Eastern Time (US and Canada)

Online / Zoom Course Syllabus	
Course Name	Introduction to Cybersecurity
Couse Duration	12 weekends
Course Instructor	Dustin Fraser, CASP+, SSCP
Course Fees	
2-Day Weekend Bootcamp	Check website for current fees
12-Weekend Intensive Course	Check website for current fees
Course Start Dates	
2-Day Weekend Bootcamp	May to September 2021
12-Weekend Intensive Course	June to September 2021
Booking information	
2-Day Weekend Bootcamp	Online Booking
12-Weekend Intensive Course	Online Booking
Contact details	
Cyber Benab	events@cyberbenab.com

Course Description:

Cybersecurity has developed into a broad category of science & engineering with specific technology & practices to protect computers, communication networks, and data from harm, theft, or exploitation. It is an applied science, where the practice is ahead of the theory.

The Cyber Benab 12-weekend intensive course introduces students to the core tenets of cybersecurity, including:

- Confidentiality, integrity, and availability of systems, networks, and data
- Cryptography and its tactics
- Offensive capabilities across the cyber-kill-chain
- Psychology of malicious attackers and their methods
- Risk assessment and mitigation
- Systems dynamics and thinking
- Typical capabilities of computer systems and networking
- Defense-in-depth strategies

Course Objectives:

After this course, the student will have learned the following:

- The daily, operational meaning of "cybersecurity" for organizations
- Assessment of security situations, common vulnerabilities, and consequences of cybersecurity failures
- A high-level overview of crucial cybersecurity models like the CIA triad, NIST RMF, and ISO frameworks, all of which guide information assurance
- Essential computer-based tools and tactics used to identify, assess, and mitigate cybersecurity threats, using examples on Linux-based or Windows-based hosts

Key Sections of the Course Syllabus:

1. Core Foundations and Security of Today's Technology Infrastructure
2. Synopsis of Modern (Generalized) Frameworks for Cyber Security
3. Security in the Enterprise: People, Process, & Technology
4. Cyber Security Policy Development & Management
5. Synthesizing Together: Technologies and Defense in Depth Strategies

Course Outline:

Week	Topic/Assignment	Due Date
1	Introduction to First Principles of Cyber Security Computer Security: Third Edition Chapter 1 & 2 What is cybersecurity? Who practices it? Why study cybersecurity as a field? What is meant by the "security environment?" Common vernacular: risks, threats, vulnerabilities, and consequences? Learning the basics of computer hacking	TBC

	Being a Script Kiddy, Part 1	
2	Models & Frameworks for Cyber Security Computer Security: Third Edition Chapter 3 Introduce the basics of (general) models STAR CIA Triad Pakerian Hexad Introduce the basics of (general) frameworks NIST ISO COBIT Focusing on NIST and its basics Authentication, Authorization, Audit Role-based security	TBC
3	Tech & Security: The Threats Computer Security: Third Edition Chapter 4 & 5 What is the cybersecurity technical landscape? How are all communications and computer components interrelated? What is a risk, its threat vector(s), consequence? Let us see what these are using a computer ...	TBC
4	Tech & Security: The Tools (Part 1) Computer Security: Third Edition Chapter 6 & 7	TBC

	OS threats and tools Linux Windows Networking threats and tools WireShark	
5	Tech & Security: The Tools (Part 2) Computer Security: Third Edition Chapter 8 & 9 Network-based asset threats and tools Web Databases Wireless Firewalls Routers VPNs	TBC
6	Tech & Security: Incident Response (Part 1) Computer Security: Third Edition Chapter 10 &11 Using NIST RMF basics for Windows and Linux, using CLI Identify/Scope Protect/Defend Detect/Visibility Respond/Analysis Recover/Remediate	TBC
7	Tech & Security: Incident Response (Part 2) Computer Security: Third Edition	TBC

	Chapter 12 &13 Using NIST Framework basics for Windows and Linux, using CLI Review Identify, Protect, Detect, Respond, Recover Introduce tactics (tips & tricks) How to manage incidents (specifically on Windows, Linux, networking) Sys Internal Tools	
8	Security in the Enterprise Authentication, Authorization, Audit Role-based security Public Key Encryption Database & Storage Security Impact of moving to the Cloud	TBC
9	Security Policy Computer Security: Third Edition Chapter 14 &15 Start with value/asset inventory and classification Risk Assessment Policy development Risk Mediation	TBC
10	Synthesizing Together: Technologies and Defense in Depth Strategies Computer Security: Third Edition Chapter 16 &17	TBC

	Next steps after the course?	

Listen, Learn, Practice!

Cybersecurity Goals	**Competence**	**Confidence**	**Vocabulary**	**Psychomotor**
Knowledge	+	+	+	+
Skills	+	+	+	+
Abilities	+	+	+	+