CISSP Course Flow

CISSP Domain Number & Name	Session # (videos, presentations & quizzes)	CybrScore Hands-on Labs
Domain 1 *Security and Risk Management*	1, 2, 3, 4	Lab #13 - Identify Whether High-Risk Systems Were Affected
Domain 1 *Security and Risk Management*	5, 6, 7, 8	Lab #1 - Analyze and Update a Company BCP/BIA/DRP/CIRP
Domain 2 *Asset Security*	9,10	Lab #6 - Creating a Baseline Using the Windows Forensic Tool Chest (WFT) Lab #8 - Creating a Secondary Baseline and Conducting Comparison Lab #22 - Microsoft Baseline Security Analyzer Lab #7 - Creating a List of Installed Programs, Services and User Accounts from a WIN2K12 Server Lab #35 - Analyze and Classify Malware
Domain 3 *Security Engineering*	11,12	Lab #29 - Scanning and Mapping Networks Lab #33 - Manual Vulnerability Assessments Lab #34 - Analysis and Recommendation Report
Domain 3 *Security Engineering*	13,14,15,16	Lab #11 - Firewall Setup and Configuration Lab #15 - IDS Setup and Configuration Lab #36 - Assess a High-Risk System
Domain 3 *Security Engineering*	17,18	Lab #5 - Baseline Systems in Accordance with Policy Documentation Lab #39 - Control Assessment and Evaluation Lab #40 - Creating Recommendations Based on Vulnerability Assessments
Domain 4 *Communications & Network Security*	19, 20	Lab #4 - Applying Filters to Tcpdump and Wireshark Lab #25 - Network Segmentation (FW/DMZ/WAN/LAN)
Domain 4 *Communications & Network Security*	21, 22	Lab #26 - Parse Files Out of Network Traffic Lab #31 - Use pfTop to Analyze Network Traffic
Domain 5 *Identity & Access Management*	23, 24	Lab #16 - Implementing Least-Privilege on Windows Lab #30 - Securing Linux for System Administrators
Domain 5 *Identity & Access Management*	25, 26	Lab #12 - Identify Access to a LINUX Firewall Through SYSLOG Service Lab #17 - Linux Users and Groups
Domain 6 *Security Assessment & Testing*	27, 28, 29	Lab #19 - Manual Vulnerability Assessment Lab #14 - Identifying System Vulnerabilities with OpenVAS Lab #32 - Vulnerability Identification and Remediation
Domain 7 *Security Operations*	30, 31, 32, 33	Lab #23 - Monitoring and Verifying Management Systems Lab #27 - Patch Installation and Validation Testing Lab #24 - Monitoring Network Traffic for Potential IOA/IOC Lab #18 - Log Correlation & Analysis to Identify Potential IOC
Domain 7 *Security Operations*	34, 35, 36	Lab #10 - Data Backup and Recovery Lab #28 - Performing Incident Response in a Windows Environment Lab #9 - Creation of Standard Operating Procedures for Recovery Lab #37 - BCP DRP and Test Planning Lab #38 - CIRP Creation and Review of BCP and DRP
Domain 8 *Software Development Security*	37, 38, 39, 40	Lab#2 - Analyze Structured Exception Handler Buffer Overflow Exploit Lab #3 - Analyze SQL Injection IOC Lab #20 - Manually Analyze Malicious PDF Documents Lab #21 - Manually Analyze Malicious PDF Documents 2