Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
	• Malicious insiders • Discovery • Footprinting and social engineering • Port scanning • Phishing • Metadata discovery • Exploitation and lateral movement ➢ Exploit packs and exploit generation ➢ Pass-the-Hash technology ➢ Enumeration • Payloads ➢ Rootkits ➢ RATs(NetBus, BackOrifice, "Poison Ivy") ➢ Botnets • Dos & DDos, • Buffer overflows &Ping of Death attacks • Programming basics for security professionals • Software vulnerabilities ➢ Windows OS vulnerabilities ➢ Linuxvulnerabilities • Embedded operating systems • Web application security: Code injection ➢ Server-side Injection ➢ Cross-site Injection and request forgery ➢ Web scrapping ➢ Fiddler, Burpsuite	reflection of on-line research, databases and industry inquiry.	
5. (3 weeks)	Cryptography • Understanding cryptography basics • One time pad perfect security proof • Understanding cypher methods, algorithms, and tools ➢ Block ciphers, CBC etc. ➢ Public key infrastructure and certificates ➢ Secure protocols (TLS, SSH) • Protocols for secure communications • Attacks on cryptosystems	Lecture Discussion, collaborative work. Critical reflection of on- line research, databases	Test: to review self efficacy
6. (2 week)	Preventing cyber attacks, and network protection systems • Understanding IDS/IPS Systems • Understanding honeypots	Lecture Discussion, collaborative work. Critical reflection of on- line research, databases	Test: to review self efficacy