CSA Course Plan

Class#	Module#	Module Name	Practical Sessions	Each Class Duration (in Hrs.)
1	1	Security Operations and Management	N/A	2
2	2	Understanding Cyber Threats, IoC's and Attack Methodologies	Lab 1: Web Application Attack Lab 2: DNS Attack Lab 3: Network Attack Lab 4: SQL Injection Attack Lab 5: Brute forcing Attack Lab 6: XSS Attack Lab 7: DoS & DDoS Attack	2
3	2	Understanding Cyber Threats, IoC's and Attack Methodologies	Lab 8: Exploitation to Server Lab 9: Exploitation to Application Server	2
4	3	Incidents, Events and Logging	Lab 10: Windows Log Analysis Lab 11: Linux Log Analysis Lab 12: Windows Firewall Log Analysis	2
5	3	Incidents, Events and Logging	Lab 13: Linux Firewall Log Analysis Lab 14: Router Log Analysis Lab 15: IIS Log Analysis Lab 16: Apache Log Analysis	2
6	4	SIEM	Lab 17: Setup the WAZUH	2
7	4	SIEM	Lab 18: Setup the Suricata and/or Zabbix	2
8	5	Enhanced Incident Detection with Threat Intelligence	Lab 19: Malware Threat Analysis	2
9	5	Enhanced Incident Detection with Threat Intelligence	Lab 20: SIEM Logs and Dashboard Monitoring	2
10	6	Incident Response	NIST Risk Management Framework	2
11	6	Incident Response	NIST Risk Management Framework	2
12	Discussion and Closing of the Session	"Putting all together"	N/A	2
			Total Course Hour	**24**