【CSX　トレーニング環境】　2019/Nov Version12.1

[LAB Vol1]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級		14.Webアプリケーションのテスト (Testing Web Applications)	12.ブラウザ攻撃 (Browser Attacks)	15.マルウェアの解析 (Malware Analysis)	13.Secure Copyによる原状復帰 (Restoring Data with Secure Copy)
中級		8.ファイアウォールのポリシー変更 (Updating Firewall Rules)	9.中間者攻撃の検知 (Man-in-the-Middle Detection) 10.脅威の検知 (Threat Detection)		11.攻撃後のクリーンアップ (Cleaning Up After an Attack)
初級	1.Webサーバ攻撃の検知 (Finding the Lost Web Server) 2.ネットワークのスキャン (Network Scanning) 7.詳細なスキャニング (In-depth Scanning)	4.データの整合性 (Data Integrity)	3.HTTPパケットの解析 (HTTP Packet Analysis) 6.DNSパケットの分析 (DNS Packet Analysis)		5.Webサーバのバックアップ (Web Server Backup)

Vol1まとめ（チャレンジ：＝LAB Vol1　習得度テスト）
16.スキャンとEnumeration(JAVA)のチャレンジ［Scanning and Enumeration Challenge］
17.整合性とマルウェア解析のチャレンジ［Integrity and Malware Analysis Challenge］

[LAB Vol 2]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級			22.SQLインジェクション (SQL Injection) 23.ファイアウォールの初期設定 (Initial Firewall Setup)		
中級		20.追加のファイアウォールの設定 (Additional Firewall Setup)			19.フォレンジック復旧入門 (Introduction to Forensics Recovery) 21.モバイルフォレンジック (Mobile Forensics)
初級					18.フォレンジック 1: イメージファイルへの変換 (Forensics 1: Imaging)

Vol 2 まとめ（チャレンジ：＝LAB Vo l 2　習得度テスト）
なし

[LAB Vol3]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級			25.Ddos攻撃の検知 (DDoS Detection) 26.セッションハイジャック (Session Hijacking)		
中級	24.情報漏えい (Data Leakage)	28.パケット構成とカーネルのハードニング (Packet Construction and Kernel Hardening)			
初級		29.システムのベースライニング (System Baselining)	27.内部脅威の特定 (Insider Threat Identification)		

Vol3まとめ（チャレンジ：＝LAB Vol4　習得度テスト）
30.CSX Volume 3, チャレンジ 1[CSX Volume3, Challenge 1]
31.CSX Volume3, チャレンジ2 [CSX Volume3, Challenge2]

[CSX Linuxアプリと設定] CSX Linux Application and Configuration

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級					
初級	33.シェルとナビゲーション (Shell and Navigation) 34.ファイル/ディレクトリ/インフォメーション (Files, Directories, and Information) 35.ファイルと標準入出力 (Files and Standard Input/Output) 36.STDIOを使う (Using STDIO)	32.Linuxのインストール (Installing Linux) 37.CLIトリック (CLI Tricks) 38.サービスとユーザ (Services and Users) 39.ネットワーク (Networking) 40.ユーザとネットワーク (Users and Networking) 41.パッケージ管理、アーカイブとコンパイル (Package Management, Archives, and Compiling)			

まとめ（チャレンジ：　習得度テスト）
　　なし

[CSX ネットワーク　アプリと設定] CSX Network Application and Configuration

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級					
初級	42.ルータの熟知 (Router Familiarization) 44.クライアントの接続 (Connecting Clients)	43.LAN及びWANの構築 (Setting up a LAN and a WAN) 45.初期設定 (Initial Configuration) 46.基本設定 (Basic Configuration) 47.ポートフォワーディングとVPN設定 (Port Forwarding and VPN Setup)	48.脆弱性攻撃の特定と対応 (Exploitation Identifications and Response)	48.脆弱性攻撃の特定と対応 (Exploitation Identifications and Response)	

まとめ（チャレンジ：　習得度テスト）
　　49ネットワーク構築(チャレンジ) [Establishing a Network]
　　50.ネットワーク攻撃の検知、対応、復旧(チャレンジ)　[Detecting , Responding, Recovering from a Network Attack]

[CSX Cybersecurity Practitioner研修コース] CSX　Cybersecurity Practitioner Training Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級	51.資産の特定 (Asset Identification) 52.データフローの特定 (Data Flow Identification) 53.事業体資産の特定 (Enterprise Asset Identification) 54.データフロー分析 (Data Flow Analysis) 55.事業体のデータフロー分析 (Enterprise Data Flow Analysis)	57.ファイアウォールの設定 (Firewall Setup) 58.バックアップと復旧ポイント (Backup and Restore Points) 59.ファイルシステム防御 (File System Protections) 60.OSベースライン (OS Baseline)	62.Security Onion設定・テスト (Sec Onion Setup and Testing) 63.Snortルール (Snort Rules) 64.イベントの検知 (Event Detection) 65.データ及びネットワーク分析 (Data and Network Analysis) 66.脆弱性の分析 (Vulnerability Analysis)	68.インシデントの相互関係 (Incident Correlation) 69.ネットワーク・フォレンジックス (Network Forensics) 70.マルウェアの調査と評価 (Malware Investigation and Evaluation) 71.通知と上申 (Notification and Escalation)	73.再イメージング (Re-Imaging) 74.復旧ポイント (Restore Points)
初級					

まとめ（チャレンジ：　習得度テスト）
　　56.「特定」チャレンジ [Identify Challenge]
　　61.「防御」チャレンジ [Protect Challenge]
　　67.「検知」チャレンジ [Detect Challenge]
　　72.「対応」チャレンジ [Response Challenge]

[CSXパケット解析コース] CSX Packet Analysis Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級	75.プロトコルの解析 (Protocol Parsing) 76.ARPの解析 (ARP Analysis) 77.初期接続プロトコル (Initial Connection) 78.知っておきたい検索方法 (Interesting Searches) 80.GETリクエストとレスポンスの解析 (GET Request and Response Dissection) 82.お遊び (Playing Around) 83.プローブ要求の解析 (Probe Request Analysis) 85.ネットワークトポロジ (Network Topology) 87.Blasterワームの解析 (Blaster Worm Analysis)				
初級					

まとめ（チャレンジ：　習得度テスト）

79.追加プログラム(チャレンジ）［Additional Pets］
81悪意のある従業員(チャレンジ）［Nefarious Employee］
84.ビーコンの解析(チャレンジ）［Beacon
86.ワイヤレスネットワークトポロジ(チャレンジ）［Wireless Network Topology］
88.不正アクセスポイントとモバイル機器の解析(チャレンジ）［Rouge AP and Mobile
89.ネットワーク図とデバイスの明確化(チャレンジ）［Complete Netmap and Devices Characterization］

[CSXペネトレーション（侵入）テスト概論] CSX Penetration Testing Overview Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級					
初級	90.Linuxシェルとコマンド (Linux Shell and Commands) 91.TCP/IP基礎 (TCP/IP Basics) 92.パケット検索 (Packet Inquiry) 93.ネットワーク発見 (Network Discovery) 94.サービス列挙 (Service Enumeration) 95.ネットワーク脆弱性特定 Network Vulnerability Identification) 96.ネットワーク脆弱性探究 (Network Vulnerability Exploitation)				97.エビデンスの除去 (Evidence Removal)

まとめ（チャレンジ：　習得度テスト）

98. CPTOチャレンジ１［CPTO Challenge1］
99. CPTOチャレンジ２［CTPO Challenge2］

[CSX脆弱性とエクスプロイトコース] (CSX Vulnerability and Exploitation course)

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級			100.フットプリンティング (Footprinting) 101.脆弱性スキャナーのセットアップ (Initial Vulnerability Scanner Setup) 102.脆弱性分析 (Vulnerability Analysis) 103.初期エクスプロイト (Initial Exploitation) 104.権限昇格 (Privilege Escalation) 105.バックドア実装 (Backdoor Implementation) 106.足跡のカバー (Covering Tracks) 107.より深いエクスプロイト (Deeper Exploitation)		
初級					

まとめ（チャレンジ：　習得度テスト）
　　108.CVECチャレンジ［ CVEC Challenge ］

[LAB Vol4]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級		109.Spectre軽減 (Spectre Mitigation) 110.Meltdown軽減 (Meltdown Mitigation) 113.Webブラウザセキュリティ (Securing Web Browsers)	111.Chrome拡張機能テスト (Chrome Extension Testing)		
初級	112.Lynisを使用したLinuxベースライン (Linux Baseline with Lynis)				

まとめ（チャレンジ：　習得度テスト）
　　114.ベースラインでのマルウェア検知と削除［ Malware Detections and Removal with Baseline ］
　　115.ドメイン検知［ Domain Detection ］

[CSX上級エクスプロイトコース] (CSX Advanced Exploitation Course)

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級			116.SSHトンネル実装 (SSH Tunnel Implementation) （SSH Tunnel Implementation) 117.複数SSHトンネルエクスプロイテーション実装 (Multiple SSH Tunnel Exploitation Implementation) 118.Metasploit PortProxy実装 (Metasploit PortProxy Implementation) 119．Metrepreter Autoroute実装 (Metrepreter Autoroute Implementation)		
中級					
初級					

まとめ（チャレンジ：　習得度テスト）
　　120．ネットワーク評価チャレンジ［ Network Assessment Challenge ］

[LAB Vol5]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級			125.IoTデバイス測定 (IOT Device Indicators) 126.ホームオートメーションデバイス分析 (Home Automation Device Patterns)	124.インシデントのトリアージ (Triaging Incidents)	122.パッシブ・コンピューター・フォレンジックス (Passive Computer Forensics)
初級	121.スクリプト作成と実行 (Script Construction and Execution)		123.不正侵入検知システム実装とテスト (Intrusion Detections System Implementation and Testing)		

まとめ（チャレンジ：　習得度テスト）

127. インシデント対応スクリプト実装 [Incident Response Script Implementation]
128. フォレンジックデータ復旧と分析 [Forensic Data Recovery and Analysis]

[CSXフォレンジック分析コース] (CSX Forensic Analysis Course)

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級				134.私の最初の案件 (My First Case) 135.画像　(A Picture) 136.データDNA (Data DNA) 137.不足している部分 (The Missing Pieces)	
初級				129.Kaliフォレンジック環境 (Kali Forensic Environment) 130.Postgre SQL構成 (Postgre SQL Configuration) 131.Foreman構成 (Foreman Configuration) 132.Foreman最終セットアップ (Final Foreman Setup) 133.新規案件 (A New Case)	

まとめ（チャレンジ：　習得度テスト）

138.フォレンジックチャレンジ［ Forensics Challenge ］

[LAB Vol6]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級	143.クリプトジャックの特定 (Identifying Cryptjacking)				
中級	139.データベース管理の実装 (Implementing Database Management) 140.侵入検知システム(IDS)のテスト (Testing Intrusion Detection Systems)		141.ハニーポットの初期化 (Initializing Honeypots)	142.ログの生成と分析 (Generating and Analyzing Logs)	
初級					

まとめ（チャレンジ：　習得度テスト）

145.データベースとハニーポットの管理 [Administering Databases and Honeypots]
146.Snortルールの適用とプロセスの分析 [Applying Snort Rules and Classifying Processes]

[Cyber Hunt]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級 中級	実戦形式によるサイバーセキュリティスキルの総合演習。				
初級					

[CSX脅威の追跡コース] (CSX Threat Hunting Course)

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級			148.脅威の生成の追跡 (Exploitation Threat Creation) 149.メモリ・フォレンジックス (Memory Forensics) 150.ネットワーク・フォレンジックス (Network Forensics) 151.ブラウザベースの攻撃の生成と調査 (Creating and Investigating a Browser Based Attack) 152.HTTP脅威の追跡へのBroの利用 (Using Bro for HTTP Threat Hunting) 153.Powershellを使った脅威の追跡		
中級					
初級					

まとめ（チャレンジ：　習得度テスト）

155．椅子取りゲームチャレンジ1（Capture the Flag Challenge - Part1）

156．椅子取りゲームチャレンジ2（Capture the Flag Challenge - Part2）

[LAB Vol7]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級		157.Windowsファイヤーウォールの管理 (Managing Windows Firewall) 158.Windowsでのスクリプトスケジューリング (Scheduling Scripts on Windows) 163.Windowsの保護 (Securing Windows) 164.Linuxハッキング技術の調査	160.DNSの収集とウェブサーチ (Harvesting DNS and Focusing Web Searches)		
中級		159.Windowsの堅牢化 (Hardening Windows) 162.ファイヤーウォールを経由したIoTデバイスの保護 (Securing IoT Devices via Firewall)		161.HTTPリクエスト方法の調査 (Investigating HTTP Request Methods)	
初級					

[OWASP Top10リスクの特定と軽減コース] CSX Identifying and Mitigating the OWASP Top10 Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級		165.インジェクション脆弱性の特定と軽減[A1:2017-インジェクション　対応] (Injection Vulnerability Identification and Mitigation) 166.認証の不備の特定と軽減[A2:2017-認証の不備　対応] (Broken Authentication Identification and Mitigation) 167.機微な情報の露出リスクの特定と軽減[A3:2017-機微な情報の露出　対応] (Sensitive Data Exposure Identification and Mitigation) 168.XXEの特定と軽減[A4:2017-XML外部エンティティ参照（XXE)　対応] (XXE Identification and Mitigation) 169.アクセス制御の不備[A5:2017-アクセス制御の不備　対応] (Broken Access Control) 170.不適切なセキュリティ設定の特定と再設定[A6:2017-不適切なセキュリティ設定対応] (Security Misconfiguration Identification and Reconfiguration) 171.XSSの特定と回避[A7:2017-クロスサイトスクリプティング（XSS)　対応] (XSS Identification and Prevention) 172.安全でないデシリアライゼーションの回避[A8:2017-安全でないデシリアライゼーション　対応](Insecure Deserialization Prevention)			
初級					

まとめ（チャレンジ：　習得度テスト）

175.SQLインジェクション　チャレンジ(SQL Injection Challenge)

176.アクセス制御の不備　チャレンジ(Broken Access Control Challenge)

[LAB Vol8]

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級			181.Windowsペネトレーションテスト (Windows Penetration Tests) 182.Windowsサービス　－　最少機能の原則 (Windows Services – Principal of least functionality)		
中級		178.NSAセキュアホストの基礎 (NSA Secure Host Baseline) 179.Windowsイベントモニター (Windows Event Monitor)			
初級	177.Windowsサーバーのアクセス管理 (Access Management with Windows Server)	180. Powershell (Powershell)			

まとめ（チャレンジ：　習得度テスト）

183.システムの堅牢化(System Hardening)

184.Powershellの活用(Fun with Powershell)

[CSXブロックチェーン基礎コース] Blockchain Basics Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級		185.暗号化の機能 (Crypto Functions) 186.暗号化ブロックの作成 (Crypto Block Creation) 187.暗号化ブロックの計算 (Crypto Block Calculations) 188.P2Pネットワークの設定 (P2P Network Setup) 189.ハイパーレッジャー構造の設定 (Hyperledger Fabric Setup) 190.トランザクションの作成 (Creating a Transaction) 191.トランザクションの作成2 (Creating a Transaction 2) 192.暗号マイニングシミュレーション			
中級					
初級					

まとめ（チャレンジ：　習得度テスト）

193.暗号化チャレンジ(Crypto Challenge)

194. ハイパーレッジャー　チャレンジ(Hyperledger Challenge)

[CSXサイバーセキュリティ　ハンズオン基礎　ラボパッケージ] CSX Cybersecurity Hands-On Basics Lab Packages

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級					
中級					
初級	199.ポートのスキャンとSSHの活用 (Scanning Port and Utilizing SSH)	197.ファイルハッシュ法 (File Hashing) 198.WindowsとLinuxのファイルパーミッション (Windows and Linux File Permissions) 200.WindowsとLinuxのOSファイアウォール (Windows and Linux OS Firewall) 201.IDS/IPS (IDS/IPS) 203. SQLインジェクション (SQL Injection)	195.デジタルフォレンジックス (Digital Forensics) 196.DoS (DoS) 202.パケット分析 (Packet Analysis)	204.ネットワーク上の権限のないアクティビティ (Unauthorized Network Activity)	

まとめ（チャレンジ：　習得度テスト）

206.CSX基礎チャレンジ(CSX Basics Challenge)

[CSX上級フォレンジックスコース] CSX Advanced Forensics Course

工程・要素	【特定Identify】	【防御・Protect】	【検知・Detect】	【対応・Response】	【復旧・Recover】
上級				207.**Kaliフォレンジックス入門** **(Kali Forensics Introduction)** 208**フォレンジックスラボのセットアップ** (Forensics Lab Setup) 209**ネットワークフォレンジックス** (Network Forensics) 210.**Wiresharkとステノグラフィーの要点** (Wireshark and Steganography Essentials) 211.**Windowsレジストリ** (Windows Registry) 212.**リモートフォレンジックス** (Remote Forensics)	
中級					
初級					

まとめ（チャレンジ：　習得度テスト）

213.上級フォレンジックスチャレンジ 1 (Advanced Forensics Challenge1)

214.上級フォレンジックスチャレンジ2 (Advanced Forensics Challenge2)