CYBERSECURITY NEXUS™ (CSX) TRAINING PLATFORM LABS

LABS + COURSES PACKAGE

Ver9 2019/01

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語名 英語タイトル	Lesson Lesson名	Related Course コース関連/形態	LAB Type 授業スタイ	Level レベル	Functional Domain 機能領域	Estimated Duration 予想就業時間	Description 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、該当するトラヒ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、プラットホームの変更等に伴い、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	**Threat Detection**	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 end user 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

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
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動させる前に、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れたファイルに保存すること。(大文字、小文字を区別要。区別を間違うと異なった結果を招く)
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ンジ	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れたファイルに保存すること。(大文字、小文字を区別要。区別を間違うと異なった結果を招く)
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体験することにより、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攻撃の異なった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 Baselining**	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 Baselining	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

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
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	CLIトリック	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オールで使用される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 an 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

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
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	知/対応/復	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るので、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ファイヤーウォールに対するファイヤー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ンレンジを完了する。

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
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ンレンジを完了する。
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。Kibara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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	Instructional	Intermediate	Identify	1	Students will leverage Wireshark to identify dissect and understand ARP packets.	Arp Analysis	ARPの解析	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	自動教育指導	中級	特定	1時間	ネットワーク上で稼動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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
80	**GET Request and Response Dissection**	CSX Packet Analysis Course	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	CSXパケット解析コース	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・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、システムの特性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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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.	Probe Request Analysis	プローブ要求の解析	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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	**Rouge AP and Mobile Analysis**	CSX Packet Analysis Course	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.	Rouge AP and Mobile Analysis	不正アクセスポイントとモバイル機器の解析	CSXパケット解析コース	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**	CSX Packet Analysis Course	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	CSXパケット解析コース	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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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のスクリプ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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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。

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
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ペネトレーション（侵入）テスト概論	自動教育指導	初級	特定	2時間	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シンタックスを利用してMy SQL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ペネトレーション（侵入）テスト概論	自動教育指導	初級	復旧	2時間	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ペネトレーション（侵入）テスト概論	チャレンジ	初級	特定	2時間	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ペネトレーション（侵入）テスト概論	チャレンジ	初級	検知	2時間	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時間	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時間	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マネージャーデー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時間	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時間	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名を組み合わせた単純な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時間	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、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時間	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時間	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時間	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時間	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時間	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。言いかえると、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時間	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時間	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時間	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時間	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時間	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時間	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。

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
116 (v7)	**SSH Tunnel Implementation**	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	In this advanced-level lab, students will learn how to setup an SSH Tunnel, enumerate services through a tunnel, and exploit through a tunnel.	SSH Tunnel Implementation	SSHトンネル実装	CSX上級エクスプロイトコース	自動教育指導	上級	検知	2時間	この上級ラボでは、SSHトンネルの設定方法、トンネルを通じたサービス列挙や脆弱性検索の方法について学習する。
117 (v7)	**Multiple SSH Tunnel Exploitation Implementation**	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	Students will learn how to utilize multiple redirectors on multiple ports for scanning, enumeration, and exploitation. They will also learn how to create a reverse tunnel through a [illegible]	Multiple SSH Tunnel Exploitation Implementation	複数SSHトンネルエクスプロイテーション実装	CSX上級エクスプロイトコース	自動教育指導	上級	検知	2時間	スキャン、列挙、脆弱性検索のため、多重ポート上の多重リダイレクターの活用方法を学習する。またネットワークを通じたリバーストンネルの作成方法も学習する。
118 (v7)	**Metasploit PortProxy Implementation**	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	In this lab, students will use Metaploit's PortProxy post-exploitation module to redirect a port scan, an exploit and a backdoor communication.	Metasploit PortProxy Implementation	Metasploit PortProxy 実装	CSX上級エクスプロイトコース	自動教育指導	上級	検知	2時間	本ラボでは、MetasploitのPortProxyモジュールを使用して、ポートスキャン、エクスプロイト、バックドア通信のリダイレクトを学習する。
119 (v7)	**Metrepreter Autoroute Implementation**	CSX Advanced Exploitation Course	Instructional	Advanced	Detect	2	This time, a student will learn how to use Metaploit's AutoRoute Script to redirect a port scan, an exploit and a backdoor communication.	Metrepreter Autoroute Implementation	Metrepreter Autoroute 実装	CSX上級エクスプロイトコース	自動教育指導	上級	検知	2時間	ポートスキャン、エクスプロイト、バックドア通信のリダイレクトをするための、MetasploitのAutoRouteスクリプトの使用方法を学習する。
120 (v7)	**Network Assessment Challenge**	CSX Advanced Exploitation Course	Challenge	Advanced	Detect	4	For this final exercise, students will utilize the tunneling and redirection skills learned in this course, as well as all previous training, to gain access to a network and investigate	Network Assessment Challenge	ネットワーク評価チャレンジ	CSX上級エクスプロイトコース	チャレンジ	上級	検知	4時間	この最終実習では、コースやトレーニング全てで学習したトンネルとリダイレクトスキルを活用し、ネットワークへアクセスして調査を行う。
121 (v7)	**Script Construction and Execution**	Labs Volume 5	Instructional	Beginner	Identify	2	Assuming the role of a network security expert, who is responsible for creating, executing and then examining the output of a bash script and a batch file, students will learn the basics of scripting using both the Kali Linux bash and the [illegible]	Script Construction and Execution	スクリプト作成と実行	ラボ5	自動教育指導	初級	特定	2時間	ネットワークセキュリティ専門家の役割としてbashスクリプトとバッチファイルの作成、実行、結果の検証がある。Kali Linux bashとWindows 10のコマンドプロンプトを使用してスクリプト作成の基礎を学習する。
122 (v7)	**Passive Computer Forensics**	Labs Volume 5	Instructional	Intermediate	Recover	2	Leveraging the Kali and Clonezilla Linux distributions, students will image a file system, inspect identified files and leverage tools to identify nefarious deleted emails.	Passive Computer Forensics	パッシブ・コンピューターフォレンジックス	ラボ5	自動教育指導	中級	復旧	2時間	KaliおよびClonezilla Linuxディストリビューションを利用し、ファイルシステムのイメージング、特定したファイルの調査、削除された不正なEメールを特定するためのツール活用を行う。
123 (v7)	**Intrusion Detection System Implementation and Testing**	Labs Volume 5	Instructional	Beginner	Detect	2	Students will evaluate the functionality and applicability of IDS tools provided by the Security Onion Linux distribution, by identifying incidents and responding to alerts within the	Intrusion Detection System Implementation and Testing	不正侵入検知システム実装とテスト	ラボ5	自動教育指導	初級	検知	2時間	Security Onion Linuxディストリビューションで提供されるIDSツールの機能と可用性を評価する。範疇内のネットワークにおけるインシデントの特定とアラートへの対応を行う。
124 (v7)	**Triaging Incidents**	Labs Volume 5	Instructional	Intermediate	Respond	2	Students will generate malicious traffic, examine the generated traffic, and respond to the incidents based upon their order of importance. These actions will enable the [illegible]	Triaging Incidents	インシデントのトリアージ	ラボ5	自動教育指導	中級	対応	2時間	悪意のあるトラフィックを生成、検証し、重要度に基づいてインシデントに対応する。これにより、対応者と同様攻撃者の観点からインシデントを理解できる。
125 (v7)	**IOT Device Indicators**	Labs Volume 5	Instructional	Intermediate	Detect	2	Students will analyze a collection of IOT device communications packets and correlate the timing of data spikes with IOT user habits.	IOT Device Indicators	IoTデバイス測定	ラボ5	自動教育指導	中級	検知	2時間	IoTデバイスの通信パケットを分析し、IoTユーザーの習慣とデータスパイクの関連付けを行う。
126 (v7)	**Home Automation Device Patterns**	Labs Volume 5	Instructional	Intermediate	Detect	2	This lab will teach a student how to analyze wireless data collection in order to map and characterize a network and the devices resident upon said network.	Home Automation Device Patterns	ホームオートメーションデバイス分析	ラボ5	自動教育指導	中級	検知	2時間	ネットワークとその中に存在するデバイスをマッピングし特性を理解するための、無線データの分析方法を学習する。
127 (v7)	**Incident Response Script Implementation**	Labs Volume 5	Challenge	Advanced	Respond	2	This lab will challenge students to create scripts and appropriately leverage tools within Security Onion to enhance IDS implementation and response times.	Incident Response Script Implementation	インシデント対応スクリプト実装	ラボ5	チャレンジ	上級	対応	2時間	このラボでは、スクリプトを作成し、Security Onionのツールを適切に活用して、IDS実装と対応時間の向上を図ることにチャレンジする。
128 (v7)	**Forensic Data Recovery and Analysis**	Labs Volume 5	Challenge	Advanced	Detect	2	This lab will challenge students to leverage tools such as Photorec and Wireshark to conduct forensic analysis in order to identify potential malicious activity indicators.	Forensic Data Recovery and Analysis	フォレンジックデータ復旧と分析	ラボ5	チャレンジ	上級	検知	2時間	このラボでは、潜在的な悪意のある活動を特定するため、PhotorecやWiresharkといったツールを活用しフォレンジック分析を行うことにチャレンジする。
129 (v8)	**Kali Forensics Environment**	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Kali Linux provides many utilities to navigate the folder structure, list file, read files, create files, move files, remove files, add directories, and remove directories. As the owner of G's Forensics LLC, you have been curious about using Kali for conducting digital forensic examinations. As a seasoned Forensics Examiner, you know a tool is only as good as the craftsman's hand. And, the craftsmen must master their tools to be successful.	Kali Forensics Environment	Kaliフォレンジック環境	CSXフォレンジック分析コース	自動教育指導	初級	対応	2時間	Kali Linuxは、フォルダー構造確認、ファイルのリスト/読み出し/作成/移動/削除、ディレクトリの追加/削除など多くのユーティリティを提供している。本研修では、受講者はG's Forensic LLCのオーナーとして、デジタルフォレンジック試験を実施するのにKaliに興味を抱いてきたという前提である。フォレンジック調査者として、ツールは技能にたけた人が使ってこそ有用であると認識している。技能者として成功するためにはツールを使いこなさなくてはならない。
130 (v8)	**PostgreSQL Configuration**	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	A database is a desirable tool when dealing with documentation and evidence management. It provides structure and compartmentalization of cases and their associated files. As a forensic examiner, it is your job to understand how database management works with your investigations. It is your responsibility to ensure that your environment is configured correctly.	PostgreSQL Configuration	PostgreSQL構成	CSXフォレンジック分析コース	自動教育指導	初級	対応	2時間	データベースは、文書やエビデンス管理に有効なツールであり、案件とその関連ファイルの構造や区分化を提供する。フォレンジック調査者は、調査においてデータベース管理がどのように働くかを理解している責務がある。また環境が正しく構成されているかを確認する責任もある。
131 (v8)	**Foreman Configuration**	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Documentation is a very important aspect of any forensic investigation. Your documents attest to your methodology and provide evidence that you executed with due care and due diligence your responsibilities as a Forensics Examiner.	Foreman Configuration	Foreman構成	CSXフォレンジック分析コース	自動教育指導	初級	対応	2時間	どのようなフォレンジック調査においても、文書は非常に重要な側面である。文書は、フォレンジック調査者としての方法論を裏づけし、しかるべき注意と適切な配慮をもって責務を実施したことに関するエビデンスを提供する。
132 (v8)	**Final Foreman Setup**	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	In this lab, you will continue your efforts from the previous lab in order to finalize your Foreman forensics case management tool setup using proper documentation.	Final Foreman Setup	Foreman最終セットアップ	CSXフォレンジック分析コース	自動教育指導	初級	対応	2時間	このラボでは、前ラボに引き続き、適切な文書を用いてForemanフォレンジック管理ツールのセットアップを完了する。
133 (v8)	**A New Case**	CSX Forensic Analysis Course	Instructional	Beginner	Respond	2	Receiving evidence, continuing the Chain of Custody, and creating exact working copies of the evidence is a major component of the forensics process. You have been contacted by a prosecuting attorney to aid in an important case. Moments ago, a bonded courier arrived at your location with digital evidence. The evidence has been processed and loaded into your Digital Evidence Locker.	A New Case	新規案件	CSXフォレンジック分析コース	自動教育指導	初級	対応	2時間	フォレンジックプロセスにおいて、エビデンスの受領、分析過程の継続的な監視、エビデンスの正確なコピーの作成は、主要な要素である。このラボでは、検察官から連絡があり重要な案件について支援してくれるよう要請されている。そして、デジタルエビデンスの入った封印された宅配便が届いた。エビデンスは処理され、デジタルエビデンスロッカーにロードされる手順を学習する。
134 (v8)	**My First Case**	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Acceptance of a case is it at the discretion of the examiner in charge. The examiner must feel competent in his/her ability to complete the assignment in an unbiased manner. For this scenario, you will play the role of Happy Foreman, newly promoted lead examiner of G's Forensics, LLC. Mr. G has informed you of a new case. This will be your first case as the lead examiner.	My First Case	私の最初の案件	CSXフォレンジック分析コース	自動教育指導	中級	対応	2時間	案件を引き受けるか否かは、担当する調査者の判断になる。調査者は先入観のない状態で任務を完了するにあたり、自身の能力に自信を持っている必要がある。このシナリオでは、G's Forensics, LLCで主調査者に新たに昇進したHappy Foreman役を演じる。Mr. Gから新たな案件の連絡があり、これが主調査者として初めての案件対応手法を学習する。
135 (v8)	**A Picture**	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	In Forensics, pictures are an important factor in evidence. Pictures themselves are a point in time snapshot of what might have been, and they contain a lot more information then what we see during a visual examination. All files, pictures included, contain metadata, which is data about the data.	A Picture	画像	CSXフォレンジック分析コース	自動教育指導	中級	対応	2時間	フォレンジックにおいて、画像はエビデンスの重要な要因である。画像そのものが、ある時点でのスナップショットであるとともに、可視検証中に観察する多くの情報を含んでいる。画像を含め、全てのファイルにはデータに関するデータであるメタデータが含まれている。
136 (v8)	**Data DNA**	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Forensics commonly analyzes collections of files in a structured form. In this endeavor, we will start from the lowest level, the partition table, and gradually work our way up.	Data DNA	データDNA	CSXフォレンジック分析コース	自動教育指導	中級	対応	2時間	フォレンジックでは通常、構造化された収集データを分析する。このラボでは、最下層レベルのパーティションテーブルから始め、徐々に上層を分析する。
137 (v8)	**The Missing Piece**	CSX Forensic Analysis Course	Instructional	Intermediate	Respond	2	Now that we have images let's conduct forensic file analysis to start building a case. We'll use built-in file carving and analysis tools that Kali has to offer such as Foremost and Autopsy.	The Missing Piece	不足している部分	CSXフォレンジック分析コース	自動教育指導	中級	対応	2時間	入手した画像データを用いフォレンジックファイル分析を実施するための構築を実施する。Kaliに搭載されているForemostやAutopsyといった組み込み用のファイルカービングツールや分析ツールを使用したフォレンジックを学習する
138 (v8)	**Forensics Challenge**	CSX Forensic Analysis Course	Challenge	Advanced	Respond	2	Using the knowledge gained in during this course it's time to catch a bad guy! During this challenge lab you will be required to keep up documentation while discovering evidence for a forensic operation!	Forensics Challenge	フォレンジックチャレンジ	CSXフォレンジック分析コース	チャレンジ	上級	対応	2時間	本コースで習得した知識を使って、悪者を捕まえる。このチャレンジラボではフォレンジックのエビデンスを発見しつつ、文書を保持することが必要となる。

No.	LAB	RELATED COURSE	LAB TYPE	LEVEL	FUNCTIONAL DOMAIN	CPE HOURS	DESCRIPTION	英語タイトル	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
139 (v8)	**Implementing Database Management**	Labs Volume 6	Instructional	Intermediate	Identify	2	MySQL uses the Structured Query Language to provide a free and open source RDBMS. As an employee new to the database management team, it is your responsibility to understand the essentials of the Structured Query Language. You will be using MySQL to create a database, create a table, and insert valuable data in order to get a basic understanding of database management.	Implementing Database Management	データベース管理の実装	ラボ6	自動教育指導	中級	特定	2時間	My SQLは、オープンソースのRDBMSを提供する無料の構造化照会言語（SQL）である。このラボでは、データベース管理チームの新顔として、SQLの要点を理解する必要があるという想定で、MySQLを使って、データベースの作成、テーブルの作成、重要データの挿入をおこない、データベース管理の基本を学ぶ。
140 (v8)	**Testing Intrusion Detection Systems**	Labs Volume 6	Instructional	Intermediate	Identify	2	Cybersecurity Practitioners must understand how intrusion detection systems work and how they can be fine-tuned for a specific organizations needs. This lab will teach students how to create Snort rules for web-based attacks and how to manage alerts in Sguil.	Testing Intrusion Detection Systems	侵入検知システム（IDS）のテスト	ラボ6	自動教育指導	中級	特定	2時間	サイバーセキュリティ熟練者は、侵入検知システムの働きや、組織の特定の要件に合わせた微調整の方法を理解している必要がある。このラボでは、ウェブベースの攻撃に対するSnortルールの作り方や、Sguilでのアラートの管理方法について学ぶ。
141 (v8)	**Initializing Honeypots**	Labs Volume 6	Instructional	Intermediate	Detect	2	Honeypots are used as bait against hackers wanting unauthorized access into networks. As a network security expert, it is your responsibility to set up honeypots on different machines in order to see its benefits. You will then save, read, and copy the logs for further investigation.	Initializing Honeypots	ハニーポットの初期化	ラボ6	自動教育指導	中級	検知	2時間	ハニーポットは、ネットワークへの不正アクセスを試みるハッカーに対する罠として使われる。ネットワークセキュリティの専門家として、異なるマシーンにハニーポットを設定し、その効果をみる必要がある。その後、さらなる調査のためログの保存、読み込み、コピーを行う。
142 (v8)	**Generating and Analyzing Logs**	Labs Volume 6	Instructional	Intermediate	Respond	2	As a network security expert, it is your responsibility to know how to use various tools within the Security Onion system. You will generate an attack within Kali Linux in order to trip alerts in Sguil and Kibana. You will need to be able to navigate through the Elastic Stack to investigate logs in order to be a blue team practitioner.	Generating and Analyzing Logs	ログの生成と分析	ラボ6	自動教育指導	中級	対応	2時間	ネットワークセキュリティ専門家としては、セキュリティOnionシステム中の種々のツールの使い方に習熟している必要がある。SguilとKibanaのアラートを作動させるため、Kali Linux中に攻撃を生成する。情報システムセキュリティ分析の実践者となるため、Elastic Stackで検索し、ログを検証する。
143 (v8)	**Identifying Cryptojacking Processes**	Labs Volume 6	Instructional	Advanced	Identify	2	Using a small amount of JavaScript code, websites can utilize your computers CPU and GPU resources, without your knowledge, to mine cryptocurrencies. This type of cyber attack, referred to as "Cryptojacking", saw an 8,500% increase in occurrences throughout 2017. This lab will teach students how to identify these types of attacks through system resource monitoring.	Identifying Cryptojacking Processes	クリプトジャックプロセスの特定	ラボ6	自動教育指導	上級	特定	2時間	小規模なJavaScriptコードを用い、ウェブサイトでユーザーに気づかれることなくコンピュータのCPUやGPUリソースを利用し、暗号通貨を引き出すことができる。この種のサイバー攻撃はCryptojackingと呼ばれ、2017年中に8,500%増加した。このラボでは、システムリソース監視を通じて、この種の攻撃を特定することを学習する。
144 (v8)	**Protecting Against VPNFilter**	Labs Volume 6	Instructional	Advanced	Detect	2	VPNFilter malware was detected on over 500,000 devices in the US by the FBI in May of 2018. As a network security expert, it's crucial you are able to identify the presence of malware on your network. This lab will teach students how to identify the presence of VPNFilter on their network by using Snort to create alerts for traffic associated with the malware.	Protecting Against VPNFilter	VPNフィルターからの保護	ラボ6	自動教育指導	上級	検知	2時間	VPNFilterマルウェアは、FBIにより2018年5月中にアメリカの500,000以上のデバイスで検知された。ネットワークセキュリティ専門家として、ネットワーク上のマルウェアの存在を特定できることは極めて重要である。このラボでは、Snortを用いてマルウェアに関連付けられたトラフィックへのアラートを作成し、ネットワーク上のVPNFilterの存在を特定する方法を学ぶ。
145 (v8)	**Administering Databases and Honeypots**	Labs Volume 6	Challenge	Advanced	Detect	2	As a cybersecurity practitioner, it is your job to use the lessons learned in the Implementing Database Management and Initializing Honeypots labs in order to complete a new challenge.	Administering Databases and Honeypots	データベースとハニーポットの管理	ラボ6	チャレンジ	上級	検知	2時間	サイバーセキュリティ実践者として、データベース管理実装とハニーポットの初期化で学んだ知識を活用し、新しいチャレンジを完了する。
146 (v8)	**Applying Snort Rules and Classifying Pr**	Labs Volume 6	Challenge	Advanced	Detect	2	Using knowledge from the Cryptojacking Identification, Testing Intrusion Detection Systems, and Protecting Against VPNFilter labs, students will complete this final challenge lab for Volume 6.	Applying Snort Rules and Classifying Processes	Snortルールの適用とプロセスの分	ラボ6	チャレンジ	上級	検知	2時間	クリプトジャックの特定、IDSのテスト、VPNFilterからの保護で学んだ知識を用い、ラボ6の最後のチャレンジを完了する。
147 (v9)	**Cyber Hunt**	N/A	Challenge	Intermediate/ Advance	All Domains	8	Go beyond typical lecture-style training to put participants' cybersecurity skills to the test in a capture-the-flag challenge where they can compete against each other and their red teaming skills are evaluated in a live, real-world environment scored by the system. Participants will leverage capabilities from all cybersecurity domains and gain skills in network scanning, vulnerability identification, system hardening, system exploitation, exploitation response and more.	Cyber Hunt	サイバーハント	N/A	チャレンジ	中級/ 上級	全ドメイン	8時間	典型的な講義形式のトレーニングを超えて、参加者のサイバーセキュリティスキルを旗取り合戦形式でテストする。参加者は互いに競争し、ライブの実環境で、レッドチームスキルがシステムによる採点により評価される。参加者は、すべてのサイバーセキュリティドメインに関する能力を活用し、ネットワークスキャン、脆弱性の識別、システムの強化、システムの弱点発見、弱点への対応などのスキルを習得する。

CSX SKILLS ASSESSMENT TOOL	Exclusive to the CSX platform, the CSX Skills Assessment Tool allows you to assess the technical abilities and current skill levels of both your current employees and potential hires. Each assessment provides an on-the-spot evaluation of an individual's cyber strengths and weaknesses, allowing you to make informed hiring, promotional, and development decisions.	CSX SKILLS ASSESSMENT TOOL	CSXスキル評価ツール	本ツールにより、従業員や採用候補者の技術能力や現在のスキルレベルを評価することができます。各評価が、個人のサイバーセキュリティに関する強みや弱点を即座に提供し、採用、昇進、能力開発に関する意思決定の助けとなります。
CSX CYBERSECURITY FUNDAMENTALS COURSE	For those just getting started in cybersecurity, or who need a refresher on foundational concepts, we have included our popular Cybersecurity Fundamentals Course in your package. This non-technical, self-paced course helps students build their knowledge of core cybersecurity concepts, techniques, roles and terminology. A perfect course to quickly train entry-level employees and professionals in related IT roles needing to understand more about cybersecurity concepts.	CSX CYBERSECURITY FUNDAMENTALS COURSE	CSXサイバーセキュリティ基礎コース	サイバーセキュリティの初心者や、基礎概念の復習を必要とする人向けに、本パッケージにサイバーセキュリティ基礎コースを追加しました。この自学習コースでは、サイバーセキュリティの中核となる概念、技術、役割や用語について学ぶことができます。ITの新入社員やサイバーセキュリティの概念への理解を深める必要がある要員の研修に最適なコースです。

AVAILABLE FOR ADDITIONAL PURCHASE TO SUPPLEMENT YOUR PACKAGE:		**パッケージに追加で購入可能なモジュール**		
CSX CYBERSECURITY FUNDAMENTALS CERTIFICATE EXAM	This remote-proctored, online exam is available as an add-on or separate purchase to your Training Platform package. Those passing the exam will earn the CSX Cybersecurity Fundamentals Certificate — a professional, globally-recognized certificate in the foundational concepts and principles that frame cybersecurity.	CSX CYBERSECURITY FUNDAMENTALS CERTIFICATE EXAM	**CSXサイバーセキュリティ基礎試験**	トレーニングプラットフォームパッケージへの追加、もしくは別売で、この遠隔監視のオンライン試験を購入することができます。合格者には、サイバーセキュリティを形成する基礎的な概念や原理に関する世界的に認められた証明書であるCSX基礎証書が付与されます。
CSX PRACTITIONER EXAM	Also available to supplement your package, the CSX Practitioner Certification Exam is an online, remote-proctored exam. This rigorous, 4-hour exam assesses the technical performance of candidates – requiring exam takers to demonstrate critical cybersecurity skills in a live, virtual environment. The exam measures a candidates' analytical ability to identify and resolve network and host cybersecurity issues by applying foundational cybersecurity knowledge and skills required of an evolving cyber first responder.	CSX PRACTITIONER EXAM	**CSX Practitioner 試験**	本パッケージの追加として、オンライン遠隔監視試験であるCSX Practitioner試験も提供しています。この4時間の試験は、ライブの仮想環境で、重要なサイバーセキュリティスキルを実演させることにより、受験者の技術能力を評価するものです。サイバーへの対応者として必要な基礎的サイバーセキュリティの知識やスキルを活用し、ネットワークやホストにおけるサイバーセキュリティン問題を特定し解決する分析能力を試験します。