Comprehensive Cybersecurity Defense Course Agenda

Course Schedule
Day 1 Agenda

Day 1 Time:	Day 1 Activity:
8:00 am-8:50 am	Welcome and Introductions
8:50 am-9:00 am	Break
9:00 am-9:50 am	Pre-Test
9:50 am-10:00 am	Break
10:00 am-10:50 am	Module 1: Introduction to Cybersecurity
10:50 am-11:00 am	Break
11:00 am-11:10 am	Lab 1: Introduction to Using VMWare Workstation (10 min)
11:10 am-12:00 pm	Module 2: Planning and Preparation of Defenses
12:00 pm-1:00 pm	Lunch
1:00 pm-1:50 pm	Module 2: Planning and Preparation of Defenses
1:50 pm-2:00 pm	Break
2:00 pm-2:50 pm	Module 2: Planning and Preparation of Defenses
2:50 pm-3:00 pm	Break
3:00 pm-3:10 pm	Lab 2: Reconnaissance Using the Internet (10 min)
3:10 pm-3:20 pm	Lab 3: Exploring Steganography with Invisible Secrets (10 min)
3:20 pm-3:30 pm	Lab 4: Exploring Steganography with DeepSound (10 min)
3:30 pm-3:50 pm	Module 2: Planning and Preparation of Defenses
3:50 pm-4:00 pm	Break
4:00 pm-4:40 pm	End of Day 1 Scenario
4:40 pm-5:00 pm	Daily Review and Adjournment

Day 2 Agenda

Day 2 Time	Day 2 Activity
8:00 am-8:10 am	Review and Q&A
8:10 am-8:20 am	Module 2: Planning and Preparation of Defenses
8:20 am-8:50 am	Lab 5: Incident Response on Windows (30 min)
8:50 am-9:00 am	Break
9:00 am-9:20 am	Lab 6: Incident Response on Linux (20 min)
9:20 am-9:35 am	Lab 7: Footprinting with Shodan (15 min)
9:35 am-9:50 am	Lab 4: Preparing Network Diagrams with Diagram Designer (15 min)
9:50 am-10:00 am	Break
10:00 am-10:50 am	Module 2: Planning and Preparation of Defenses
10:50 am-11:00 am	Break
11:00 am-12:00 pm	Module 3: Mobile Devices and Internet of Things (IoT)
12:00 pm-1:00 pm	Lunch
1:00 pm-1:50 pm	Module 3: Mobile Devices and Internet of Things (IoT)
1:50 pm-2:00 pm	Break
2:00 pm-2:50 pm	Module 4: WiFi Technologies
2:50 pm-3:00 pm	Break
3:00 pm-3:10 pm	Lab 9: Using Wireless Netview to Discover Wireless Networks (10 min)
3:10 pm-3:30 pm	Lab 10: Capturing Wireless Packets and Breaking Keys (20 min)
3:30 pm-3:50 pm	Module 4: WiFi Technologies
3:50 pm-4:00 pm	Break
4:00 pm-4:20 pm	Lab 11: Obtaining the SSID from a Router Broadcasting a Null SSID
4:20 pm-4:30 pm	Modules 3 and 4 Review (Mobile Devices and IoT & WiFi Technologies)
4:30 pm-4:50 pm	End of Day 2 Scenario
4:50 pm-5:00 pm	Review and Adjournment

Day 3 Agenda

Day 3 Time	Day 3 Activity
8:00 am-8:10 am	Review and Q&A
8:10 am-8:30 am	Module 5: Administration of Defenses
8:30 am-8:50 am	Lab 12: Auditing Passwords with L0phtCrack (20 min)
8:50 am-9:00 am	Break
9:00 am-9:50 am	Module 5: Administration of Defenses
9:50 am-10:00 am	Break
10:00 am-10:20 am	Lab 13: Probing Vulnerabilities with Belarc Advisor (20 min)
10:20 am-10:50 am	Lab 14: Probing Vulnerabilities with Nessus (20 min)
10:50 am-11:00 am	Break
11:00 am-12:00 pm	Module 5: Administration of Defenses
12:00 pm-1:00 pm	Lunch
1:00 pm-1:30 pm	Module 5: Administration of Defenses
1:30 pm-1:50 pm	Lab 15: Using CatchPulse for Application Allowlisting (20 min)
1:50 pm-2:00 pm	Break
2:00 pm-2:20 pm	Lab 16: Performing SQL Injection Attacks Using WebGoat (20 min)
2:20 pm-2:35 pm	Lab 17: Testing with Burp Suite (15 min)
2:35 pm-3:05 pm	Lab 18: Windows Exploitation with Metasploit's Msfvenom (30 min)
3:05 pm-3:15 pm	Break
3:15 pm-3:35 pm	Lab 19: Sniffing Packets with Wireshark (20 min)
3:35 pm-3:55 pm	Lab 20: Extracting a File from a Wireshark Capture (20 min)
3:55 pm-4:05 pm	Break
4:05 pm-4:25pm	Lab 21: Detecting Intrusions with Snort (20 min)
4:25 pm -4:40 pm	Lab 22: Using Kiwi Syslog and Snare to Conduct Intrusion Analysis (15 min)
4:40 pm-4:50 pm	Lab 23: Using Microsoft Log Parser to Review Logs for Anomalies (10 min)
4:50 pm-4:55 pm	End of Day 3 Scenario
4:55 pm-5:00 pm	Review and Adjournment

Day 4 Agenda

Day 4 Time	Day 4 Activity
8:00 am-8:10 am	Review and Q&A
8:10 am-8:50 am	Module 7: Testing and Modifying Your Defenses
8:50 am-9:00 am	Break
9:00 am-9:10 am	Lab 24: Conducting Reconnaissance Using DNS Query Tools (10 min)
9:10 am-9:20 am	Lab 25: Conducting Enumeration with WinPEAS (10 min)
9:20 am-9:35 am	Lab 26: Scanning For and Hacking RDP (15 min)
9:35 am-9:55 am	Lab 27: Packet Crafting with Engage Packet Builder (20 min)
9:55 am-10:05 am	Break
10:05 am-10:30 am	Module 7: Testing and Modifying Your Defenses
10:30 am-10:50 am	Lab 28: Scanning Target Systems with Nmap in Kali Linux (20 min)
10:50 am-11:00 am	Break
11:00 am-12:00 pm	Module 7: Testing and Modifying Your Defenses
12:00 pm-1:00 pm	Lunch
1:00 pm-1:20 pm	Lab 29: Scanning with Nmap and Blocking Scans w/ iptables (20 min)
1:20 pm-2:00 pm	Module 7: Testing and Modifying Your Defenses
2:00 pm-2:20 pm	Lab 30: Scanning for Open Ports Using Superscan (20 min)
2:20 pm- 2:50 pm	Module 7: Testing and Modifying Your Defenses
2:50 pm-3:00 pm	Break
3:00 pm-3:15 pm	Module 7: Testing and Modifying Your Defenses
3:15 pm-3:25 pm	Lab 31: Using HPing to Simulate an Attack (10 min)
3:25 pm-3:55pm	Module 8: Review of Cybersecurity Defenses and Emerging Trends
3:55 pm-4:00 pm	Break
4:00 pm-4:30 pm	Post-Test
4:30 pm-4:40 pm	End of Course Scenario 1
4:40 pm-4:50 pm	End of Course Scenario 2
4:50 pm-5:00 pm	Course Evaluations, Final Comments, and Adjournment