

CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM LABS

LABS + COURSES PACKAGE

Ver6 2018/04

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	OPE HOURS	DESCRIPTION	英語名	Lesson	Related Course	LAB Type	Level	Functional	Estimated Duration	Description
									Lesson名	コース関連/形態	授業スタイル	レベル	機能領域	予想就業時間	概要
1	Finding the Lost Web Server	Labs Volume 1	Instructional	Beginner	Identify	2	Students will leverage network discovery and diagnostic capabilities to identify what happened to a corporate webserver severely damaged during an attack.	Finding the Lost Web Server	Webサーバ攻撃の検知	Labのみ	自動教育指導	初級	特定	2時間	サイバー攻撃を受けた企業のWebサーバの発見と被害内容特定に必要なネットワーク技術の習得
2	Network Scanning	Labs Volume 1	Instructional	Beginner	Identify	2	Students will leverage network scanning tools to identify nodes and services on an internal network. The end goal is to create an up to date network map of their company's internal network for troubleshooting, analysis, and future reference.	Network Scanning	ネットワークのスキャン	Labのみ	自動教育指導	初級	特定	2時間	イントラネット(内部ネットワーク)上のサービスとノード(端末)特定に必要なネットワーク・スキャンツールの使い方の学習。トラブルシューティング・NW分析・今後の参考資料となる該当企業の内部ネットワーク図の作成を最終ゴールとする。
3	HTTP Packet Analysis	Labs Volume 1	Instructional	Beginner	Detect	2	Conducting basic packet analysis is a key skill for anyone working in the cyber security field. Students will learn how to filter and parse packets to detect if corporate intellectual property is being stolen from their organization.	HTTP Packet Analysis	HTTPパケットの解析	Labのみ	自動教育指導	初級	検知	2時間	サイバーセキュリティ分野において必須のパケット解析技術の習得。企業の知的財産が盗み出されようとしていることを検知するのに必要なパケットのフィルタ、解析方法の学習
4	Data Integrity	Labs Volume 1	Instructional	Beginner	Protect	2	Students will learn the importance of data integrity through comparative analysis of hash algorithm output. Leveraging hashing tools, students will learn how to ensure that data is not compromised post-incident.	Data Integrity	データの整合性	Labのみ	自動教育指導	初級	防御	2時間	ハッシュアルゴリズムのアウトプットの比較分析を通じ、データ整合の重要性を学習。ハッシュツールを利用して、インシデント発生後にデータが改変されていないことを確認する方法を習得
5	Web Server Backup	Labs Volume 1	Instructional	Beginner	Recover	2	Maintaining copies of non-compromised data and files are paramount to the incident response and disaster recovery process. This lab ensures that students understand how to archive and hash non-compromised data and back it up to a safe location.	Web Server Backup	Webサーバのバックアップ	Labのみ	自動教育指導	初級	復旧	2時間	インシデントレスポンスおよび災害復旧(ディザスタリカバリ)において、最重要となるのが、現状データ/ファイルのコピーと保存。現状データのハッシュ及びアーカイブ化の方法と、コピーしたデータ群を安全なエリアに保存する方法を習得。
6	DNS Packet Analysis	Labs Volume 1	Instructional	Beginner	Detect	2	Cyber security practitioners understand the importance of Domain Name System (DNS) packets and how they enable the flow of data across the Internet. They also understand that the subversion of DNS services on a network is a common attack seen in cyber security. In this lab, students will learn how to detect odd DNS activity and isolate samples of the traffic.	DNS Packet Analysis	DNSパケットの分析	Labのみ	自動教育指導	初級	検知	2時間	サイバーセキュリティに携るには、DNS (ドメインシステム)パケットの重要性と、インターネット上のデータフローへの関わりに精通していることが必須。DNSの乗っ取りこそが、最も多く発生するサイバー攻撃。DNSの異常な動きを検知し、該当するトラフィックを隔離する方法を習得
7	Scripts with Nmap	Labs Volume 1	Instructional	Beginner	Identify	2	Understanding if a system's ports are open and exposed is only half the battle of fully identifying and understanding an asset. You must also assess which services may be running on the asset. Every cyber security practitioner should understand how to leverage tools to understand which services are running on their networks. Students will leverage Nmap to see which services their computers are running.	Scripts with Nmap	Nmapのプログラミング	Labのみ	自動教育指導	初級	特定	2時間	通信システムのオープンとなっているポートの把握だけでは、ネットワーク資産の真の特定と理解には不十分。ネットワーク資産上で稼動するサービスを把握が重要。ネットワーク上で稼動するサービスを把握する方法を、Nmapツールを使って自身のコンピュータ上で稼動するサービスを把握することで習得
8	Updating Firewall Rules	Labs Volume 1	Instructional	Intermediate	Protect	2	Cyber security professionals are often responsible for implementing acceptable use policies on their networks of responsibility. Thanks to the constant change of application usage and computing platforms, incident responders and technical professionals find themselves updating these policies regularly. In this lab, students learn how to change firewall rules to block unacceptable traffic.	Updating Firewall Rules	ファイアウォールのポリシー変更	Labのみ	自動教育指導	中級	防御	2時間	利用するアプリケーション、プラットフォームの変更に伴い、定期的にポリシーを変更することは、サイバーセキュリティの観点から重要。許可されないトラフィックをブロックするための、ファイアウォールのポリシー変更方法を学習
9	Man-in-the-Middle Detection	Labs Volume 1	Instructional	Intermediate	Detect	2	One of the most common attacks in the field of cyber security is the Man-in-the-Middle (MitM) attack. Students taking this lab will learn how to detect when a potential MitM attack is occurring.	Man-in-the-Middle Detection	中間者攻撃の検知	Labのみ	自動教育指導	中級	検知	2時間	中間者攻撃(MitM)は、サイバーセキュリティ攻撃で最も一般的な手法です。中間者攻撃が発生した場合の検知方法を学習
10	Vulnerability Analysis	Labs Volume 1	Instructional	Intermediate	Detect	2	Cyber security professionals are often given vague declarations of discontent from end-users experiencing technical difficulties. Understanding how to take minimal information and implement tools from their suite of capabilities to further understand the potential problems is key to proficiency. In this lab, students will implement typical network diagnostic tools to determine the type of issue an enduser is having.	Threat Detection	脅威の検知	Labのみ	自動教育指導	中級	検知	2時間	エンドユーザからの技術的なクレームは、曖昧な供述であることが多い。問題点を詳細に理解するためには、ツールを利用して最小限必要な情報を取得する必要がある。エンドユーザが抱える問題を切り分けるための典型的ネットワーク診断ツールを学習
11	Cleaning Up After an Attack	Labs Volume 1	Instructional	Intermediate	Recover	2	Cyber security professionals understand that simply detecting and responding to an incident is not enough to adequately protect an organization's business processes and corporate assets. Therefore, it is important that practitioners understand how to recover from an incident. In this lab, students will learn how to ensure no backdoors or additional compromises exist on a system after an attack.	Cleaning Up After an Attack	攻撃後のクリーンアップ	Labのみ	自動教育指導	中級	復旧	2時間	サイバー攻撃を受けた際の後始末として、単なるインシデントを検知し対応するだけでは、企業の業務/資産を守るには、不十分。インシデント後の完全復旧を実現するために、攻撃後のシステムにバックドア等の抜け道がないことを確認する方法を学習

12	Browser Attacks	Labs Volume 1	Instructional	Advanced	Detect	2	Phishing attacks are the lynchpin of many organizational breaches and exploitations. Cyber security professionals that understand this also understand that many of these attacks are successful due to lack of understanding by end users. This course will teach cyber security professionals how to perform a phishing attack and illustrate the importance of cyber security awareness when browsing the internet.	Browser Attacks	ブラウザ攻撃	Labのみ	自動教育指導	上級	検知	2時間	フィッシングは、組織のネットワークへの侵害/攻撃の常套手段。フィッシングが成功するのは、エンドユーザの理解不足に起因しています。フィッシング攻撃の全容とインターネット閲覧を実施する際の重要な注意点を図解し学習
13	Restoring Data with Secure Copy	Labs Volume 1	Instructional	Advanced	Recover	2	Every cybersecurity professional should understand the importance of obtaining, maintaining, and implementing a baseline of key system element in case of an incident. During the recovery process, pushing out clean baselines is paramount to restore system operations. In this lab, students will learn how to restore important, unaltered information by leveraging secure copy.	Restoring Data with Secure Copy	Secure Copyによる原状復帰	Labのみ	自動教育指導	上級	復旧	2時間	インシデント発生後、キーシステムのベースラインとなる要素の入手/管理/実装が重要。復旧作業の最優先事項は、ベースラインを完全にクリーンにすること。Secure Copyを利用して、重要な情報を原状復旧する方法を学習
14	Testing Web Applications	Labs Volume 1	Instructional	Advanced	Protect	2	Part of a comprehensive defense-in-depth implementation includes testing new capabilities and applications before implementing them into an organizations production network. This course illustrates how students can conduct testing against newly developed web applications to ensure they do not pose a risk to organizational assets.	Testing Web Application	Webアプリケーションのテスト	Labのみ	自動教育指導	上級	防御	2時間	企業ネットワークの実環境で新機能やアプリケーションを稼働させる前に、テストすることが多層防御の一環。組織の資産をリスクに晒すことなく、新規に開発されたWebアプリケーションをテストする方法を学習
15	Malware Analysis	Labs Volume 1	Instructional	Advanced	Respond	2	Part of combating an incident or ensuring that an incident does not re- occur includes conducting in-depth analysis on the elements which compromised the network of the system. Thus, malware analysis has become a key capability which is applied during and after an incident. In this lab, students will gain an understanding of how to conduct malware analysis.	Malware Analysis	マルウェアの解析	Labのみ	自動教育指導	上級	対処	2時間	インシデント対応及び再発防止のためには、ネットワークを構成する要素の多層防御を考慮することが必要。そのためには、インシデント発生時及び発生後のマルウェア解析がキーとなる。マルウェア解析の遂行方法を学習
16	Scanning and Enumeration Challenge	Labs Volume 1	Challenge	Challenge		2	In this challenge, you will have to utilize some of the knowledge you acquired in the previous labs to complete a few tasks. Please make sure to read all instructions carefully and save all results or reports into the specified files. These files are case sensitive and can change results	Scanning and Enumeration Challenge	スキャンとEnumeration(JAVA)のチ	Labのみ	チャレンジ	チャレンジ	区分なし	2時間	本チャレンジのタスクを完了するには、学習した知識の活用が必要。すべての指示を熟読し、結果あるいはレポートを定めたファイルに保存すること。(大文字、小文字を区別要。区別を間違えると異なる結果を招く)
17	Integrity and Malware Analysis Challenge	Labs Volume 1	Challenge	Challenge		2	In this challenge, you will have to utilize some of the knowledge you acquired in the previous labs to complete a few tasks. Please make sure to read all instructions carefully and save all results or reports into the specified files. These files are case sensitive and can change results	Integrity and Malware Analysis Challenge	整合性とマルウェア解析のチャレ	Labのみ	チャレンジ	チャレンジ	区分なし	2時間	本チャレンジのタスクを完了するには、学習した知識の活用が必要。すべての指示を熟読し、結果あるいはレポートを定めたファイルに保存すること。(大文字、小文字を区別要。区別を間違えると異なる結果を招く)
18	Forensics 1: Imaging	Labs Volume 2	Instructional	Beginner	Recover	2	The first step in computer forensics is obtaining a copy of the computers hard drive in question. This lab will guide students through that process.	Forensics 1: Imaging	フォレンジック 1: イメージファイルへの変換	Labのみ	自動教育指導	初級	復旧	2時間	フォレンジックの第一歩は該当コンピュータのハードディスクを複製すること。複製のプロセスを学習
19	Forensics 2: File Recovery	Labs Volume 2	Instructional	Intermediate Page 2	Recover	2	Once an image of the device in question has been obtained, file and recovery forensics can be attempted. In this lab, students will take the image created in a previous lab to investigate a possible data breach in their company.	Forensics 2: File Recovery	フォレンジック 2: ファイルの復旧	Labのみ	自動教育指導	中級	復旧	2時間	ハードディスクのイメージ複製完了後、企業のデータ漏洩の可能性を調査するためのファイル復旧を学習
20	Firewall Setup 2	Labs Volume 2	Instructional	Intermediate	Protect	2	Once the initial firewall setup has been completed it's time to start adding some rules to protect specific network devices from potential threats.	Firewall Setup 2	ファイアウォールの設定 2	Labのみ	自動教育指導	中級	防御	2時間	ファイアウォールの初期設定完了後、サイバー脅威から特定のネットワークデバイスを防御するためのポリシーを設定
21	Mobile Forensics	Labs Volume 2	Instructional	Intermediate	Recover	2	This lab takes students through the nuances of mobile forensics. Mobile Applications, or Apps, utilize very specific technologies to store user data and configurations.	Mobile Forensics	モバイルフォレンジック	Labのみ	自動教育指導	中級	復旧	2時間	モバイルフォレンジックのニュアンスを理解するために、モバイルアプリケーション、Appsを使って、ユーザのデータ、設定を保存する技術を学習
22	SQL Injection	Labs Volume 2	Instructional	Advanced	Detect	2	In this lab, students will be exposed to SQL injection attacks and learn how to implement the elements of prevention.	SQL Injection	SQLインジェクション	Labのみ	自動教育指導	上級	検知	2時間	SQLインジェクション攻撃を実験することにより、防御要素の実装方法を学習
23	Firewall Setup 1	Labs Volume 2	Instructional	Advanced	Detect	2	Firewall routers will help protect your network from external and internal threats. This lab takes students through the first step of setting up a firewall.	Firewall Setup 1	ファイアウォールの設定 1	Labのみ	自動教育指導	上級	検知	2時間	内部、外部の脅威からネットワークを防護するには、ファイアウォールルータが役立つ。ファイアウォールの設定を学習
24	Data Leakage	Labs Volume 3	Instructional	Intermediate	Identify	2	In this lab, students will interact with a username and password leak from a web app.	Data Leakage	情報漏えい	Labのみ	自動教育指導	中級	特定	2時間	web appからのユーザネームおよびパスワード流出を学習
25	DDoS Detection	Labs Volume 3	Instructional	Advanced	Detect	2	Students will experience the different components of a distributed denial of service attack.	DDoS Detection	DDoS攻撃の検知	Labのみ	自動教育指導	上級	検知	2時間	DDoS攻撃の異なる構成要素の体験学習
26	Session Hijacking	Labs Volume 3	Instructional	Advanced	Detect	2	Students will identify web application cookies, interact with Burp, and a MITM attack.	Session Hijacking	セッションハイジャック	Labのみ	自動教育指導	上級	検知	2時間	Web アプリケーションクッキー、Burp、MITM攻撃の特定を学習
27	Insider Threat Identification	Labs Volume 3	Instructional	Beginner	Detect	2	This lab takes students through a situation where a former employee poses a serious threat to the company network.	Insider Threat Identification	内部脅威の特定	Labのみ	自動教育指導	初級	特定	2時間	元従業員が企業ネットワークに深刻な脅威を与えた状況を学習

28	Packet Construction and Kernel Hardening	Labs Volume 3	Instructional	Intermediate	Protect	2	In this lab, students will analyze a flood script built with Scapy, then configure their Linux kernel to detect flooding attacks.	Packet Construction and Kernel Hardening	パケット構成とカーネルのハードニング	Labのみ	自動教育指導	中級	防御	2時間	Scapyを利用したfloodスクリプトの解析と、Flood攻撃を防御するためのLinuxカーネルの設定方法を学習
29	System Baselineing	Labs Volume 3	Instructional	Beginner	Protect	2	Students will get more practice with MBSA, as well as be introduced to the Linux Tiger IDS in this lab.	System Baselineing	システムのベースライニング	Labのみ	自動教育指導	初級	防御	2時間	MBSAの演習とLinux Tiger IDSを学習
30	CSX Volume 3, Challenge 1	Labs Volume 3	Challenge	Intermediate	Protect/Detect	2	As part of this challenge, students must capture packets with Wireshark, configure their firewalls, and use Burp to intercept traffic.	CSX Volume 3, Challenge 1	CSX Volume 3, チャレンジ 1	Labのみ	チャレンジ	中級	防御/検知	2時間	Wiresharkを利用したパケットキャプチャ、ファイアウォール設定及びBurpを利用したトラフィック傍受の演習
31	CSX Volume 3, Challenge 2	Labs Volume 3	Challenge	Intermediate	Protect/Detect	2	Students will detect and respond to a cyber attack.	CSX Volume 3, Challenge 2	CSX Volume 3, チャレンジ 2	Labのみ	チャレンジ	中級	防御/検知	2時間	サイバー攻撃の検知と対応を演習
32	Installing Linux	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students will learn how to install and start using Linux Mint, a user-friendly operating system variant.	Installing Linux	Linuxのインストール	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	使いやすいLinux Mintを利用してインストールと起動を学習
33	Shell and Navigation	CSX Linux Application and Configuration	Instructional	Beginner	Identify	1	Students are introduced to basic commands which they can leverage in the Linux command line interface (CLI).	Shell and Navigation	シェルとナビゲーション	CSX Linuxアプリと設定	自動教育指導	初級	特定	2時間	Linuxコマンドラインインターフェイス (CLI) で利用できる基本コマンドを学習
34	Files, Directories, and Information	CSX Linux Application and Configuration	Instructional	Beginner	Identify	1	Students are provided an opportunity to demonstrate their ability to execute basic Linux terminal commands and navigate different directories.	Files, Directories, and Information	ファイル/ディレクトリ/インフォメーション	CSX Linuxアプリと設定	自動教育指導	初級	特定	2時間	ベーシックなLinuxターミナルコマンドと異なるディレクトリへの移動をデモ演習
35	Files and Standard Input / Output	CSX Linux Application and Configuration	Instructional	Beginner	Identify	2	Students are introduced to the standard input and output capability of the Linux terminal and learn additional commands which will help them leverage Linux effectively.	Files and Standard Input/ Output	ファイルと標準入出力	CSX Linuxアプリと設定	自動教育指導	初級	特定	2時間	Linuxターミナルの入出力機能、Linuxを有効利用するための追加コマンドを学習
36	Using STDIO	CSX Linux Application and Configuration	Instructional	Beginner	Identify	2	Students are presented with an opportunity to demonstrate their ability to leverage STDIO appropriately in a Linux environment.	Using STDIO	STDIOを使う	CSX Linuxアプリと設定	自動教育指導	初級	特定	2時間	Linux環境での適切なSTDIOの利用をデモ演習
37	CLI Tricks	CSX Linux Application and Configuration	Instructional	Beginner	Protect	1	Students learn additional Linux terminal commands which better enable understanding of bash history and environment variables.	CLI Tricks	CLITリック	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	Bashヒストリおよび環境変数をより理解するために役立つLinuxターミナルコマンドを学習
38	Services and Users	CSX Linux Application and Configuration	Instructional	Beginner	Protect	1	Students will learn the how user and group accounts work within the Linux environment and how they impact files and file permissions.	Services and Users	サービスとユーザ	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	Linux環境におけるユーザとグループアカウント機能およびファイルアクセス権を学習
39	Networking	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students learn various networking commands and gain a deeper understanding of the networking capabilities within Linux.	Networking	ネットワーク	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	Linuxの種々のネットワークコマンドを習得し、Linuxネットワークの性能を学習
40	Users and Networking	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students will demonstrate their ability to leverage key Linux commands learned thus far in the course, creating users, variables, and network connections.	Users and Networking	ユーザとネットワーク	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	習得したLinuxコマンドを利用して、ユーザ作成、関数、ネットワーク接続等をデモ演習
41	Package Management, Archives, and Compiling	CSX Linux Application and Configuration	Instructional	Beginner	Protect	2	Students learn how package managers function and how to compress and archive files using TAR. Additionally, they will learn how to compile source code.	Package Management, Archives, and Compiling	パッケージ管理、アーカイブとコンパイル	CSX Linuxアプリと設定	自動教育指導	初級	防御	2時間	package managerの機能、ファイルの圧縮、TARを利用したアーカイブ、ソースコードのコンパイル方法を学習
42	Router Familiarization	CSX Network Application and Configuration	Instructional	Beginner	Identify	1	Without understanding the command line interface (CLI) or the graphical user interface (GUI) of an organization's gateway and/or firewall, cyber security analysts find themselves lost in confusion when an incident occurs. This lab will familiarize students with the CLI and GUI of pFsense, one of the preeminently used open-source firewalls available to organizations.	Router Familiarization	ルータの熟知	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	特定	2時間	インシデント発生時には、組織のファイアウォール等のゲートウェイサーバのコマンドラインインターフェース (CLI) や、グラフィカルユーザインターフェース (GUI) を理解していることが必須。オープンソースファイアウォールで使用されるpFsenseのCLIとGUIを学習
43	Setting up a LAN and a WAN	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Understanding the difference between a Wide Area Network (WAN) and Local Area Network (LAN) connection is critical to cyber security analysts and network engineers alike. Regardless of whether an individual is an incident responder or a help-desk technician, it is important to understand the different types of networks and how they impact the organization. In this lab, students will set up and conduct basic configuration of a WAN and LAN interface on a gateway.	Setting up a LAN and a WAN	LAN及びWANの構築	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	防御	2時間	サイバーセキュリティの解析およびネットワークエンジニアにとって、WANとLANの相違と、組織への影響を理解しておくことは必須。ゲートウェイにおける、WANとLANのインターフェースの基本設定を学習
44	Connecting Clients	CSX Network Application and Configuration	Instructional	Beginner	Identify	2	Cyber security professionals understand that most clients do not magically connect to a network unless Dynamic Host Configuration Protocol (DHCP) is involved. Even then, the use of DHCP needs to be established at key points within a network and requires configuration. In this lab, students will work to ensure that clients are able to connect to a network properly.	Connecting Clients	クライアントの接続	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	防御	2時間	ダイナミックホストコンフィギュレーションプロトコル (DHCP) は、ネットワークコンポーネントを接続する上で欠かせません。DHCPをどのキーとなるポイントに設置し、クライアントが正しくネットワークに接続されるためのDHCP設定を学習

45	Initial Configuration	CSX Network Application and Configuration	Instructional	Beginner	Protect	1	Understanding how to configure a firewall and/or gateway for a first use instance is one of the most important elements of establishing a properly functioning network. In this lab, students will set up a pfSense configuration.	Initial Configuration	初期設定	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	防御	2時間	正しく機能するネットワークを構築するには、ファイアウォールやゲートウェイの初期段階での設定が重要。pfSenseの設定を学習
46	Basic Configuration	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Simply providing connectivity to an organization is insufficient when considering cyber security implications. Ensuring that a firewall is properly configured will guarantee a higher degree of safety when organizational users access network resources. In this lab, students will learn how to navigate a firewall interface to establish appropriate protection mechanisms for organizational users.	Basic Configuration	基本設定	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	防御	2時間	サイバーセキュリティを考慮した場合、単純に接続が完了しただけでは、不十分。正しく設定されたファイアウォールは、組織内のユーザがネットワークリソースにアクセスする際のセキュリティ度を高める。ユーザを適切に保護するためのファイアウォールインターフェースの設定を学習
47	Port Forwarding and VPN Setup	CSX Network Application and Configuration	Instructional	Beginner	Protect	2	Many organizations make use of virtual private networks (VPNs) to protect data coming into and leaving the network. Many remote workers, for example, rely on VPNs to ensure that they can securely work on a corporate network from a distance. In this lab, students will set up and perform preliminary configuration of an organizational VPN.	Port Forwarding and VPN Setup	ポートフォワーディングとVPN設定	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	防御	2時間	多くの組織は、ネットワークを出入りするデータを保護するために、バーチャルプライベートネットワーク(VPN)を利用。特に社外から企業ネットワークにアクセスし、業務を遂行するリモートワーカーは、VPNをセキュリティ確保の手段として利用。企業VPNの基本設定を学習
48	Exploitation Identification and Response	CSX Network Application and Configuration	Instructional	Beginner	Detect Respond	2	Identifying when an exploitation is on a network is one of the key abilities separating a cyber security professional from other IT work roles. Identifying when an exploit is sending data out of a network of responsibility and stopping the data leakage ensures that organizations can safely commence disaster recovery proceedings without losing additional data. In this lab, students will learn how to identify and block an exploitation on their network of responsibility.	Exploitation Identification and Response	脆弱性攻撃の特定と対応	CSX ネットワーク アプリとコンフィグ	自動教育指導	初級	検知/対応	2時間	サイバーセキュリティの専門家には、脆弱性攻撃を特定する能力が必須。ネットワークからデータが流出しようとしている際に、データ流出を阻止することにより、追加情報を流出することなく、安全に災害復旧の実施が可能。ネットワーク上の攻撃の特定とブロック方法を学習
49	Establishing a Network	CSX Network Application and Configuration	Challenge	Intermediate	Identify	2	Cyber security professionals should be able to set up and backup router and firewall configurations in the event of an incident. Ensuring that these backups are on hand is critical, yet, more important is that they exist in the first place. Students will implement what they have learned thus far to ensure that a network is established and a backup of it is secured.	Establishing a Network	ネットワーク構築	CSX ネットワーク アプリとコンフィグ	チャレンジ	中級	特定	2時間	インシデント時にルータとファイアウォールの設定をバックアップすることが重要。手元にバックアップが用意されていること以上に初期段階で実施できることが重要。ネットワーク構築とのセキュアなバックアップ方法を演習
50	Detecting, Responding, Recovering from a Network Attack	CSX Network Application and Configuration	Challenge	Intermediate	Detect Respond Recover	2	Students have learned a myriad of networking skills throughout this course and this final challenge will require them to critically apply all of their newfound talents to an incident occurring on their network of responsibility.	Detecting, Responding, Recovering from a Network Attack	ネットワーク攻撃の検知、対応、復旧	CSX ネットワーク アプリとコンフィグ	チャレンジ	中級	検知/対応	2時間	学習した種々のネットワークスキルを活用してネットワーク上に発生しているインシデントに適用する演習
51	Asset Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	Understanding how to perform basic asset identification is an important skill for any cybersecurity practitioner. Leveraging Nmap, students will learn how to scan a network and determine the identity of computers for which they are responsible.	Asset Identification	資産の特定	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	サイバーセキュリティPractitionerにとって、基本資産の特定方法を理解するのは重要なスキル。Nmapを使用し、ネットワークをスキャンして、管理範疇のコンピュータを特定することを学習
52	Data Flow Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In order to capture and analyze data flow, it is important to understand how to use Wireshark and Tshark, two critical tools in the packet analysis field. This lab helps students use these tools to map endpoints on the network.	Data Flow Identification	データフローの特定	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	データフローの取得・分析には、パケット分析の重要なツールであるWiresharkとTsharkの使用法を理解することが重要。このラボでは上記のツールを利用しネットワークのエンドポイントをマッピングする。
53	Enterprise Asset Identification	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In addition to small networks, it is also just as important to practice working with large networks. Using Nmap and zenmap, students will identify assets on an enterprise network in order to build a topology.	Enterprise Asset Identification	事業体資産の特定	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	小規模ネットワークに加え、大規模ネットワークについても実習することが重要。Nmapとzenmapを使用し、事業体ネットワークの資産を特定してトポロジーを作成する。
54	Data Flow Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	In this lab, students will be identifying packets with Wireshark. Due to the fact that data loss is a prevalent aspect of technology, students will learn to recover the packet identification data using the tool Foremost.	Data Flow Analysis	データフロー分析	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	このラボでは、Wiresharkを使用してパケットを特定する。データの損失は技術上一般的な事象なので、Foremostツールを利用したパケット特定データの復旧を学習。
55	Enterprise Data Flow Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Identify	2	Since Wireshark cannot handle large amounts of data, students will be using SiLK for this lab. SiLK is a command line network protocol analyzer designed to help users map out endpoints within a network.	Enterprise Data Flow Analysis	事業体のデータフロー分析	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	Wiresharkは大容量データを扱えないので、このラボではSiLKを使用。SiLKはネットワーク内のエンドポイントを描くのを補助するコマンドライン・ネットワークプロトコルアナライザーである。
56	Identify Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Identify	2	In this exercise, students will utilize their skills learned during the identify module to complete a challenge mapping their network and identifying an attack on a local machine.	Identify Challenge	「特定」チャレンジ	CSX Practitioner試験対策コース	チャレンジ	中級	特定	2時間	この実習では、「特定」モジュールで学んだスキルを活用し、ネットワークのマッピングとローカルマシンへの攻撃を特定する。
57	Firewall Setup	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn to create firewall rules for a pfSense firewall based on their network's layout.	Firewall Setup	ファイアウォールの設定	CSX Practitioner試験対策コース	自動教育指導	中級	特定	2時間	ネットワーク図に基づき、pfSenseファイアウォールに対するファイアウォールルールの構築を学習。

58	Backup and Restore Points	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn how to create a Windows restore point and backup Linux servers from a baseline functioning. In addition, they will create a task with Windows Task Scheduler.	Backup and Restore Points	バックアップと復旧ポイント	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	基本機能から、Windowsの復旧ポイントの構築およびLinuxサーバーのバックアップ方法を学習。さらに、Windowsタスクスケジューラーでタスクを作成。
59	File System Protections	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	Students will learn how to set file permissions on a Windows Server, as well as an Ubuntu machine, in this lab.	File System Protections	ファイルシステム防御	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	WindowsサーバーおよびUbuntuマシン上でのファイルパーミッション設定方法を学習。
60	OS Baseline	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Protect	2	In this lab, students will get more practice with MBSA, as well as be introduced to the Linux tools Tiger and Lynis.	OS Baseline	OSベースライン	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	MBSAでのさらなる実習、およびLinuxツールであるTigerとLynisについて学習。
61	Protect Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Protect	2	In this exercise, students will utilize skills learned during the Protect module to complete a challenge.	Protect Challenge	「防御」チャレンジ	CSX Practitioner試験対策コース	チャレンジ	中級	防御	2時間	この実習では、「防御」モジュールで学んだスキルを活用しチャレンジを完了する。
62	Sec Onion Setup and Testing	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	In the first lab of the Detect module, students will learn how to set up a standalone Security Onion Server and explore and test its functionality.	Sec Onion Setup and Testing	Security Onion設定・テスト	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	「検知」モジュールの最初のこのラボでは、スタンドアロンのSecurity Onionサーバーの設定、および機能の調査やテスト方法を学習。
63	Snort Rules	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	In this lab, students will learn to construct simple SNORT rules and use Kibana to conduct post-attack analysis.	Snort Rules	Snortルール	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	このラボでは、単純なSNORTルールの構築を学習し、Kibanaを使って攻撃を受けた後の分析を実施。
64	Event Detection	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	An investigation is needed for an intrusion detection system alert. In this lab, students must find out what is occurring in the network.	Event Detection	イベントの検知	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	不正侵入検知システムのアラートは調査が必要である。このラボでは、ネットワークで何が起きているか発見しなければならない。
65	Data and Network Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	Students will use WireShark to conduct a live packet capture while they are under attack. Using WireShark, students will identify the attacker's IP, type of attack, and isolate anomalous packets related to the attack	Data and Network Analysis	データ及びネットワーク分析	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	WireSharkを使って攻撃にあっている最中での実際のパケットキャプチャを実施する。攻撃者のIP、攻撃の種類を特定し、攻撃に関わる異常なパケットを分離する。
66	Vulnerability Analysis	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Detect	2	This lab focuses on the security of the local area network. Vulnerability scans are critical when maintaining strong security within a network. In this lab, students will conduct vulnerability assessments.	Vulnerability Analysis	脆弱性の分析	CSX Practitioner試験対策コース	自動教育指導	中級	防御	2時間	このラボでは、LAN上のセキュリティに焦点を当てる。ネットワーク内の強固なセキュリティを維持するには脆弱性スキャンが重要である。このラボでは、脆弱性評価を実施する。
67	Detect Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Detect	2	In this exercise, students will utilize skills learned during the Detect module to complete a challenge.	Detect Challenge	「検知」チャレンジ	CSX Practitioner試験対策コース	チャレンジ	中級	防御	2時間	この実習では、「検知」モジュールで学んだスキルを活用しチャレンジを完了する。
68	Incident Correlation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	SecOnion has reported a possible threat to the network. Students will investigate the tripped SNORT rule and the system logs of the possible affected systems via Kibana	Incident Correlation	インシデントの相互関係	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	SecOnionがネットワークに対する脅威を報告した。Kibanaを通じて感知されたSNORTルールと、影響を受けた可能性のあるシステムのシステムログを調査する。
69	Network Forensics	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	After snort reported a network issue, students must conduct network forensics on the compromised system to identify and isolate the possible malware during this lab.	Network Forensics	ネットワーク・フォレンジックス	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	Snortがネットワークに問題があることを報告した後、感染したシステムに対してネットワーク・フォレンジックスを実施し、あり得るマルウェアの特定と分離をすること。
70	Malware Investigation and Evaluation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	This lab has students utilize various tools (ClamAV, strings, PDF Parser, and PDF Toolkit), to not only investigate, but also evaluate, possible malware that has been attached to emails in the form of PDFs. In addition, the tool cron will come into play while students conduct their investigation.	Malware Investigation and Evaluation	マルウェアの調査と評価	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	このラボでは、様々なツール(ClamAV、文字列、PDFパーサー、PDFツールキット)を使って、PDF形式でEメールに添付されたマルウェアの調査だけでなく評価を行う。さらに、調査中に、ツールのcronが稼働を始める。
71	Notification and Escalation	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Respond	2	Students will learn to properly document and preserve evidence of an attack, and notify the appropriate personnel in accordance with the Incident Response Plan.	Notification and Escalation	通知と上申	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	攻撃について適切に文書化し、そのエビデンスを保持し、インシデント対応計画に基づき適切な人員に通知することを学習。
72	Response Challenge	CSX Practitioner Exam Prep Course	Challenge	Intermediate	Respond	2	Using Security Onion, SGUIL, Snort, SSH, and ClamAV, students will put their Respond domain skills to the test to complete this challenge.	Response Challenge	「対応」チャレンジ	CSX Practitioner試験対策コース	チャレンジ	中級	検知	2時間	Security Onion、SGUIL、Snort、SSH、ClamAVを使って、「対応」モジュールで習得したスキルをテスト。

73	Re-imaging	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Recover	2	In this lab, students will restore a Linux server from an image. Students will use Clonezilla in order to restore the Linux system to its baseline.	Re-Imaging	再イメージング	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	このラボでは、Linuxサーバーをイメージから復旧する。Clonezillaを使ってLinuxシステムをベースラインから復旧する。
74	Restore Points	CSX Practitioner Exam Prep Course	Instructional	Intermediate	Recover	2	Students will learn to restore a Windows Server using the restore point created in Lab 2.2 "Restore and Backup" in this lab.	Restore Points	復旧ポイント	CSX Practitioner試験対策コース	自動教育指導	中級	検知	2時間	ラボ2.2「復旧とバックアップ」で作成した復旧ポイントを使って、Windowsサーバーを復旧することを学習。
75	Protocol Parsing	Packet Analysis	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify basic information from a packet capture.	Protocol Parsing	プロトコルの解析	パケット解析	自動教育指導	中級	特定	1時間	Wireshark を利用して、キャプチャしたパケットから基本情報の取得方法を学習
76	ARP Analysis	Packet Analysis	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify dissect and understand ARP packets.	Arp Analysis	ARPの解析	パケット解析	自動教育指導	中級	特定	1時間	Wireshark を利用して、ARPパケットの分析と理解を習得
77	Initial Connection	Packet Analysis	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify dissect and understand the type of network activity associated with Internet Control Messaging Protocol (ICMP) and traceroute activity.	Initial Connection	初期接続プロトコル	パケット解析	自動教育指導	中級	特定	1時間	WireSharkを利用してICMPに関わるネットワークアクティビティのタイプ及びトレースルートの分析と理解を習得
78	Interesting Searches	Packet Analysis	Instructional	Intermediate	Identify	1	Students will learn how to conduct packet analysis to identify the types of searches which devices are executing on their network.	Interesting Searches	知っておきたい検索方法	パケット解析	自動教育指導	中級	特定	1時間	ネットワーク上で稼働しているデバイスを検索するためのパケット解析実施要領を学習
79	Additional Pets	Packet Analysis	Challenge	Intermediate	Identify	1	Based on what students have learned, thus far, they are challenged to conduct preliminary analysis on a provided packet capture in order to ascertain information about the device and individual using it.	Additional Pets	追加プログラム	パケット解析	チャレンジ	中級	特定	1時間	習得した知識およびスキルの習熟度を確認するために、例題のパケットキャプチャを解析を実践する演習
80	GET Request and Response Dissection	Packet Analysis	Instructional	Intermediate	Identify	1	Understanding the user-agent affiliated with devices allow analysts to assess what kind of devices are on their network of responsibility. This lab will show students how to properly evaluate a user-agent and characterize a system. Additionally, it will illustrate how to gain contextual information from GET Requests and server responses.	GET Request and Response Dissection	GETリクエストとレスポンスの解析	パケット解析	自動教育指導	中級	特定	1時間	ネットワーク上のデバイスを評価するには、デバイスに関連するユーザーエージェントを理解することが重要。このラボでは、ユーザーエージェントの評価と、システムの特徴を正しく評価する方法を学習するとともに、GETリクエストとサーバーレスポンスから関連性情報を取得する方法を習得
81	Nefarious Employee	Packet Analysis	Challenge	Intermediate	Identify	1	Using the skills learned thus far in the course, students will characterize the traffic and device of a potentially nefarious employee, suspected of selling company secrets.	Nefarious Employee	悪意のある従業員	パケット解析	チャレンジ	中級	特定	1時間	演習で習得した技術を利用して、企業の機密を販売しようとした悪意のある従業員のデバイスとトラフィックを明確化する演習
82	Playing Around	Packet Analysis	Instructional	Intermediate	Identify	1	This lab leverages all of the Wireshark filters and methods presented in the course thus far to show a student how to characterize network traffic and an individual on the network.	Playing Around	お遊び	パケット解析	自動教育指導	中級	特定	1時間	いままでの演習で学習したWiresharkのフィルタと解析方法のまとめとして、ネットワークトラフィックとネットワーク上の個々を明確化する方法を学習
83	Probe Request Analysis	Packet Analysis	Instructional	Intermediate	Identify	1	This lab leverages demonstrates how to analyze a probe request. Students learn what key information can be pulled out of a probe request about a device and a wireless network.	Probae Request Analysis	プローブ要求の解析	パケット解析	自動教育指導	中級	特定	1時間	ワイヤレスネットワーク及びデバイスのプローブ要求を解析し、キーとなる情報を取得する方法を学習
84	Beacon Analysis	Packet Analysis	Challenge	Intermediate	Identify	1	This lab leverages requires students to leverage the skills and filters learned in the probe request lab and use them to analyze a captured beacon packet.	Beacon Analysis	ビーコンの解析	パケット解析	チャレンジ	中級	特定	1時間	プローブ要求で学習したスキルとフィルタを利用して、キャプチャされたビーコンパケットの解析方法を学習
85	Network Topology	Packet Analysis	Instructional	Intermediate	Identify	1	Understanding how to create a network map from a provided packet capture is important for individuals desiring to gain a better understanding of a network, but are prohibited from disrupting the network by introducing packets into the medium.	Network Topology	ネットワークトポロジ	パケット解析	自動教育指導	中級	特定	1時間	ネットワークの理解をより深めるために重要な、キャプチャされたパケットを基にネットワーク図の作成方法を学習。但し、ネットワークを崩壊させる危険があるため、媒体(メディア)への開示は行わない
86	Wireless Network Topology	Packet Analysis	Challenge	Intermediate	Identify	1	Testing all the skills learned in the Packet Analysis course and labs, this challenge requires students to create a network topology (netmap) of the 192.168.1.0 network in the provided packet capture.	Wireless Network Topology	ワイヤレスネットワークトポロジ	パケット解析	チャレンジ	中級	特定	1時間	パケット解析コースで習得したスキルを利用して、例題のパケットキャプチャから192.168.1.0ネットワークのネットワークトポロジを作成する演習
87	Blaster Worm Analysis	Packet Analysis	Instructional	Intermediate	Identify	1	Understanding how systems become infected and recognizing affiliated packets is an important skill for incident responders and IT personnel. In this lab, students will analyze a Blaster worm infection's affiliated packets.	Blaster Worm Analysis	Blasterワームの解析	パケット解析	自動教育指導	中級	特定	1時間	インシデントレスポンスにおいて、システムの感染に関係するパケットを認識し、感染経路を理解することが重要。Blasterワーム感染に関連したパケットの解析を学習
88	Rogue AP and Mobile Analysis	Packet Analysis	Challenge	Intermediate	Identify	1	Students will identify and characterize the rouge access point that is connected to a network of responsibility. They will also assess the traffic on the access point to determine what type of device is using it and what that device is doing.	Rogue AP and Mobile Analysis	不正アクセスポイントとモバイル機器の解析	パケット解析	チャレンジ	中級	特定	1時間	ネットワークに接続された不正アクセスポイントの明確化とともに、アクセスポイントのトラフィックから、接続されている機器と接続目的の解析を学習
89	Complete Netmap and Device Characterization	Packet Analysis	Challenge	Intermediate	Identify	2	Students will leverage all of the skills learned in the Packet Analysis course and labs to provide in-depth analysis of a provided capture. Final submissions will include a complete network topology and a fully characterized device.	Complete Netmap and Device Characterization	ネットワーク図とデバイスの明確化	パケット解析	チャレンジ	中級	特定	1時間	パケット解析コースで習得したスキルを利用して、例題のパケットキャプチャの詳細な解析する演習。ネットワークトポロジの完全な把握とデバイスの明確化を最終目的とする。

90 (v6)	Linux Shell and Commands	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	The Unix bourne-again shell, also known as Bash, is a command processor that runs in the Kali Linux terminal. Bash scripting and command execution is the foundation of penetration testing.	Linux Shell and Commands	Linuxシェルとコマンド	CSX侵入テスト概論	自動教育指導	初級	特定	2	侵入テストの基礎となる、Kali Linux上で動くコマンドプロセッサBashのスク립トおよびコマンド実行を学習
91 (v6)	TCP/IP Basics	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	In Linux, viewing and configuring network connections is not only a fundamental aspect of computer and network security, but it is also an essential piece of the penetration testing infrastructure.	TCP/IP Basics	TCP/IP基礎	CSX侵入テスト概論	自動教育指導	初級	特定	2	Linuxでは、ネットワーク接続を調査・構成することはコンピュータとネットワーク・セキュリティの基本であるばかりでなく、侵入テストインフラの重要な要素である。
92 (v6)	Packet Inquiry	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Wireshark is a free and open source network protocol analyzer that is both efficient and effective. In Kali Linux, packets are captured in Wireshark by penetration testers and cybersecurity professionals on a daily basis.	Packet Inquiry	パケット検索	CSX侵入テスト概論	自動教育指導	初級	特定	2	Wiresharkは、効果的かつ有用なオープンソースネットワークプロトコルアナライザで、侵入テスト実施者やサイバーセキュリティ専門家により、Kali Linuxでパケットキャプチャに利用されている。
93 (v6)	Network Discovery	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Again, Wireshark is a free and open source network protocol analyzer that is both efficient and effective. It is necessary for penetration testers to understand the packets that are traversing through a network segment while discovering network hosts and navigating to websites.	Network Discovery	ネットワーク発見	CSX侵入テスト概論	自動教育指導	初級	特定	2	Wiresharkは、効果的かつ有用なオープンソースネットワークプロトコルアナライザである。侵入テスト実施者は、ネットワークホストの発見やウェブサイトをナビゲートする間、ネットワークセグメントを行き来するパケットを理解する必要がある。
94 (v6)	Service Enumeration	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	The CLI tool, nmap, and its GUI counterpart, Zenmap, are both extremely important when it comes to identifying and enumerating network hosts, ports and services, and more.	Service Enumeration	サービス列挙	CSX侵入テスト概論	自動教育指導	初級	特定	2	CLIツール、nmap、そのGUI版であるZenmapは、ネットワークホスト、ポート、サービスその他を列挙するのに非常に重要なツールである。
95 (v6)	Network Vulnerability Identification	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Metasploit is a software project that is arranged for penetration testing. Metasploit provides essential information about computer and network security vulnerabilities and helps users exploit machines.	Network Vulnerability Identification	ネットワーク脆弱性特定	CSX侵入テスト概論	自動教育指導	初級	特定	2	Metasploit は侵入テスト用に用意されたソフトウェアプロジェクトであり、コンピュータとネットワークのセキュリティの脆弱性に関する重要な情報を提供し、コンピュータの弱点を突く手助けをする。
96 (v6)	Network Vulnerability Exploitation	CSX Penetration Testing Overview	Instructional	Beginner	Identify	2	Using the results of an exploit to enable another exploit is something penetration testers do on a daily basis. Once their exploits take them deep enough into a remote system, using MySQL syntax to navigate a MySQL database can be a crucial skill when they're in search of information.	Network Vulnerability Exploitation	ネットワーク脆弱性探究	CSX侵入テスト概論	自動教育指導	初級	特定	2	侵入テスト実施者は、日々エクスプロイトした結果を利用してさらに侵入を試みている。リモートシステムまでたどりついたら、MySQLシNTAXSを利用してMySQLデータベースを検索するのが、情報を探す上で非常に重要なスキルである。
97 (v6)	Evidence Removal	CSX Penetration Testing Overview	Instructional	Beginner	Recover	2	Removing evidence, also known as covering your tracks, is the last step in penetration testing. Although it is the last step, it is by far not the least important.	Evidence Removal	エビデンスの除去	CSX侵入テスト概論	自動教育指導	初級	復旧	2	エビデンスを除去する、もしくは足跡を隠すのが、侵入テストの最後の大切なステップである。
98 (v6)	CPTO Challenge 1	CSX Penetration Testing Overview	Challenge	Beginner	Identify	2	This challenge is based on the first four labs of this series. This lab reflects the Identify domain of penetration testing.	CPTO Challenge 1	CPTO チャレンジ 1	CSX侵入テスト概論	チャレンジ	初級	特定	2	本チャレンジは、CSX侵入テスト概論の最初の4つのラボに基づき侵入テストの「特定」ドメインに関連したものである。
99 (v6)	CPTO Challenge 2	CSX Penetration Testing Overview	Challenge	Beginner	Detect	2	This challenge is based on the last four labs of this series. This lab reflects the Identify, Detect, and Recover domains of penetration testing.	CPTO Challenge 2	CPTO チャレンジ 2	CSX侵入テスト概論	チャレンジ	初級	検知	2	本チャレンジは、CSX侵入テスト概論の後半の4つのラボに基づき、侵入テストの「特定」「検知」「復旧」ドメインに関連したものである。
100 (v6)	Footprinting	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	This lab instructs students on the basics of open source researching a target domain.	Footprinting	フットプリンティング	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	ターゲットドメインを調査し、オープンソースの基礎を学習。
101 (v6)	Initial Vulnerability Scanner Setup	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	OpenVAS is a popular open-source vulnerability scanner and management tool. One of the tools included with OpenVAS is the Greenbone Security Assistant (GSA), a web application which connects to the OpenVAS manager daemon to provide a GUI for vulnerability management. In this lab, you'll become familiar with how these tools work and how to use them.	Initial Vulnerability Scanner Setup	脆弱性スキャナーのセットアップ	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	OpenVASは、よく知られたオープンソースの脆弱性スキャナーおよび管理ツールである。OpenVASに含まれるGreenbone Security Assistant (GSA)は、ウェブアプリケーションで、OpenVASマネージャードアモンと接続し脆弱性管理のGUIを提供する。このラボでは、これらのツールの動きや使い方を学習。
102 (v6)	Vulnerability Analysis	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Conducting a vulnerability scan is important. In this lab, students will learn how to interpret the results from the vulnerability scans.	Vulnerability Analysis	脆弱性分析	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	脆弱性スキャンの実施は重要である。脆弱性スキャンの結果を解釈する方法を学習。
103 (v6)	Initial Exploitation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	It's important to realize not all exploits require scripted code and payloads. Sometimes a simple Nmap scan - coupled with a Telnet connection and a clever username - is all you need.	Initial Exploitation	初期エクスプロイト	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	エクスプロイトには、コードスクリプトとペイロードが必要とは限らない。Telnet接続と巧みなユーザー名を組み合わせただけで単純なNmapスキャンで可能なことを学習。
104 (v6)	Privilege Escalation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Privilege escalation exploits are one of the most common exploit types. By exploiting flaws in the OS, this type of exploit allows a user to elevate their level of system access. Once elevated, a user can make permanent changes and gain control of the vulnerable system.	Privilege Escalation	権限昇格	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	権限昇格は最も一般的なエクスプロイトである。OSの欠陥を利用して、ユーザのシステムアクセス権限を昇格させて、永続的な変更を行い脆弱性のあるシステムを制御する。
105 (v6)	Backdoor Implementation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	This lab will take students through creating backdoors in systems as well as implementing inadvertent backdoors and exploitations.	Backdoor Implementation	バックドア実装	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	このラボでは、システム内のバックドアの作り方、および不注意なバックドアやエクスプロイトの実施について学習する。
106 (v6)	Covering Tracks	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	When a system is accessed, either by normal or clandestine operations, evidence is left behind in log files. Sanitation of those log files is important to cover up any activity that had taken place.	Covering Tracks	足跡のカバー	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	システムへのアクセスは正当、違法にかかわらずログファイルにエビデンスが残る。実行したアクティビティを隠すためには、こうしたログファイルの除去が重要である。
107 (v6)	Deeper Exploitation	CSX Vulnerability and Exploitation Course	Instructional	Intermediate	Detect	2	Once a system has been compromised with administrator level access all sensitive system information is available to the attacker. In this lab, we'll take you through obtaining that system information.	Deeper Exploitation	より深いエクスプロイト	CSX脆弱性とエクスプロイトコース	自動教育指導	中級	検知	2	管理者レベルでのシステムへの不正アクセスにより、攻撃者はすべての重要なシステム情報を利用できるようになる。このラボでは、システム情報の取得について学習。
108 (v6)	CVEC Challenge	CSX Vulnerability and Exploitation Course	Challenge	Intermediate	Detect	2	This is a challenge lab based on the materials covered in the previous 8 labs.	CVEC Challenge	CVECチャレンジ	CSX脆弱性とエクスプロイトコース	チャレンジ	中級	検知	2	前述の8ラボで学習した資料に基づくラボベースのチャレンジ

109 (v6)	Spectre Mitigation	Labs Volume 4	Instructional	Intermediate	Protect	2	Spectre exploits crucial and vital susceptibilities in today's processors. Spectre uses speculative execution on processors using branch prediction. In other terms, Spectre takes advantages of the processors' performance techniques.	Spectre Mitigation	Spectre軽減	ラボ4	自動教育 指導	中級	検知	2	Spectreは今日のプロセッサにある重大で致命的な脆弱性で、分岐予測を使用しているプロセッサの投機的実行を利用する。言いかえれば、Spectreはプロセッサの実行テクニックを利用している。
110 (v6)	Meltdown Mitigation	Labs Volume 4	Instructional	Intermediate	Protect	2	Meltdown exploits crucial and vital susceptibilities in today's processors. Meltdown is similar to Spectre but there are some differences. Meltdown allows access to ANY data that is mapped to current memory space.	Meltdown Mitigation	Meltdown軽減	ラボ4	自動教育 指導	中級	検知	2	MeltdownはSpectre同様今日のプロセッサなる重大で致命的な脆弱性である。Spectreとの違いは、現在のメモリ領域にどのようなデータでもマッピングできることである。
111 (v6)	Chrome Extension Testing	Labs Volume 4	Instructional	Intermediate	Detect	2	In early 2018, security researchers discovered several nefarious Chrome extensions that were making unwanted calls to ad servers. This resulted in the removal of these Chrome extensions from the Google Extension Store and a heightened awareness to the possible effects of Chrome extensions on business networks.	Chrome Extension Testing	Chrome拡張機能テスト	ラボ4	自動教育 指導	中級	検知	2	2018年初め、管理サーバに意図しないコールを行う不正なChrome拡張機能が複数セキュリティ調査者により発見された。その結果、Google拡張機能ストアからこれらのChrome拡張機能は削除され、業務ネットワークへのChrome拡張機能に及ぼす影響についての意識が高まった。
112 (v6)	Linux Baseline with Lynis	Labs Volume 4	Instructional	Beginner	Identify	2	Lynis is a security auditing tool designed specifically for Linux systems. Lynis is an open-source product that runs on the host itself and is essential when it comes to obtaining knowledge on Linux baselining.	Linux Baseline with Lynis	Lynisを使用したLinuxベースライン	ラボ4	自動教育 指導	初級	特定	2	LynisはLinuxシステム用のセキュリティ監査ツールで、ホスト上で動くオープンソース製品であり、Linuxベースラインの知識を取得するのに必須のツールである。
113 (v6)	Securing Web Browsers	Labs Volume 4	Instructional	Intermediate	Protect	2	Ensuring web browsing security is an integral part of cybersecurity as a whole. Google Chrome and Mozilla Firefox are both used in this lab.	Securing Web Browsers	Webブラウザセキュリティ	ラボ4	自動教育 指導	中級	検知	2	Webブラウザのセキュリティ確保は、サイバーセキュリティ全般に不可欠な要素である。このラボではGoogle ChromeとMozilla Firefoxを使用する。
114 (v6)	Malware Detection and Removal with Baseline	Labs Volume 4	Challenge	Advanced	Respond	2	In addition to Lynis, this lab features Difference, ClamAV, and other vital Linux tools. This lab fuses these essentials together in order to present a challenge.	Malware Detection and Removal with Baseline	ベースラインでのマルウェア検知と削除	ラボ4	チャレンジ	上級	対応	2	このラボでは、Lynisに加えて、Difference、ClamAVその他必須のLinuxツールを取り上げ、統合的に使用することでチャレンジを提起する。
115 (v6)	Domain Detection	Labs Volume 4	Challenge	Advanced	Detect	2	This challenge lab will be testing your packet analysis and domain detections skills.	Domain Detection	ドメイン検知	ラボ4	チャレンジ	上級	検知	2	このチャレンジでは、パケット分析とドメイン検知スキルをテストする。

*CPE is not available for individual labs in each of the CSX Practitioner courses, however 40 hours of CPE are available for successful completion of the entire course (40 hours for Course 1, 40 hours for Course 2, and 40 hours for Course 3)