Cyber Warfare – Defense & Attack –

Advanced Course

Course Outline

Module 0 Cybersecurity Awareness Training 40 hours	Module 1 Introduction 40 hours	Module 2 Cyber Defense Strategies 40 hours	Module 3 Cyber Operations 40 hours	Module 4 Deep delve into Cyber Threats 40 hours	Module 5 Monitoring & Detection 40 hours
Organization Security posture	**What is Cyber Security**	**Fundamental defense concepts**	**Organization and functionalities**	**Attacker Techniques**	**Log Management and Information Sources**
What is the organisation's security priority	Where it starts and where it stops	Conceptual framework for cyber defense Strategic Vs. Operational Cyberwar The goals of cyber defense Defense Architecture Defense Policy Defense Strategy Cyber Operations	People, Processes, and Technologies	Covering Identity Tunneling Techniques Fraud Techniques Social Engineering Tactics, Techniques and Procedures	Sources of Information Quality of Information
Executive Driven Cyber Security Agenda	**Recap on OSI Model**	**Cyber Deterrence**	**Identity and Access Management**	**Threat Infrastructure**	**Attack Indicators**
With the changing digital landscape what are the security implications	Layers of the cyber world and security implication	Defining Cyber Deterrence The unique nature of Cyber Deterrence A strategy of Response Cyber Retaliation	Goals, motivations, and guiding principles Access Controls mechanism AAA concepts IAM processes IAM technologies IAM best practices	Botnets DNS and Fast-flux	
Technology Advancement	**Importance of Security in the Cyber World**	**Cyber Resilience**	**Threat and Vulnerability Management**	**Exploitation**	**Automated Attack Detection Tools and Methods**
Where are we now	What are the foundations of cyber security	Principles for cyber Resilience Cyber Resilience Goals and Requirements Cyber Resiliency Engineering Mission Assurance Cyber Resiliency Framework	Goals, motivations, and guiding principles TVM processes TVM technologies Cyber TVM	Techniques to gain a foothold Disruption Methods	

		Cyber Resiliency Objectives Cyber Resiliency Practices Cyber Risk management Cyber Governance Cyber Defense program Maturity measurement Security Metrics			
Advanced Malware	**Networking Security**		**Security Configuration Management, Audit and Compliance**	**Malware essentials**	**SIEM's**
How easy it is to expose the company despite the best equipment	Securing your network and systems		Goals, motivations, and guiding principles CM processes and technologies Management platforms	Types of malicious code Anti-Forensics Techniques Persistence Techniques BIOS\CMOS\MBR Hypervisors Registry Entries and auto-startups Rootkits Spywares Privilege Escalation	Overview of the Functionality Presentation Layer Alarms and Thresholds Priorities Correlation
Method used for successful Cyber Attacks	**Introduction to cryptography**		**Security Continuous Monitoring**	**Stealing Information**	**Writing SIEM rules**
Shoulder surfing Spear-phishing Social Engineering Dumpster dive Baiting Tailgating and piggybacking Eavesdropping RFID theft Scareware	What you know to know about Cryptography to stay secure?		Network Security Architecture Network Security Monitoring Endpoint Security Architecture Automation and Continuous Security Monitoring		Best Practices Avoiding False Positives and Noise Case-studies
Nation State Hacking	**What is Kali Linux**		**Cyber Training and Simulation**		**Intrusion Attribution Framework**
How important it is for government to have teams that can hack for them	Tools that are necessary to start the cyber security journey		Goals, motivations, and guiding principles Types of Cyber simulations Building a Cyber Range Challenges Technologies Best Practices		Introduction and objectives of attribution Trace-back techniques Intrusion analysis Counter attack
Who are the other actors in the world	**Setting Kali Linux to start the Cyber Journey**				

What are the methods used to get access to your data?	Setting up virtual environments for Kali and configuring the cyber lab				
Attacking Timeline					
With the changing digital landscape what are the security implications					
1st Rule of Cyber Security					
Why this rule in the cyber world and the example?					