Topics/Content outline

Learning Outcome number and Time	Expanded Outcomes	Method	Assessment Type
No. 1 (3 weeks)	Course overview Knowledge of programming languages necessary to analyse malware.	Lecture Lab work	
No. 2 (4 weeks)	Static and Dynamic analysis of malware • Disassembly • Call graphs • Debugging techniques • Network forensics (brief)	Lecture Lab work	
No. 3 (1 week)	Understanding malware functionality and how malware enables the underground economy • Malware functionality • Malware taxonomy • Covert malware launching • Underground economics • Malware ecosystems	Lecture Discussion Lab work	
No 4. (3 weeks)	Reverse engineering and obfuscation techniques used in modern malware • Reverse engineering • Rootkits • Data encoding • Encryption of malware communication channels	Lecture Lab work	
No. 5 (1 week)	Shellcode analysis • Execution locations • NOP sleds • Shellcode programming • Shellcode from metasploit	Lecture Lab work	
Revision (1 week)	Revision	Lecture Discussion Practice Exam	

Assessment

Weighting	Nature of assessment	Learning outcomes
60%	Research Project(s) and/or Assignment(s) that include the analysis of current malware in a lab environment, presentation of investigation plan and findings	1, 2, 3, 4, 5
10%	Class Test(s)	1, 2
30%	Final Exam	1, 2, 3, 4, 5