-Supporting Materials**	**Labs:** -Configure Tor Browser -Create Portable Tor Browser -Introduction to Cookies for Cyber -Perform Browser Fingerprinting -Introduction to the Brave Privacy Browser -Anti-Detection Browsers -Anti-Fingerprinting with Vytal Chrome Extension **Weekend: Quiz 1 (1-4 Labs)**
5	Sep 21, 2022	**Darknet** • Visit Darknet Sites • Darknet Search **Other Darknet Access Methods** • Tails • Whonix	**-Supporting Materials**	**Review:** Quiz 1 **Labs:** -Visit Darknet Sites -Search the Darknet -Create Tails Boot ISO -Create Tails VM in VirtualBox -Introduction to Tails OS -Introduction to Whonix

6	Sep 28, 2022	**Other Darknet Access Methods (cont)** **Darknet** • Tor Network Architecture • Tor Metrics • Tor Traffic • Introduction to Wired Packet Capture • Introduction to Wireshark	**-Supporting Materials**	**Labs:** -Introduction to Tor Metrics -Wireshark Fundamentals -Work with Capture Files in Wireshark -Configure Capture and Display Filters in Wireshark -Capture and Analyze Tor Traffic with Wireshark

7	Oct 5, 2022	**Darknet**
		• Darknet Markets
		  ○ Arrests and Takedowns
		  ○ Cyber Bunker (Germany)
		
		Underlying Darknet Technologies
		• TCP/IP Protocols
		• Internet Architecture
			-Supporting Materials
			
			Case Study: Silk Road
				Labs:
				-None
				
				Weekend: Quiz 2 (5-7 Labs)

8	Oct 12, 2022	**Midterm Exam (Sessions 1-7)**		

9	Oct 19, 2022	**Review: Midterm Exam**
		
		Underlying Technologies
		• Encryption
		  ○ Going Dark (Law Enforcement vs. Industry)
		  ○ Store Now, Decrypt Later (SNDL)
		• Hashing
		• Encoding
			-Supporting Materials
			
			Homework: Carnegie Foundation's "Moving the Encryption Policy Conversation Forward" (https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573)
				Review: Quiz 2
				
				Labs:
				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 -Encode with Base64 on Linux for Cyber
10	Oct 26, 2022	**Underlying Technologies** • Digital Certificates • Digital Signatures • Transport Layer Security (TLS)	**-Supporting Materials**	**Labs:** -View Digital Certificates in Web Browsers -Run Sysinternals Sigcheck for Cyber **Weekend: Quiz 3 (9-10 Labs)**

11	Nov 2, 2022	**Cryptocurrencies and the Darknet**
		• Cryptocurrencies Introduction
		• Altcoins, Bitcoin, and Stablecoins
		• Blockchain
		• Cryptocurrencies and Cybercrime
		  ○ Onecoin and Dr. Ruja
		  ○ Cryptocurrency Mining Malware
		• Future
			-Supporting Materials
			
			-Special: Chainalysis 2022 Crypto Crime Report
			
			-Case Study: Welcome to Video
			
			-Homework:
			+The Blockchain Bandit: How $54 million in Ethereum was Stolen (https://www.youtube.com/watch?v=HX8-BCfYBmU)
			+Missing Cryptoqueen Podcast - Onecoin (https://www.bbc.co.uk/programmes/p07nkd84/episodes/downloads)
				Review: Quiz 3
				
				Labs:
				-Search the Blockchain

12	Nov 9, 2022	**Other Privacy Technologies** • Personal VPNs • DNS over HTTPS (DoH/DNS over TLS (DoT) ○ Review: DNS	**-Supporting Materials** **-Homework:** Don't Use a VPN...it's not the ultimate security fix you've been told (https://youtu.be/8x1BJCKwqpI)	**Labs:** -Introduction to Personal VPNs -Introduction to Personal VPN WireGuard
13	Nov 16, 2022	**Tor and Digital Forensics** **Tor Alternatives** • I2P, Freenet	**-Supporting Materials**	
	Nov 23, 2022	**No Class – Thanksgiving Holiday**		
15	Nov 30, 2022	**Final Exam (Sessions 9-13)**		**Quiz 4 (11-13 Labs)**

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 and 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