Course Agenda: Malware Prevention, Discovery, and Recovery

Day 1

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 - 10:35 am	Module 1: Introduction to Malware Analysis (Total: 3 Hr 30 Min)
10:35 am - 10:50 am	Lab 1 - VMware Refresher (15 min)
10:50 am – 11:00 am	Break
11:00 am - 11:30 am	Module 1: Introduction to Malware Analysis
11:30 am - 12:30 pm	Lunch
12:30 pm - 12:50 pm	Module 2: Malware Prevention and Detection (Total: 2 Hr 0 Min)
12:50 pm - 1:00 pm	Break
1:00 pm - 1:15 pm	Lab 2 – Using Cisco ACL Editor and Simulator to Simulate Configuring a Firewall
1:15 pm – 1:30 pm	Module 2: Malware Prevention and Detection
1:30 pm – 1:50 pm	Lab 3 – Using AppSamvid for Application Whitelisting
1:50 pm - 2:00 pm	Break
2:00 pm – 2:20 pm	Module 2: Malware Prevention and Detection
2:20 pm - 2:30 pm	Lab 4 – Identifying Phishing e-Mail Messages
2:30 pm – 2:50 pm	Module 3: Malware Discovery and Incident Response (Total: 2 Hr 30 Min)
2:50 pm – 3:00 pm	Break
3:00 pm – 3:50 pm	Module 3: Malware Discovery and Incident Response
3:50 pm – 4:00 pm	Break
4:00 pm – 4:10 pm	Lab 5 – Using VirusTotal to Analyze a Malware Sample
4:10 pm – 4:20 pm	Lab 6 – Using PacketTotal to Analyze a Packet Capture File
4:20 pm – 4:40 pm	Module 3: Malware Discovery and Incident Response
4:40 pm – 4:55 pm	End of Day 1 Scenario
4:55 pm - 5:00 pm	Review and Adjournment

Day 2

8:00 am - 8:10 am	Review and Q&A
8:10 am - 8:50 am	Module 4: Static Malware Analysis (Total: 8 Hr 0 Min)
8:50 am - 9:00 am	Break
9:00 am - 9:15 am	Lab 7 – Using OfficeMalScanner to Analyze a Word Document
9:15 am - 9:30 am	Lab 8 – Using PDFStreamDumper to Examine a PDF file
9:30 am - 9:50 am	Module 4: Static Malware Analysis
9:50 am - 10:00 am	Break
10:00 am - 10:15 am	Lab 9 – Using PEiD to Identify Packed Malware
10:15 am - 10:30 am	Lab 10 – Using Exeinfo PE to Examine Malware
10:30 am - 10:40 am	Lab 11 – Determine Dependencies with Dependency Walker
10:40 am - 10:55 am	Module 4: Static Malware Analysis
10:55 am - 11:00 am	Break
11:00 am - 11:15 am	Lab 12 – Determine Embedded Icons with Resource Hacker
11:15 am – 11:30 am	Module 4: Static Malware Analysis
11:30 am - 12:30 pm	Lunch
12:30 pm - 12:50 pm	Module 4: Static Malware Analysis
12:50 pm - 1:00 pm	Break
1:00 pm - 1:30 pm	Module 4: Static Malware Analysis
1:30 pm - 1:50 pm	Lab 13 – Using FileAlyzer to Examine Malware
1:50 pm – 2:00 pm	Break
2:00 pm – 2:30 pm	Module 4: Static Malware Analysis
2:30 pm - 2:50 pm	Lab 14 – Using CFF Explorer to Examine Malware
2:50 pm – 3:00 pm	Break
3:00 pm - 3:30 pm	Module 4: Static Malware Analysis
3:30 pm – 3:50 pm	Lab 15 – Using PEStudio to Examine Malware
3:50 pm – 4:00 pm	Break
4:00 pm – 4:30 pm	Module 4: Static Malware Analysis
4:30 pm - 4:50 pm	End of Day 2 Scenario
4:50 pm - 5:00 pm	Review and Adjournment

Day 3

8:00 am - 8:10 am	Review and Q&A
8:10 am - 8:50 am	Module 5: Dynamic Malware Analysis (Total: 8 Hr 0 Min)
8:50 am - 9:00 am	Break
9:00 am - 9:10 am	Lab 16 – Using Autorun to Examine Startup Entries
9:10 am – 9:25 am	Lab 17 – Using Process Monitor to Examine a Process
9:25 am – 9:35 am	Module 5: Dynamic Malware Analysis
9:35 am – 9:50 am	Lab 18 – Using Process Explorer to Examine Running Processes
9:50 am - 10:00 am	Break
10:00 am - 10:20 am	Module 5: Dynamic Malware Analysis
10:20 am – 10:40 am	Lab 19 – Configuring Wireshark for Malware Analysis
10:40 am – 10:55 am	Lab 20 – Using Wireshark to follow a TCP Stream
10:55 am – 11:30 am	Module 5: Dynamic Malware Analysis
11:30 pm - 12:30 pm	Lunch
12:30 pm - 12:50 pm	Module 5: Dynamic Malware Analysis
12:50 pm – 1:00 pm	Break
1:00 pm - 1:20 pm	Lab 21 – Using Wireshark for Incident Response 1
1:20 pm – 1:50 pm	Lab 22 – Using Wireshark for Incident Response 2
1:50 pm – 2:00 pm	Break
2:00 pm – 2:20 pm	Lab 23 – Using Wireshark for Incident Response 3
2:20 pm – 2:40 pm	Lab 24 – Extracting Files from Network Traffic
2:40 pm – 3:00 pm	Lab 25 – Assessment of Suspect Network Traffic
3:00 pm - 3:10 pm	Break
3:10 pm - 3:50 pm	Module 5: Dynamic Malware Analysis
3:50 pm – 4:00 pm	Break
4:00 pm - 4:30 pm	Lab 26 – Using X64dbg to Examine a Binary
4:30 pm - 4:55 pm	End of Day 3 Scenario
4:55 pm - 5:00 pm	Review and Adjournment

Day 4

8:00 am - 8:10 am	Review and Q&A
8:10 am - 8:50 am	Module 6: Malware Remediation and Recovery (Total: 3 Hr 30 Min)
8:50 am - 9:00 am	Break
9:00 am - 9:50 am	Module 6: Malware Remediation and Recovery
9:50 am - 10:00 am	Break
10:00 am - 10:50 am	Module 6: Malware Remediation and Recovery
10:50 am - 11:00 am	Break
11:00 am - 11:30 am	Module 6: Malware Remediation and Recovery
11:30 am - 12:30 pm	Lunch
12:30 pm - 12:50 pm	Module 7: Emerging Trends in Modern Malware (Total: 0 Hr 40 Min)
12:50 pm - 1:00 pm	Break
1:00 pm – 1:10 pm	Module 7: Emerging Trends in Modern Malware
1:10 pm - 1:40 pm	End of Course Scenario 1
1:40 pm – 1:50 pm	Scenario 1 Review
1:50 pm - 2:00 pm	Break
2:00 pm - 2:30 pm	End of Course Scenario 2
2:30 pm - 2:50 pm	Scenario 2 Review
2:50 pm – 3:00 pm	Break
3:00 pm - 4:00 pm	Post Test
4:00 pm - 4:30 pm	Course Evaluations
4:30 pm - 5:00 pm	Wrap-Up and Adjournment