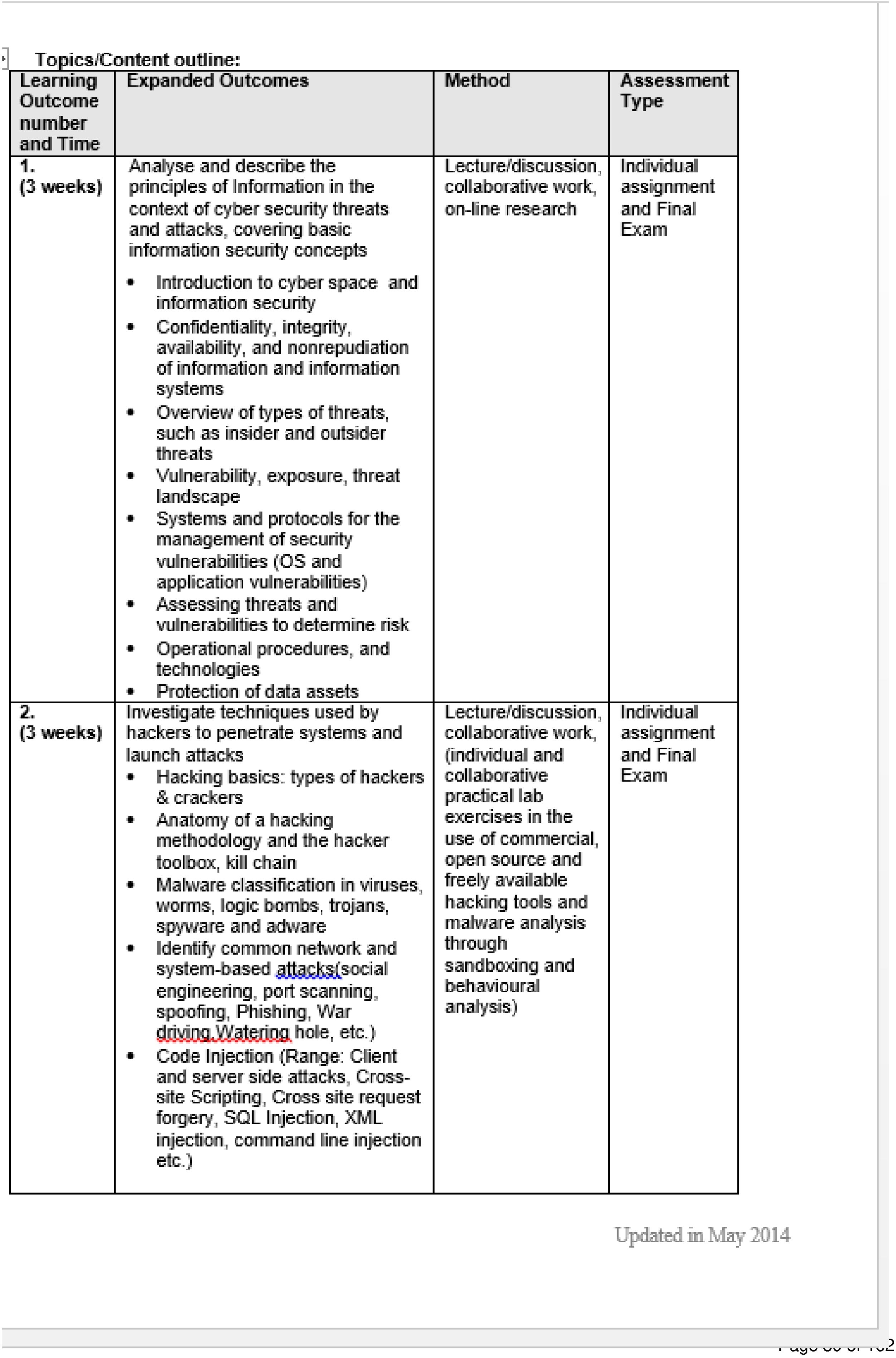

Topics/Content outline:

Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
1. **(3 weeks)**	Analyse and describe the principles of Information in the context of cyber security threats and attacks, covering basic information security concepts • Introduction to cyber space and information security • Confidentiality, integrity, availability, and nonrepudiation of information and information systems • Overview of types of threats, such as insider and outsider threats • Vulnerability, exposure, threat landscape • Systems and protocols for the management of security vulnerabilities (OS and application vulnerabilities) • Assessing threats and vulnerabilities to determine risk • Operational procedures, and technologies • Protection of data assets	Lecture/discussion, collaborative work, on-line research	Individual assignment and Final Exam
2. **(3 weeks)**	Investigate techniques used by hackers to penetrate systems and launch attacks • Hacking basics: types of hackers & crackers • Anatomy of a hacking methodology and the hacker toolbox, kill chain • Malware classification in viruses, worms, logic bombs, trojans, spyware and adware • Identify common network and system-based attacks(social engineering, port scanning, spoofing, Phishing, War driving,Watering hole, etc.) • Code Injection (Range: Client and server side attacks, Cross-site Scripting, Cross site request forgery, SQL Injection, XML injection, command line injection etc.)	Lecture/discussion, collaborative work, (individual and collaborative practical lab exercises in the use of commercial, open source and freely available hacking tools and malware analysis through sandboxing and behavioural analysis)	Individual assignment and Final Exam