SAIT

COURSE SCHEDULE

Week	Module Title	Outcome	Assessments Due
1	Operating System Vulnerabilities and Exploits	Review OS components, identify vulnerabilities and outline general purposes and uses of exploiting computer operating systems.	
2	Shellcode	Create Shell code	Lab 1
3	Buffer Overflow Exploit	Implement buffer overflow to exploit operating systems	Lab 2
4	Windows Exploits and Buffer Overflow	Implement buffer overflow – NOP and ROP techniques to exploit operating system	Lab 3
5	Advanced Windows Exploits	Implement Structured Exception Handling (SEH) and UAC to exploit Windows operating systems	Lab 4
6	Loadable Kernel Modules	Create Loadable Kernel Modules	Theory Quiz 1 Lab Quiz 1 (It covers Labs1,2,3 and 4)
7	Linux rootkits	Hooking system calls and kernel objects Hooking system calls and kernel objects	Lab 5
8			Lab 6
9	Windows rootkits and post-exploitation	Hooking system calls and kernel objects Hooking system calls and kernel objects	Lab 7
10			Theory Quiz 2 Lab Quiz 2 (it covers Labs 5,6 and 7)
11	Bootkits Firmware Exploits	Exploit firmware	Lab 8
12	Detection	Monitor and detect operating systems events	Lab 9
13	Detection	Monitor and detect operating systems events	Lab 10
14	Pen Testing tools	Pen Test tools to exploit, and perform post-exploits of operating systems	Theory Quiz 3 Lab Quiz 3 (It covers Labs 8, 9 and 10)

15	Final Project		Final Project

Note: Schedule may be subject to change.